Základy kybernetickej a informačnej bezpečnosti

— 1. vydanie —

Univerzita Komenského v Bratislave 2020

Táto kniha je výstupom Aktivity D Rozvojového projektu Univerzity Komenského „Vzdelávanie pre informačnú spoločnosť (002UK-2-1/2018)“ v oblasti Podpora vysokých škôl pri plnení záväzkov prijatých v rámci Digitálnej koalície.

Autori:

doc. RNDr. Daniel Olejár, PhD.
je mimoriadny profesor informatiky na FMFI UK a je prorektorom UK pre informačné technológie. Vyše tridsať rokov pôsobí vedecky, odborne a pedagogicky v oblasti informačnej a kybernetickej bezpečnosti. Podieľal sa na tvorbe legislatívy, strategických a koncepčných materiálov, štandardov informačnej a kybernetickej bezpečnosti, pracoval ako expert pre štátne orgány aj súkromné organizácie.

JUDr. Jozef Andraško, PhD.
je prodekan Právnickej fakulty UK pre IT a riaditeľom Ústavu práva informačných technológií a práva duševného vlastníctva. V rámci svojej pedagogickej, vedeckej a výskumnej činnosti sa venuje otázkam informačnej a kybernetickej bezpečnosti, e-Governmentu, elektronickej identity a otvorených údajov.

Ing. Lenka Gondová, CISA, CGEIT, CRISC
je predsedníčkou ISACA Chapter Slovensko. Dlhodobo pracuje v oblasti informačnej a kybernetickej bezpečnosti, najmä v oblasti auditu a pôsobí ako expert pre štátne orgány. Je tiež predsedníčkou Technickej komisie 37 – Informačné technológie Úradu pre normalizáciu, metrológiu a skúšobníctvo SR.

Ing. Ján Hochmann
dlhodobo pôsobí v oblasti informatiky, informatizácie a informačnej bezpečnosti v štátnej správe. Podieľal sa na tvorbe zákonov a štandardov pre informačné systémy verejnej správy, na formovaní a realizácii stratégie informačnej bezpečnosti v SR, budovaní CSIRT.sk, zaslúžil sa o rozvoj vzdelávania v informačnej bezpečnosti.

doc. Ing. Ladislav Hudec, CSc., CISA
je docentom na Fakulte informatiky a informačných technológií Slovenskej technickej univerzity v Bratislave. Vyše dvadsaťpäť rokov sa venuje otázkam spoľahlivosti a bezpečnosti informačných systémov. Tiež pôsobí ako znalec, certifikovaný audítor a nezávislý konzultant v oblasti bezpečnosti informačných systémov.

RNDr. Jaroslav Janáček, PhD.
je odborným asistentom na Katedre informatiky na Fakulte matematiky, fyziky a informatiky UK v Bratislave. Zaoberá sa informačnou bezpečnosťou, počítačovými sieťami, operačnými systémami UNIX/Linux a systémovým programovaním.

RNDr. Richard Ostertág, PhD.
je odborným asistentom na Katedre informatiky na Fakulte matematiky, fyziky a informatiky Univerzity Komenského v Bratislave. Zaoberá sa bezpečnosťou IKT, pričom sa špecializuje na bezpečnosť systémov a zariadení.

Ing. Peter Pištek, PhD.
je senior výskumníkom v Kempelenovom inštitúte inteligentných technológií, kde pôsobí v rámci skupiny zameranej na informačnú bezpečnosť.

doc. RNDr. Martin Stanek, PhD.
je docentom na Katedre informatiky na Fakulte matematiky, fyziky a informatiky Univerzity Komenského v Bratislave. Zaoberá sa informačnou bezpečnosťou a kryptológiou.

Jazyková úprava: Rukopis neprešiel jazykovou úpravou.

Obsah

Kapitola 1

Úvod

Daniel Olejár

Táto kniha je učebnica kybernetickej a informačnej bezpečnosti (KIB). Je určená predovšetkým pre špecialistov KIB a informatikov, ktorí sa priamo nešpecializujú v KIB, ale zabezpečujú prevádzku informačných systémov verejnej správy (ISVS), alebo systémov, na ktoré sú kladené podobné bezpečnostné požiadavky ako na ISVS. Po obsahovej stránke učebnica pokrýva problematiku KIB v rozsahu a na úrovni danej medzinárodnými normami ISO/IEC (konkrétne normami [3–5]) a je kompatibilná s medzinárodnými *de-facto* štandardami definujúcimi obsah informačnej bezpečnosti, [1] a [2]. Primárne je určená ako študijný materiál pre postgraduálne (celoživotné) vzdelávanie, ale môže tiež poslúžiť iným záujemcom na prvé oboznámenie sa s kybernetickou a informačnou bezpečnosťou a úlohami, ktoré KIB rieši. Učebnica vznikla podstatným prepracovaním a doplnením našej knihy [6] a je výstupom rozvojového projektu Vzdelávanie pre informačnú spoločnosť.

Problematika KIB je veľmi rozsiahla a rôznorodá. Narušiť normálne fungovanie IKT totiž môžu prírodné vplyvy, technické poruchy, neúmyselné chyby používateľov, zlá organizácia práce, nedostatok zdrojov, škodlivý softvér, cielené útoky hackerov. Preto aj ochrana IKT využíva množstvo rozličných riešení od obyčajnej kontroly zamestancov a návštevníkov na vrátnici, cez organizačné opatrenia typu „nenechávaj svoj počítač zapnutý, keď na chvíľu opustíš pracovisko“ až po drahé a sofistikované systémy na detekciu pokusov o narušenie IKT. Aby si vedel čitateľ predstaviť, čo všetko môže IKT ohrozovať, ako sa proti tomu brániť, ako zladiť jednotlivé opatrenia do celistvého systému, v druhej kapitole uvádzame stručný prehľad informačnej bezpečnosti a vysvetľujeme základné pojmy KIB. V ďalších kapitolách sa potom zaoberáme jednotlivými oblasťami KIB podrobnejšie.

Tak ako sú rôznorodé hrozby a spôsoby, ktorým sa môžu naplniť, budú rôznorodé aj opatrenia, ktoré tomu majú zabrániť. Opatrenia nie sú nezávislé a bolo by neekonomické (a zrejme aj neefektívne) nezohľadňovať súvislosti medzi hrozbami a samozrejme aj medzi opatreniami. To isté riešenie na ochranu jedného aktíva môže poslúžiť na ochranu ďalších aktív organizácie. Navyše, jednotlivé opatrenia sa dopĺňajú a (pri dobrom návrhu, implementácii a správe) vytvárajú účinný viacvrstvový ochranný systém. Tretia kapitola je venovaná manažmentu kybernetickej a informačnej bezpečnosti, t.j. tomu, ako od jednotlivých *ad hoc* riešení a neustáleho plátania bezpečnostných dier prejsť k systematickému, efektívnemu a udržateľnému riešeniu KIB v organizácii. Okrem toho obsahuje dôležité témy, na ktoré nebude vzhľadom na obmedzený rozsah knihy, priestor, aby mal čitateľ predstavu o úlohe rôznych nástrojov bezpečnostného

orchestra organizácie

Keďže kniha je určená aj pre čitateľov, ktorí nemusia mať informatické vzdelanie, v štvrtej kapitole stručne (a dúfame že stále na prijateľnej úrovni) popisujeme počítače, ich programové vybavenie, najdôležitejšie typy aplikácií a počítačové siete, aby čitateľ získal ucelenejší pohľad na IKT a vedel si predstaviť, ako fungujú informačné a komunikačné systémy, resp. keď budeme hovoriť o možných útokoch a obrane proti nim, aby si vedel predstaviť, na čo sú zamerané útoky a aké možnosti ochrany poskytujú/podporujú jednotlivé komponenty IKS. V tejto kapitole sa stručne dotýkame certifikácie IKT systémov. Hoci sa systémy líšia účelom aj podmienkami, v ktorých pôsobia, je možné definovať základné bezpečnostné požiadavky na systémy (akýsi bezpečnostný model systému, security target), ako návod pre organizácie, ako premietnuť svoje bezpečnostné požiadavky do bezpečnostných funkcií systému a akú úroveň záruk (silu bezpečnostných funkcií) pre svoje účely potrebujú mať. Pritom organizácia si môže vybrať z katalógu hotových bezpečnostných modelov, nejaký z nich si upraviť alebo vytvoriť vlastný. Takáto špecifikácia slúži aj pre vývojárov/dodavateľov systému a tí dokumentujú bezpečnostné funkcie a úrovne bezpečnostných záruk v tzv. protection profile vytvoreného/dodávaného systému. Čitatelia, ktorí majú potrebné znalosti o IKT, môžu začiatok tejto kapitoly preskočiť a prečítať si časti venované certifikácii systémov.

Hovorí sa, že ľudia sú zároveň najslabším aj najsilnejším článkom obrany. Aj najsilnejšie opatrenia sa minú účinkom, ak ich ľudia pracujúci so systémami budú ignorovať. Piata kapitola pojednáva o personánej bezpečnosti. Popisujeme „životný cyklus“ obyčajného zamestnanca— od výberového konania, cez prijatie, zmeny v pracovnom zaradení, až po prepustenie, resp. odchod z organizácie. Zamestnanci organizácie v závislosti od svojho pracovného zaradenia plnia z rozličné úlohy v KIB. Veľa bezpečnostných incidentov v organizácii vzniká preto, že že ľudia nevedia, čo v nejakej situácii majú robiť.[1] Aby zamestnanci (ale aj externí spolupracovníci, dodávatelia a poskytovatelia služieb) vedeli, čo nesmú robiť, čo majú robiť a ako, potrebujú mať znalosti zodpovedajúce ich pracovnému zaradeniu. Budovanie bezpečnostného povedomia zamestnancov je jednou z hlavných úloh manažéra kybernetickej a informačnej bezpečnosti organizácie. V piatej kapitole sú popísané znalosti potrebné pre päť základných bezpečnostných rolí: laikov, vedúcich zamestnancov, informatikov nešpecializujúcich sa v IB, špecialistov v KIB a lektorov.

Aj keď je informácia v elektronickej podobe neviditeľná, technické zariadenia, pomocou ktorých sa spracováva a pamäťové médiá, na ktorých sa uchováva, sú fyzické objekty, ktoré pôsobia v reálnom svete a sú vystavené jeho pôsobeniu. Viaceré negatívne faktory sa môžu uplatniť práve voči materiálnym komponentom IKT. Šiesta kapitola pojednáva o fyzickej bezpečnosti a zaoberá sa hrozbami, voči ktorým sa dá brániť prostredníctvom opatrení fyzického alebo organizačného charakteru.

Veľa útokov na IKT si vyžaduje, aby útočník k nim mal prístup (k fyzickému zariadeniu, alebo do systému napr. prostredníctvom počítačovej siete). Prvá línia ochrany je jasná, nepustiť „dnu“ nepovolaného človeka, neumožniť mu niečo robiť so systémom. Na to slúži riadenie prístupu, ktoré aj bežný používateľ pozná a využíva pri prihlasovaní sa do systému prostredníctvom mena a potvrdzovaní svojich oprávnení pomocou hesla. Siedma kapitola pojednáva stručne, názorne o riadení prístupu a metódach, pomocou ktorých sa uplatňuje.

Internet a počítačové siete vytvorili prepojením jednotlivých systémov globálny virtuálny

[1] ale veľa bezpečnostných problémov narobí úmyselne menší počet nespokojných zamestnancov

priestor a otvorili nebývalé možnosti pre využívanie IKT (komunikácia, informačné zdroje, vzdelávanie, obchodovanie, zábava). Príležitosti sa však chopila aj druhá strana, hackeri, teroristi, podvodníci, zlodeji, skrátka zločinci, ktorí potenciál počítačových sietí a Internetu znaužívajú na vlastné nekalé účely. Nasledujúca ôsma kapitola je určená tým, čo v organizácii zodpovedajú za prevádzku a bezpečnosť IKT a najmä počítačových sietí. Obsahuje podrobný výklad piatich vybraných tém, ktoré sú z hľadiska bezpečnosti počítačových sietí kľúčové.

Kybernetickú a informačnú bezpečnosť je potrebné zohľadňovať v priebehu celého životného cyklu systému. Čo sa však zanedbá na začiatku, ťažko sa napraví neskôr. Preto je deviata kapitola venovaná bezpečnostným požiadavkám ktoré treba zohľadňovať pri nadobúdaní (obstarávaní) nových systémov.

Kryptografia (veda o šifrovaní) poskytuje IB viacero cenných a nenahraditeľných prostriedkov na ochranu obsahu údajov pred nepovolanými osobami, vylúčenie možnosti nepozorovanej zmeny údajov, podvrhnutia falošnej správy a i. Základom kryptografie a spôsobom, ako používať kryptografické mechanizmy v bežných aplikáciách je venovaná desiata kapitola, vybrané problémy kryptológie sú potom podrobnejšie rozobraté v jedenástej kapitole..

Bez IKT už dnes väčšina organizácií nedokáže dlhodobo fungovať. Napriek najlepšej snahe môže dôjsť ke bezpečnostnému incidentu, ktorý vyradí IKT organizácie z činnosti (napr. požiar, záplava, teroristický útok, havária). Organizácia musí rátať aj s takouto krajnou možnosťou a mať pripravený postup na okamžité riešenie prebiehajúceho bezpečnostného incidentu, ktorým by mala zmierniť jeho dopad a minimalizovať škody. Takisto by mala mať definovanú postupnosť krokov na odstránenie následkov bezpečnostného incidentu, aby čo najskôr mohla začať fungovať v náhradnom režime a čo najrýchlejšie obnovila plnú prevádzku (aj) svojich IKT (zachovala kontinuitu svojej činnosti). Dvanásta kapitola sa zaoberá riadením kontinuity činnosti.

Aj pri maximálnej snahe môžu ľudia zodpovední za kybernetickú a informačnú bezpečnsť v organizácii na niečo zabudnúť, alebo si to nevšimnúť (autorská slepota). Audit je nezávislé posúdenie skutočného stavu (systému, organizácie) oproti nejakému ideálnemu stavu. Pomôže organizácii zistiť objektívny stav (v našom prípade) KIB a odhaliť nedostatky, ktoré by v budúcnosti mohli spôsobovať problémy. Auditu je venovaná trinásta kapitola.

Aj keby sa podarilo zákonmi ustanoviť dokonalé pravidlá upravujúce vzťahy v digitálnom priestore, vždy sa nájdu ľudia, ktorí ich budú obchádzať. Aby bolo možné účinne presadzovať právo aj v digitálnom priestore je potrebné vedieť dokázať, že bol porušený zákon, kto to spravil a zaistiť dôkazy, aby bolo možné páchateľa súdne stíhať. Hoci sa aj v digitálnom priestore páchajú klasické, ekonomicky motivované zločiny, páchatelia používajú iné prostriedky ako v reálnom svete a preto si aj riešenie počítačovej kriminality vyžaduje špecifické postupy. Forenznej analýze je venovaná rozsiahla štrnásta kapitola.

Kybernetická a informačná bezpečnosť sa nedá riešiť len lokálne, na úrovni organizácií a jednotlivých systémov. Existujú hrozby, ktoré majú globálny charakter a ich odvrátenie si vyžaduje koordináciu štátnych orgánov a iných zainteresovaných subjektov. Pätnásta kapitola pojednáva o kybernetickej obrane štátu.

Poslednou, 16. kapitolou je stručný výkladový slovník základných pojmov kybernetickej a informačnej bezpečnosti.

Problematika kybernetickej a informačnej bezpečnosti sa vyvíja mimoriadne rýchlo; menia

sa technológie, objavujú nové zraniteľnosti a hrozby. JTC1 SC 27 medzinárodnej štandardizačnej organizácie ISO, zodpovedný za normy informačnej a kybernetickej bezpečnosti reviduje existujúce normy každých 5 rokov a vyvíja nové. Európska únia si uvedomuje nielen aký potenciál predstavujú IKT pre rozvoj spoločnosti, ale aj ich zraniteľnosť. Za niekoľko posledných rokov EÚ posilnila postavenie agentúry ENISA a prijala viacero koncepčných dokumentov, nariadení a direktív zameraných na posilnenie bezpečnosti európskeho kybernetického/digitálneho priestoru (e-IDAS, NIS, GDPR). K veľkým zmenám došlo aj v slovenskej legislatíve. Bol prijatý zákon o kybernetickej bezpečnosti [8], Zákon o ITVS [9] a vypracované podrobné vykonávacie predpisy [7]. Koncepcie a zákony naznačujú trendy, pomenovávajú problémy a vytvárajú rámec pre ich riešenie. Samotné riešenia však závisia od ľudí, kvôli ktorým sa informácie spracovávajú a ktorí sa rôznou mierou podieľajú na prevádzke a používaní IKT. Väčšinu z nich tvoria a pravdepodobne aj dlhodobo budú tvoriť laickí používatelia, ktorí potrebujú mať dostatočné bezpečnostné povedomie, aby vo virtuálnom priestore neutrpeli sami nejakú ujmu, ale ani ju úmyselne alebo zámerne nespôsobili iným. Slovensko však bude potrebovať aj podstatne viac ľudí s vyššou úrovňou znalostí v KIB, ako sú v krátkodobom horizonte schopné pripraviť školy. Navyše, vzhľadom na rýchle sa meniace podmienky, školy môžu svojim študentom poskytnúť základy KIB, ale tieto vedomosti bude potrebné udržiavať a aktualizovať po celý život. Táto učebnica je určená práve pre ľudí z praxe, ktorí potrebujú riešiť bezpečnostné problémy IKT svojej organizácie. Rátame s tým, že ju budeme priebežne aktualizovať a pravidelne vydávať aktualizované vydania tak v elektronickej ako aj papierovej forme.

Literatúra

[1] A. Gordon, ed. *Official (ISC)² Guide to the CISSP CBK*. Angl. 4. vyd. (ISC)² Press. Auerbach Publications, 11. mar. 2015. 1304 strán. ISBN: 9781482262759 (citované na strane 1).

[2] *Information Technology (IT) Security Essential Body of Knowledge (EBK): A Competency and Functional Framework for IT Security Workforce Development*. Washington, D.C.: United States Department of Homeland Security, okt. 2007 (citované na strane 1).

[3] *ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements*. Angl. 2. vyd. ISO a IEC, okt. 2013. 23 strán (citované na strane 1).

[4] *ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls*. Angl. 2. vyd. ISO a IEC, okt. 2013. 80 strán (citované na strane 1).

[5] *ISO/IEC 27005:2018 Information technology – Security techniques – Information security risk management*. Angl. 3. vyd. ISO a IEC, júl 2018. 56 strán (citované na strane 1).

[6] D. Olejár a kol. *Informačná bezpečnosť*. Bratislava: MF SR, 2013 (citované na strane 1).

[7] *Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z.z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy*. 2020 (citované na strane 4).

[8] *Zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov*. 2018 (citované na strane 4).

[9] *Zákon č. 95/2019 Z.z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov*. 2019 (citované na strane 4).

Kapitola 2

Prehľad informačnej a kybernetickej bezpečnosti

Daniel Olejár

2.1 Informatizácia spoločnosti a informačná bezpečnosť

Pri plnení svojich úloh potrebujú organizácie spracovávať množstvo rozličných údajov. Rozsah údajov, ktoré potrebujú spracovávať, v mnohých z nich dávno presiahol možnosti ručného spracovania, a preto sa hľadali možnosti, ako potrebné údaje spracovávať efektívnejšieho. Uspokojivé riešenie priniesol rozvoj a nasadenie digitálnych informačných a komunikačných technológií (digitálnych IKT, ktoré spájajú najdôležitejšie vlastnosti počítačov, telekomunikačných sietí a masovokomunikačných prostriedkov). Digitálne IKT sa na rozdiel od iných informačných a komunikačných technológií (IKT) vyznačujú tým, že

- spracovávajú informáciu zaznamenanú v digitálnej forme,
- na prenos informácie využívajú tie isté komunikačné kanály,
- informácia sa spracováva automatizovane, na základe programov.

Masové nasadenie digitálnych IKT[1] však nevyriešilo len kapacitný problém (spracovanie veľkého množstva informácií), ale spôsobilo hlboké zmeny v metódach spracovania informácie a znamenalo koniec mnohých tradičných postupov založených na papierových dokumentoch. Informácia sa dnes zväčša kóduje digitálne, zaznamenáva v elektronickej forme, prenáša pomocou sietí a spracováva (automaticky alebo poloautomaticky za účasti človeka-operátora) pomocou počítačov. Papierová forma býva nanajvýš na začiatku a občas aj na konci celého procesu, ale informácia sa z papierového sveta „presťahovala“ do virtuálneho priestoru. Tým sa na jednej strane podstatne zvýšila efektívnosť spracovania informácie (množstvo informácie a rýchlosť jej spracovania), ale na druhej strane nebývalo narástla zraniteľnosť organizácie (a v konečnom dôsledku aj celej spoločnosti). Porucha, výpadok, kompromitácia, či zničenie informačných a komunikačných systémov (IKS) a/alebo údajov, ktoré sa v nich spracovávajú môže

[1] keďže v ďalšom texte a celej knihe sa budeme zaoberať predovšetkým digitálnymi IKT, budeme tam, kde to nepovedie k nedorozumeniu používať pre ne len označenie informačné a komunikačné technológie, IKT

vážne ohroziť organizáciu, znemožniť, alebo aspoň výrazne obmedziť jej činnosť (predstavme si, čo by znamenal výpadok riadiaceho systému alebo narušenie údajov atómovej elektrárne, bankového systému, daňového systému, komunikačného systému telekomunikačného operátora, pošty, nemocničného informačného systému, sociálnej poisťovne a pod.) Vzhľadom na objem údajov, ktoré je potrebné priebežne/pravidelne spracovávať, nie je návrat k ručnému spracovaniu informácií možný, a preto normálny chod organizácie, ale aj celej spoločnosti závisí do značnej miery od spoľahlivého fungovania IKT. IKT sú dnes kritickou infraštruktúrou spoločnosti; a to tak tie, od ktorých závisí fungovanie informačnej a komunikačnej infraštruktúry spoločnosti, ale aj tie, ktoré podporujú činnosť dôležitých „neinformačných“ systémov spoločnosti. Nutnou podmienkou na to, aby spoločnosť, jej inštitúcie, ale aj súkromné firmy a občania mohli existovať a pracovať bez problémov, je zaistenie spoľahlivého fungovania informačnej a komunikačnej infraštruktúry spoločnosti. Vzhľadom na vzájomnú prepojenosť systémov sa nestačí obmedziť na ochranu vybraných systémov, ale je potrebné v primeranej miere chrániť všetky informačné a komunikačné systémy, ktoré sa nachádzajú v digitálnom priestore SR a navyše spolupracovať so zahraničnými partnermi na ochrane globálneho digitálneho priestoru, pretože nedostatočne chránený IKS sa môže nielen stať obeťou útočníka, ale aj nástrojom, ktorý útočník využije na útok na iné, významnejšie IKS.

IKT sú zložité, rozsiahle, vzájomne prepojené, pracujú s nimi častokrát laickí používatelia, ohrozujú ich prírodné živly, technické poruchy, ľudské chyby a omyly, škodlivý softvér, cieľavedomé útoky konkurencie, nespokojných zamestnancov, zlodejov, hackerov, teroristov, inštitúcií cudzích štátov či iných protivníkov. Zabezpečiť ich spoľahlivé fungovanie si vyžaduje, aby každý používateľ IKT primerane svojim možnostiam, vedomostiam a postaveniu prispieval k ich ochrane. V tejto knihe budeme hľadať odpoveď na otázky čo je kybernetická a informačná bezpečnosť, ako sa dá zaistiť ochrana IKS v organizácii, aké úlohy pri zaisťovaní kybernetickej a informačnej bezpečnosti v organizácii vyplývajú pre zamestnancov organizácie z ich pracovného zaradenia a napokon čo, prečo a akým spôsobom má používateľ robiť na zaistenie ochrany IKS, s ktorými pracuje, resp. za ktoré zodpovedá.

2.2 Základné pojmy informačnej bezpečnosti

V tejto časti zavedieme a vysvetlíme základné pojmy z informačnej bezpečnosti[2]. Podobne ako samotná informačná bezpečnosť (ako oblasť ľudskej činnosti), tak aj terminológia informačnej bezpečnosti je v súčasnosti vo fáze rýchleho a trocha chaotického vývoja. Je to spôsobené multidisciplinárnym charakterom informačnej bezpečnosti a používaním pojmov z iných disciplín často krát v inom význame ako mali pôvodne; ale najmä rýchlym vývojom informačnej bezpečnosti, ktorý prináša denne nové nepomenované skutočnosti, pre ktoré ich objavitelia neraz zavádzajú pojmy bez očividnej logickej súvislosti (ping of death, spam, smurf attack[3]). Slovenská terminológia informačnej bezpečnosti zatiaľ neexistuje, ale vyhneme sa pokušeniu vytvárať originálne slovenské termíny, ktorým nebude nikto rozumieť ani ich používať a budeme radšej vychádzať z aktuálnej medzinárodnej terminológie. Pri vysvetľovaní základných pojmov sa nevyhneme nutnosti používať ďalšie odborné (zväčša informatické) pojmy. Aby sme čitateľa nezahltili prílišným množstvom podrobností, všetky použité odborné pojmy (vysádzané kurzívou), ktoré nie sú vysvetlené v texte, nájde vo výkladovom slovníku.

[2] kybernetickou bezpečnosťou a jej vzťahom k informačnej bezpečnosti sa budeme zaoberať v druhej časti tejto kapitoly

[3] ping smrti, lunchmeat, šmolkovský útok

Základným pojmom je *informácia*. Vyhneme sa všeobecným filozofickým definíciám[4] a budeme vychádzať z toho, že s informáciou budeme potrebovať pracovať, a teda informácia musí existovať v podobe, alebo sa dať transformovať (človekom, technickým zariadením, počítačovým programom) do podoby, ktorá ďalšie spracovanie umožňuje. Budeme preto predpokladať, že informácia je zaznamenaná v podobe údajov, ktoré majú podobu konečných postupností *znakov* nad nejakou konečnou *abecedou*. Tá istá informácia môže byť zapísaná pomocou rôznych údajov; číslo 100 sa dá vyjadriť slovne: sto, one hundred, ein hundert, zapísať pomocou rímskej číslice C, v hexadecimálnom vyjadrení ako 0x64 a podobne. *Údaje* budeme teda chápať ako zápis informácie a informáciu ako obsah údajov. Informácie získavame rozličným spôsobom - aby sme všetky možnosti pokryli bez nutnosti zachádzania do detailov, budeme predpokladať, že existujú *zdroje informácie*, z ktorých informáciu dokážeme získať a zaznamenať v podobe údajov. Informácia je zriedkavo priamo použiteľná na mieste, kde sme ju získali, a preto ju potrebujeme prenášať na iné miesto, kde ju spracovávame. Informáciu prenášame pomocou *prenosového kanála* spájajúceho zdroj informácie a príjemcu informácie (miesto spracovania). Informácia sa prenosovým kanálom prenáša buď v podobe údajov zaznamenaných na nejakom materiálnom nosiči (list papiera, DVD, USB kľúč) alebo prostredníctvom signálov (elektromagnetických, svetelných zvukových a i.) šíriacich sa prenosovým kanálom (kovový alebo optický vodič, vzduch, kozmický priestor). Prenosový kanál je čokoľvek (technické zariadenie, posol, priestor) čo je schopné preniesť údaje (pri prenose nazývané správou) z miesta A (zdroj) na miesto určenia B (príjemca). Údaje pritom nemusia obsahovať informáciu v podobe, ktorá by umožňovala jej bezprostredné využitie a tak je potrebné ich/ju spracovať. *Spracovaním informácie v úzkom zmysle* rozumieme také operácie s údajmi ako sú triedenie, spájanie, výber, preusporiadanie, vytváranie nových údajov na základe starých, teda v podstate ide o transformácie údajov. V širokom zmysle sa pod spracovaním informácie rozumieme zber, prenos, samotné spracovanie[5], uchovávanie, archiváciu a ničenie údajov. Informácia sa nemusí použiť ihneď po získaní a spracovaní, môže byť zaznamenaná vo forme zápisu údajov na nejakom pamäťovom médiu pre neskoršie použitie (uchovávanie údajov). Ak nie je predpoklad, že sa informácia bude na niečo pravidelne používať, ale možno očakávať, že raz za nejaký čas bude potrebné ju využiť, potom sa archivuje. Archivácia údajov sa od uchovávania údajov líši najmä dostupnosťou: uložené údaje sú spravidla dostupné v podstatne kratšom čase ako archivované údaje a aj oprávnenia na prístup k uloženým a archivovaným údajom sa spravidla líšia. Ak nie je dôvod na archivovanie informácie (napr. uplynula zákonná lehota ich povinného uchovávania a nechceme vynakladať prostriedky na udržiavanie archivovanej informácie, alebo sa obávame, že padne do nepovolaných rúk), údaje sa ničia. Ničenie údajov je jednosmerný proces, ktorého úlohou je zaistiť, aby sa nedala získať informácia obsiahnutá v zničených údajoch. Ničenie údajov sa robí fyzicky—fyzickou likvidáciou pamäťových nosičov, na ktorých boli údaje zaznamenané (mechanickým rozdelením na malé časti, spálením, pôsobením silného elektromagnetického poľa), alebo logicky—bezpečným odstránením údajov z pamäťových médií (napr. vymazaním a niekoľkonásobným prepísaním údajov na magnetických páskach, diskoch).

Spracovanie informácie (v širokom zmysle) je dôležité preto, lebo informácia sa využíva pre zabezpečenie chodu organizácie a/alebo plnenia poslania organizácie (napr. personálna agenda vlastných zamestnancov organizácie, spracovávanie daňových priznaní, evidencia nevybavených objednávok, údaje o poskytnutých službách, odoslané faktúry, účtovné záznamy a pod.). Aby na základe informácie bolo možné prijímať správne rozhodnutia, informácia musí

[4] informácia je (napr.) definovaná ako obsah odrazu

[5] v úzkom zmysle

byť pravdivá, úplná a musí byť dostupná v čase, keď to je potrebné. Navyše, pri spracovaní informácie sa objavujú ďalšie požiadavky, napr. aby sa k informácii nedostali nepovolané osoby, aby bolo možné stanoviť, čo jednotlivé osoby s informáciou môžu robiť a pod. Tieto požiadavky sa nazývajú bezpečnostné požiadavky[6] (na informáciu, resp. IKS) a medzi základné patria: *dôvernosť, integrita, dostupnosť, autentickosť, súkromnosť, nepopretie pôvodu, nepopretie prijatia, anonymita, pseudonymita, zodpovednosť za činnosť v systéme.*

Zaistenie *dôvernosti údajov* znamená, že k informácii obsiahnutej v údajoch majú prístup len tie osoby, ktorým je určená (oprávnené osoby). Zdôrazňujeme rozdiel medzi prístupom k údajom a prístupom k obsahu údajov. Zaistenie prvej požiadavky by znamenalo, že sa údaje spracovávajú spôsobom, pri ktorom je vylúčená prítomnosť nepovolaných osôb, čo je nerealistický predpoklad[7]. V druhom prípade „stačí“, aby boli bola informácia zapísaná prostredníctvom takých údajov, že pre všetky osoby okrem oprávnených, bude nezrozumiteľná; t.j. aby nemohli získať z údajov ich informačný obsah.

Zaistenie *integrity údajov* znamená, že údaje nemôžu byť nepozorovane modifikované bez toho, aby si to oprávnená osoba všimla. Ideálne by bolo, keby bolo možné vylúčiť akýkoľvek neoprávnený zásah do údajov počas ich spracovania, ale to sa vzhľadom na charakter a zložitosť systémov, v ktorých sa údaje spracovávajú, nedá garantovať. Ak oprávnená osoba zistí, že údaje boli neoprávnene upravované, nebude sa spoliehať na informáciu, ktorú obsahujú, ale môže si ich od toho, kto jej ich poskytol, vyžiadať ešte raz[8].

Zaistenie *dostupnosti údajov* znamená, že údaje sú k dispozícii oprávneným osobám v ideálnom prípade kedykoľvek, keď o to požiadajú. Táto absolútna požiadavka sa dá zovšeobecniť tak, že sa stanoví maximálny čas od požiadavky na sprístupnenie údajov až po okamih, keď žiadateľ má údaje k dispozícii; alebo sa dostupnosť definuje časom, kedy sú údaje k dispozícii[9].

Naplnenie požiadavky na *autentickosť údajov* znamená, že príjemca si môže byť istý tým, že údaje sú zhodné s tými, ktoré poslal odosielateľ a identitou odosielateľa (z akého zdroja pochádzajú). Autentickosť teda v sebe spája integritu údajov a jednoznačné/garantované určenie identity tvorcu údajov.

Súkromnosť (privacy) sa vzťahuje na osobné údaje a znamená, že človek má možnosť stanoviť, ktoré jeho osobné údaje, komu a za akých podmienok budú sprístupnené. (Súkromnosť sa uplatňuje napr. pri sprístupňovaní údajov zdravotnej dokumentácie vyhradenému okruhu osôb: ošetrujúcim lekárom, explicitne stanoveným príbuzným alebo právnym zástupcom pacienta.) Súkromnosť je slabšia požiadavka ako dôvernosť; na zaistenie súkromnosti napr. zdravotnej dokumentácie stačí oddeliť osobné údaje, ktoré umožňujú určiť identitu pacienta od výsledkov vyšetrení. Ak sa potom protivník dostane k anonymným údajom, nevie, na koho sa vzťahujú.

Ďalšie dve bezpečnostné požiadavky sa vzťahujú na komunikáciu: *nepopretie pôvodu (non repu-diation of origin)* správy znamená potvrdenie toho, že tvorca/odosielateľ správy správu

[6] ak je na údaj kladená nejaká bezpečnostná požiadavka, napríklad na jeho integritu, integrita sa nazýva aj bezpečnostným atribútom údaju (a spravidla sa predpokladá, že je v prípade daného údaju aj nejakým spôsobom zabezpečená)

[7] predstavme si napríklad prenos údajov prostredníctvom bezdrôtovej siete alebo Internetu

[8] existujú aj metódy rekonštrukcie poškodených údajov, tzv. samoopravné kódy

[9] absolútna dostupnosť by sa dala vyjadriť tak, že údaje sú dostupné nepretržite alebo, že čas od požiadavky na prístup k údajom po poskytnutie údajov je nulový (resp. daný technickými parametrami - rýchlosť vyhľadania údajov a doba prenosu od zdroja k žiadateľovi)

poslal a *nepopretie prijatia (non repudiation of receipt)* zasa, že príjemca správy správu preukázateľne dostal.

Na vysvetlenie ďalších pojmov potrebujeme definovať základné pojmy týkajúce sa identifikácie. Ľubovoľná vec, údaje, dokument, človek, alebo dokonca niečo tak abstraktné ako myšlienka, sa nazýva *entita*. Entita sa vyznačuje nejakými vlastnosťami (*atribútmi*). Množina atribútov[10], ktoré umožňujú jednoznačne odlíšiť danú entitu od podobných entít, sa nazýva *identita danej entity*. Všetky atribúty, ktoré prislúchajú danej entite, tvoria *absolútnu (úplnú) identitu* danej entity. Absolútna identita môže byť veľmi rozsiahla a na jednoznačné určenie entity v nejakej menšej oblasti bude stačiť aj podmnožina atribútov absolútnej identity. Preto sa pojem identity viaže na *oblasť použitia* a identitou entity je ľubovoľná množina atribútov, ktorá stačí na jednoznačné určenie entity v danej oblasti použitia identity. Napríklad, ak sú v miestnosti dvaja ľudia matka a dieťa, tak na určenie dieťaťa stačí ktorýkoľvek z atribútov rok narodenia, výška, váha, rodinný vzťah, zamestnanie a i. Na rýchle určenie entity možno vytvoriť aj umelú entitu, *identifikátor*, špeciálny atribút, ktorého jedinou úlohou je plniť funkciu identity danej entity v presne definovanej oblasti použitia. Identifikátorom je napríklad rodné číslo osoby, IČO, DIČ, sériové číslo výrobku a pod. Na identitu sa často viažu nejaké jedinečné oprávnenia, napríklad prístup k nejakej službe, alebo ku zdrojom. Aby napr. človek nemohol prebrať zásielku určenú inému človeku, musí doručovateľovi (ktorý ho osobne nepozná), preukázať svoju identitu. Tento úkon sa skladá z dvoch častí: *identifikácie* a *autentifikácie/autentizácie*. Pri identifikácii entita deklaruje svoju identitu (alebo v inom prípade človek deklaruje identitu nejakej entity, napríklad vo forme tvrdenia „toto je moje auto“). Identifikácia sama o sebe na stanovenie identity nestačí, pretože môže byť falošná. (Človek sa môže vydávať za niekoho iného.) Druhá strana si preto musí overiť pravdivosť deklarovanej identity (tento úkon sa nazýva autentizácia). To sa v prípade osôb robí troma rôznymi spôsobmi alebo ich kombináciou:

1. na základe toho, čím človek je (biometrické charakteristiky ako sú odtlačky prstov, obraz sietnice, DNA, výzor);
2. toho, čo človek má (identifikačný/autentizačný token: preukaz totožnosti, preukaz zamestnanca),
3. alebo toho, čo človek vie (heslo, PIN, prístupový kód, osobné údaje[11]).

Pri autentizácii musí mať overovateľ identity možnosť overiť, či poskytnuté autentizačné údaje sa viažu na danú identitu. V bežnom živote na overovanie identity (totožnosti) slúžia rôzne preukazy (u osôb občiansky preukaz, pas), ktoré vydala dôveryhodná autorita (poskytovateľ identity), v počítačoch sa človek identifikuje prihlasovacím menom a na autentizáciu používa heslo, kartu, alebo odtlačok prsta.

Bezpečnostná požiadavka *zodpovednosť za činnosť v systéme (accountability)*[12] znamená, že k jednotlivým činnostiam v systéme je možné jednoznačne priradiť entitu (človeka, proces), ktorá ich vykonala alebo spôsobila.

[10] presnejšie, mali by sme rozlišovať atribút a jeho hodnotu, napr. krstné meno: Fero, ale kvôli zjednodušeniu textu nebudeme tam kde to nepovedie k nedorozumeniu striktne odlišovať atribút a jeho hodnotu, ale pod pojmom atribút budeme rozumieť názov atribútu a jeho hodnotu

[11] napr. rodné meno babičky z matkinej strany

[12] možné preklady by boli napr. dosledovateľnosť, zúčtovateľnosť

Anonymita a *pseudonymita* sú bezpečnostné požiadavky, ktoré chránia súkromie človeka a sú v istom zmysle opačné k požiadavke na accountability. *Anonymita* znamená, že zo získaných atribútov nie je možné jednoznačne určiť entitu (osobu), ktorej prislúchajú (situácie v ktorých je anonymita žiaduca sú napr. surfovanie po Internete, nakupovanie). Pseudonymita je slabšou požiadavkou ako anonymita; entita vystupuje pod identitou, ktorú vo všeobecnosti nie je možné priradiť konkrétnej osobe (prezývka, pseudonym, nick), ale obmedzený okruh (dôveryhodných) osôb vie jednoznačne identifikovať osobu na základe jej pseudonymu (a prípadne ďalších atribútov, ktoré má k dispozícii).

Pri spracovaní informácie môže dôjsť k udalostiam, ktoré spôsobia porušenie niektorej z bezpečnostných požiadaviek buď priamo pôsobením na údaje, zásahom do IKT, prostredníctvom ktorých sa spracovávajú, alebo prostredia, v ktorom IKT spracovávajúce dané údaje, pôsobia. Takéto udalosti sa nazývajú bezpečnostné incidenty. To, čo môže spôsobiť bezpečnostný incident[13], sa nazýva *hrozba (threat)*. Hrozbou je napríklad požiar, záplava, zemetrasenie, technická porucha, ľudská chyba, nedostatok zdrojov, výpadok napájania, únik citlivej informácie, sabotáž, útok hackera a pod. Hrozba má svojho *nositeľa* (záplava - prasknuté kanalizačné potrubie, dážď, rieka) a na to, aby nastala, musí v systéme, alebo jeho okolí byť niečo, čo umožňuje hrozbe prejaviť sa; a to *zraniteľnosť (vulnerability)*. Zraniteľnosťou môže byť nejaký nedostatok (poškodená strecha, slabé heslo, zlé nastavenie počítača) alebo aj spôsob používania systému (prístup do počítača zo siete kvôli správe na diaľku). Ak sa hrozba naplní, (dôjde k bezpečnostnému incidentu) má to pre údaje, systém, technické zariadenia alebo organizáciu nejaké negatívne dôsledky, *dopad*. Dopad hrozby je možné merať kvantitatívne (napr. finančné vyjadrenie) — prostriedkami, ktoré je potrebné vynaložiť na odstránenie následkov bezpečnostného incidentu, ale sú dopady, ktorých hodnotu je ťažké kvantifikovať (narušenie dobrého mena, strata obchodných príležitostí, zranenie alebo smrť človeka), a preto sa popri kvantitatívnom hodnotení dopadov používa *kvalitatívne hodnotenie* (dopad môže mať závažnosť nízku, strednú alebo vysokú). Hrozba môže mať (v prípadne keď nastane) pre organizáciu katastrofálne následky (pád lietadla na budovu, zemetrasenie), ale pravdepodobnosť, že sa takáto hrozba naplní, je malá. Veličina, ktorá zohľadňuje tak dopad naplnenia hrozby, ako aj pravdepodobnosť jej naplnenia sa nazýva *riziko*. Pre zaistenie ochrany systémov, informácií a iných aktív organizácie pred hrozbami, potrebujeme identifikovať riziká a stanoviť ich hodnoty. Hodnota rizika je z matematického hľadiska stredná hodnota dopadu spôsobeného danou hrozbou; t.j. súčin pravdepodobnosti a závažnosti dopadu. (Ak má organizácia 100 osobných počítačov v a pravdepodobnosť krádeže v priebehu jedného roka je 5%, tak riziko vyplývajúce z hrozby krádež osobného počítača je $0.05 \times 100 \times$ cena (PC + náklady na jeho obstaranie a inštaláciu)). Aj hodnota dopadu aj pravdepodobnosť naplnenia hrozieb sa spravidla ťažko vyjadruje kvantitatívne. Preto sa pri výpočte rizika používa kvalitatívne ohodnotenie pravdepodobnosti naplnenia hrozby (pravdepodobnosť je vysoká, stredná, nízka, prípadne nulová) a namiesto numerického výpočtu sa riziko vypočítava na základe tabuľky[14].

Primeraná ochrana systému (organizácie) vychádza zo znalosti rizík a zavádzaní riešení, ktoré ich buď úplne eliminujú, alebo aspoň znížia ich hodnotu na akceptovateľnú úroveň. Na určenie a ohodnotenie rizík, ktoré sú pre organizáciu relevantné, slúži *analýza rizík*. Pri analýze rizík sa najprv identifikuje všetko, čo má pre organizáciu hodnotu a čo by mohlo byť narušené

[13] definíciu bezpečnostného incidentu neskôr ešte formalizujeme, na začiatok však vystačíme s uvedenou definíciou

[14] podrobnosti čitateľ nájde v časti Spravovanie rizík

bezpečnostných incidentom. Ide o zariadenia, údaje, znalosti, finančné prostriedky, kvalifikovaných ľudí, infraštruktúru, reputáciu organizácie, skrátka všetko, čo organizácia potrebuje na to, aby mohla plniť svoje poslanie. Tieto entity sa nazývajú *aktívami (assets)* organizácie. Potom sa identifikujú hrozby, ktoré sú relevantné pre danú organizáciu (môžu negatívne pôsobiť na niektoré aktíva) a vyčíslia riziká. (Podrobnejšie sa touto problematikou budeme zaoberať v časti analýza rizík). Organizácia si určí hranicu akceptovateľného rizika a prijme opatrenia, ktoré znížia riziká pod túto úroveň. Opatrenia môžu mať rozličný charakter: fyzické opatrenia, personálne opatrenia, logické opatrenia (bezpečnostné opatrenia implementované pomocou počítačových programov) a i. Niektoré hrozby môžu mať pre organizáciu fatálne následky, ale pravdepodobnosť ich naplnenia je malá (požiar, pád lietadla, v našich podmienkach teroristický útok, zemetrasenie a pod.) Zavádzať opatrenia na elimináciu všetkých rizík vyplývajúcich z takýchto hrozieb by pravdepodobne prekračovalo možnosti organizácie a preto sa volí iné riešenie: organizácia prejde všetky možné katastrofické scenáre a pripraví postupy tak pre riešenie krízových situácií ako aj pre rýchle obnovenie normálneho stavu po prekonanej katastrofe (havarijné plány a plány kontinuity činnosti).

Podmienky v organizácii sa môžu meniť a môžu sa objaviť nové hrozby, resp. meniť hodnota rizík. Aby bola ochrana aktív organizácie účinná a primeraná, organizácia musí priebežne spravovať/riadiť riziká (monitorovať systémy, kontrolovať dodržiavanie prijatých opatrení, riešiť a analyzovať bezpečnostné incidenty, upravovať existujúce a prijímať nové bezpečnostné opatrenia). Okrem priebežných a čiastkových kontrol by organizácia pravidelne, alebo po veľkých bezpečnostných incidentoch mala nechať preveriť úplnosť a primeranosť prijatých opatrení formou bezpečnostného auditu a na základe výsledkov auditu spraviť prípadné korekcie bezpečnostných opatrení. *Bezpečnostný audit* má za cieľ zistiť, či sú v organizácii dosiahnuté ciele stanovené nejakým dokumentom (bezpečnostným štandardom, zákonom, normou alebo bezpečnostnou politikou organizácie). Bezpečnostný audit vykonáva kvalifikovaná osoba, interný alebo externý audítor (bezpečnosti informačných systémov).

Teraz môžeme definovať aj samotný pojem informačná bezpečnosť. Tento pojem sa používa v trojakom význame:

1. označuje interdisciplinárnu oblasť, ktorá sa zaoberá skúmaním hrozieb a vývojom metód ochrany;
2. na označenie aktivít zameraných na dosiahnutie dostatočnej úrovne ochrany informácie a napokon
3. znamená ideálny stav systému (organizácie), kedy sú eliminované všetky riziká vyplývajúce z hrozieb voči aktívam systému (organizácie).

V tomto texte budeme používať pojem informačná bezpečnosť vo všetkých troch, najmä však v posledných dvoch významoch.

2.3 Kybernetická bezpečnosť

Popri pojme informačná bezpečnosť sa najmä v anglicky hovoriacom prostredí používajú pojmy cyberspace, cybercrime, cybersecurity. Zaslúžil sa o to spisovateľ Wiliam Gibson, ktorý začiatkom 80-tych rokov v poviedke Burning Chrome na neskôr v románe Neuromancer použil pojem

kybernetický priestor (cyberspace). Podľa jeho vlastného vyjadrenia slovo cyberspace síce znelo dobre, ale nemalo konkrétny význam[15]. V súvislosti s rozvojom Internetu sa však bezobsažný pojem kybernetický priestor ujal a začal sa používať na označenie Internetu, resp. globálnej technickej informačnej a komunikačnej infraštruktúry (počítačov prepojených sieťou)[16]. Keďže informačná bezpečnosť mala veľmi široký záber a väčšina informácií sa spracovávala pomocou digitálnych IKT, ktoré sa extrémne rýchlo vyvíjajú v porovnaní so svojím prostredím[17], pozornosť informačnej bezpečnosti sa sústreďuje najmä na ochranu informácie v elektronickej forme, spracovávanej pomocou digitálnych IKT, t.j. v kybernetickom priestore. Niekde tam treba hľadať pôvod pojmu kybernetická bezpečnosť, ktorý síce nemá jednoznačne stanovený význam[18], ale v kľúčovom dokumente EÚ (Stratégia kybernetickej bezpečnosti) sa používa vo význame informačnej bezpečnosti kybernetického priestoru. Ani smernica NIS explicitne nehovorí o kybernetickom priestore ani o kybernetickej bezpečnosti; namiesto kybernetického priestoru používa pojem „siete a informačné systémy“ a nepriamo definuje kybernetickú bezpečnosť ako

> „bezpečnosť sietí a informačných systémov“ je schopnosť sietí a informačných systémov odolávať na určitom stupni spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov[19];

t.j. ako informačnú bezpečnosť kybernetického priestoru. Hoci prísne vzaté informačná bezpečnosť má širší záber (zaoberá sa aj ochranou informácie, ktorá nie je v elektronickej forme, rieši fyzickú, personálnu bezpečnosť, právne vzťahy, štandardy a pod.) z praktického hľadiska je rozumné považovať informačnú a kybernetickú bezpečnosť za synonymá, lebo zaistenie bezpečnosti informácie v kybernetickom priestore nie je možné bez toho, aby nebolo primerane chránené aj jeho bezpečnostné okolie. (Je jedno, či sa nepovolaná osoba dostane k dôvernej informácii v elektronickej, alebo papierovej forme.) Spojenie informačnej a kybernetickej bezpečnosti je dôležité aj z hľadiska štandardizácie. V ISO pôsobí Spoločný technický výbor číslo 1 pre štandardizáciu informačných a komunikačných technológií, ktorý má podvýbor číslo 27, zaoberajúci sa informačnou bezpečnosťou. Momentálne existuje cca 200 noriem venovaných rozličným aspektom informačnej bezpečnosti a dve (ISO/IEC 27032 a ISO/IEC 27103) venované kybernetickej bezpečnosti; prvá z nich sa hneď v preambule odvoláva na základnú terminologickú normu informačnej bezpečnosti ISO/IEC 27000, druhá popisuje použitie štandardov

[15] All I knew about the word "cyberspace" when I coined it, was that it seemed like an effective buzzword. It seemed evocative and essentially meaningless. It was suggestive of something, but had no real semantic meaning, even for me, as I saw it emerge on the page.

[16] Cyberspace-the globally interconnected information infrastructure that includes the Internet, telecommunications networks, computer systems, and industrial control systems in Trustworthy cyberspace: Strategic plan for the Federal cybersecurity Research and Development program, Executive Office of the President National Science and Technology Council, Decembar 2011

[17] spracovanie informácií zaznamenaných v listinnej/papierovej podobe ručne

[18] Definition of Cybersecurity—Gaps and overlaps in standardisation v1.0, ENISA, December 2015

[19] v origináli: 'security of network and information systems' means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems;

informačnej bezpečnosti na riešenie kybernetickej bezpečnosti. Striktné odlíšenie kybernetickej a informačnej bezpečnosti by sťažilo až znemožnilo používanie terminológie a štandardov informačnej bezpečnosti a viedlo k nutnosti vypracovať vlastné štandardy pre kybernetickú bezpečnosť, čo vzhľadom na rozsah a možnú nekompatibilitu nie je reálne. Z týchto dôvodov budeme tam, kde nebude vyložene potrebné odlíšiť kybernetickú a informačnú bezpečnosť, používať pojem kybernetická a informačná bezpečnosť, v skratke KIB.

V tejto časti sme sa obmedzili len na vysvetlenie základných pojmov informačnej bezpečnosti; dôležitých pojmov potrebných pre pochopenie bezpečnostných problémov a spôsobov ich riešenia je samozrejme podstatne viac. Najdôležitejšie z nich nájde čitateľ v ďalšom texte a zhrnuté v priloženom stručnom výkladovom slovníku pojmov informačnej bezpečnosti.

Poznámka.

V tejto časti sme okrem úpravy pôvodného textu [1] využili aj časť vlastného textu z knihy [2]

Literatúra

[1] D. Olejár a kol. *Informačná bezpečnosť*. Bratislava: MF SR, 2013 (citované na strane 15).

[2] Andraško J., Gábriš T., Hochmann J. a Olejár, D. *Zákon o kybernetickej bezpečnosti č. 69/2018. Z.z., Komentár*. Wolters Kluwer, 2018 (citované na strane 15).

Si vis pacem, para bellum

Publius Flavius Vegetius Renatus

Kapitola 3

Manažment informačnej bezpečnosti

Daniel Olejár

3.1 Úvod

Väčšina organizácií v súčasnosti spracováva informácie ktoré potrebuje pre vykonávanie svojej činnosti pomocou digitálnych IKT[1]. Ako sme spomenuli v úvode, pre spracovanie veľkého množstva informácií neexistuje v súčasnosti k IKT ekvivalentná alternatíva a preto sa IKT stali časťou kritickej infraštruktúry organizácií, bez ktorej už organizácie nedokážu plniť svoje poslanie. Ak má preto organizácia plniť svoje úlohy, musí sa postarať o to, aby nedošlo k narušeniu jej IKT, ani k narušeniu údajov/informácií, ktoré sa v nich spracovávajú. Význam IKT pre fungovanie organizácií a v konečnom dôsledku celej spoločnosti si uvedomuje aj štát a prostredníctvom zákonov, vykonávacích predpisov, povinných štandardov a iných právnych predpisov definuje povinné požiadavky na rozsah, úroveň a spôsob ochrany (niektorých alebo všetkých) údajov a IKT organizácií. Požiadavkami na zaistenie KIB vyplývajúcimi zo zákonov sa v budúcnosti plánujeme zaoberať podrobnejšie v samostatnej kapitole, teraz na tomto mieste spomenieme na ilustráciu „len“ povinné bezpečnostné opatrenia pre informačné systémy verejnej správy uvedené vo zákone [14] a vo vyhláške [13]. Požiadavky rôznych zákonov na ochranu informácie, IKT resp. informačné a komunikačné systémy (IKS) sa dajú vyjadriť pomocou štandardných bezpečnostných požiadaviek a úrovní záruk, ktoré prijaté riešenia musia poskytovať. Na ich splnenie stačí použiť jednotný postup, popísaný napr. v medzinárodných normách ISO/IEC radu 27000, z ktorých vychádzajú aj bezpečnostné štandardy spomenutej vyhlášky [13]. Úvodzovky sme v predchádzajúcej vete použili preto, lebo hoci je v ISO normách dostatočne podrobne popísané, čo je potrebné spraviť na dosiahnutie potrebnej úrovne kybernetickej a informačnej bezpečnosti v organizácii, dodržať postupy popísané v normách a naplniť požiadavky, ktoré stanovujú nie je ľahká úloha.

Na dosiahnutí a udržiavaní potrebnej úrovne KIB v organizácii nebude stačiť kúpiť a implementovať nejaké technologické riešenia, jednorazovo angažovať externých špecialistov, resp. poveriť zodpovednosťou za KIB niekoľkých ľudí v organizácii. Budovanie a udržiavanie informačnej bezpečnosti je trvalý proces, do ktorého bude potrebné v primeranej miere zapojiť všetkých ľudí, ktorí pracujú s IKT organizácie a/alebo môžu ovplyvniť ich činnosť; t.j. od vedúcich pracovníkov až po servisný personál a externých spolupracovníkov.

[1] keďže v tejto knihe sa budeme venovať predovšetkým bezpečnosti digitálnych IKT, budeme tam, kde to nepovedie k nedorozumeniu, namiesto d-IKT používať len stručnejšie IKT.

Vedúci pracovník organizácie je zodpovedný za organizáciu ktorú riadi, vrátane splnenia bezpečnostných požiadaviek vyplývajúcich zo zákonov a v konečnom dôsledku aj za zaistenie potrebnej úrovne kybernetickej a informačnej bezpečnosti vo „svojej“ organizácii. Hoci nemusí byť odborníkom na kybernetickú a informačnú bezpečnosť a môže poveriť riadením IB iných zamestnancov organizácie, nemôže sa zbaviť ani zodpovednosti za KIB v organizácii ani vyhnúť prijímaniu kľúčových rozhodnutí o KIB (ako sú stratégia KIB, personálne zabezpečenie, financovanie KIB, záväzné postupy pre zaistenie KIB, klasifikácia informácie, disciplinárne postihy za spôsobené bezpečnostné incidenty, zosúladenie riadenia organizácie a riadenia KIB a i.). Aby tieto povinnosti dokázal kompetentne plniť, musí mať aspoň základné znalosti o KIB, vedieť ich aplikovať na „svoju“ organizáciu, musí vedieť stanoviť priority KIB v organizácii, definovať zodpovednosť pracovníkov organizácie za KIB, stanoviť hlavné úlohy v KIB a musí dokázať kontrolovať ich plnenie.

Väčšinu kľúčových činností potrebných na dosiahnutie a udržiavanie dostatočnej úrovne KIB v organizácii však budú musieť vykonávať špecialisti na KIB a informatici. Tí budú musieť zvládnuť problematiku KIB do takej miery, aby vedeli napísať rozumnú koncepciu KIB v organizácii a rozpracovali ju do postupov realizovateľných v každodennom živote. Budú sa musieť naučiť posudzovať hrozby, vyhodnocovať riziká, ktoré z nich vyplývajú, hľadať zraniteľnosti a posudzovať vhodnosť, technickú a ekonomickú náročnosť opatrení, ktoré prichádzajú do úvahy na odstránenie, alebo aspoň ošetrenie odhalených zraniteľností. Hoci si organizácia môže najať externých špecialistov na riešenie jednorazových špecifických úloh, informatici a interní špecialisti na KIB sa budú musieť naučiť samostatne riešiť bežné bezpečnostné problémy v organizácii, monitorovať účinnosť prijatých opatrení a aj vykonávať audity zamerané na vyhodnotenie celkovej úrovne bezpečnosti v organizácii; resp. naučiť sa efektívne spolupracovať s externými špecialistami pri riešení problémov, na ktoré ich možnosti nebudú stačiť.

Prevažnú väčšinu pracovníkov organizácie tvoria používatelia IKT, ktorí majú o princípoch ich fungovania len laické vedomosti a o KIB nanajvýš základné predstavy. Napriek nízkym oprávneniam, ktoré používatelia majú v systémoch organizácie, môžu na jednej strane úmyselne alebo z nevedomosti spôsobovať vážne bezpečnostné problémy, ale na druhej strane môžu pozitívne prispieť k úrovni KIB v organizácii. Vzhľadom na ich informatické vzdelanie, ale najmä potreby nemá význam laických používateľov masovo školiť v KIB. Laický používateľ potrebuje vedieť, žo má robiť, čo nesmie robiť, ako rozpoznať, že sa v IKS deje niečo podozrivé, čo má spraviť a na koho sa má obrátiť. Tieto všeobecné požiadavky na laických používateľov sa rýchlo konkretizujú v bezpečnostnom procese; mnohé z nich vyplynú už z dokumentov rozpracovávajúcich bezpečnostnú politiku (bezpečnostnú koncepciu) organizácie a ak sa pri spracovaní bezpečnostnej politiky, bezpečnostných smerníc a praktík na niečo podstatné zabudlo, bezpečnostné incidenty rýchlo odhalia nedostatky. Organizácia sotva bude mať špecializovaných lektorov informačnej bezpečnosti; externí školitelia sú použiteľní na prípravu špecialistov KIB, ale nepoznajú pomery v organizácii. Laickí používatelia potrebujú konkrétne vedomosti, školiť ich (v tom, čo z KIB potrebujú pre svoju prácu vedieť) preto budú musieť informatici a špecialisti na KIB z vlastnej organizácie.

Zaistiť natrvalo potrebnú úroveň IB v organizácii nie je ani jednoduché, ani lacné. Ak má organizácia vyhovieť všetkým bezpečnostným požiadavkám a naplniť svoje potreby v KIB efektívnym spôsobom, mala by od riešenia čiastkových bezpečnostných problémov prejsť k systematickému riešeniu, kde mnohé bezpečnostné problémy vyrieši spoločnými preventívnymi opatreniami, na podobné problémy bude využívať rovnaké už raz vyvinuté riešenia, opatrenia sa

budú vzájomne dopĺňať a ich účinnosť bude organizácia priebežne monitorovať, pravidelne vyhodnocovať a v prípade potreby ich bude aktualizovať a prípadne prijímať nové. Skôr či neskôr bude organizácia potrebovať zaviesť systém riadenia (manažmentu) informačnej bezpečnosti[2]. Hoci názov systém riadenia (manažmentu) informačnej bezpečnosti (v origináli Information Security Management System, ISMS) znie zložito až odstrašujúco, zavedenie ISMS predstavuje postupnosť prirodzených krokov, ktoré si v tejto kapitole stručne popíšeme.[3]

Poznámka.

Do tejto kapitoly sme zaradili viacero tém, pre ktoré existujú rozsiahle samostatné normy, ale v tejto učebnici na ich podrobnejšie rozpracovanie nebol priestor. Uvádzame tu základné informácie o analýze rizík, personálnej bezpečnosti, klasifikácii informácie a systémov a ďalších oblastiach IB a uvádzame zdroje, z ktorých sa čitateľ v prípade záujmu môže získať podrobnejšie informácie.

3.2 Bezpečnostná stratégia a bezpečnostná politika organizácie

Organizácia aj jej vedenie si najprv potrebuje vytvoriť predstavu o úlohe, ktorú potrebuje riešiť (zaistenie dostatočnej úrovne KIB v organizácii), stanoviť základné ciele a postup na ich dosiahnutie; t.j. vypracovať vlastnú bezpečnostnú stratégiu[4]. Bezpečnostná stratégia musí mať presne stanovenú oblasť pôsobnosti; t.j. musí byť jasne definované, na čo sa vzťahuje (či na celú organizáciu, jej IKT, alebo len na nejaký dôležitý systém) a v oblasti svojej pôsobnosti musí definovať:

- čo treba chrániť,
- na akej úrovni a
- čo pre to organizácia je ochotná/pripravená spraviť.

Bezpečnostná stratégia[5] má najčastejšie podobu písomného dokumentu, ktorý sa nazýva bezpečnostná politika (výstižnejší názov by bol politika kybernetickej a informačnej bezpečnosti, alebo politika bezpečnosti IT/IKT, ale v odbornej literatúre sa používa termín bezpečnostná

[2] pre ISVS táto povinnosť vyplýva zo Zákona [14]

[3] ISO normy zatiaľ nezareagovali na zmenu terminológie, ale ako ukazuje pripravovaná norma ISO/IEC 27100 Information technology — Cybersecurity — Overview and concepts, v kybernetickej bezpečnosti sa v plnom rozsahu uplatňujú postupy popísané v sérii noriem ISO/IEC 27xxx. V ďalších častiach tejto kapitoly budeme odvolávať na ISO normy, ktoré neboli terminologicky upravené a preto budeme používať zaužívané pojmy informačnej bezpečnosti (napríklad v kontexte ISMS), ale budeme popisovať riešenia, ktoré pokrývajú aj požiadavky na kybernetickú bezpečnosť; najmä tie, ktoré vyplývajú z legislatívy a nie sú pokryté štandardnými opatreniami informačnej bezpečnosti.

[4] viacero pojmov môže u čitateľa vzbudiť obavu, že vyjadrujú niečo zložitého. Vo väčšine prípadov ide o zbytočné obavy, ale používanie jednoduchšie znejúcich vlastných termínov by mu spôsobilo problémy neskôr, keď bude potrebovať čítať odborné texty používajúce štandardnú terminológiu KIB. V prípade, keď si nebude istý, aký je význam nejakého pojmu, odporúčame mu pozrieť sa do výkladového slovníka.

[5] rôzne zákony a vykonávacie predpisy požadujú vytvorenie inak nazvaných dokumentov podobného zamerania. V tejto kapitole sa budeme pridržiavať noriem ISO/IEC 27001 a 2.

politika, a preto sa ho budeme držať aj my.) Ako sme už spomenuli, za celú organizáciu, vrátane primeranej úrovne KIB zodpovedá vedenie organizácie. To musí iniciovať aj systematické riešenie KIB v organizácii (zavedenie systému manažmentu KIB[6], ak sa ku KIB doteraz takto v organizácii nepristupovalo), resp. pravidelné revízie systému manažmentu KIB ak ho organizácia má zavedený a využíva ho, aby sa zaistila jeho aktuálnosť, účinnosť a efektívnosť. Začneme najjednoduchším[7] prípadom, keď sa KIB v organizácii ešte len začína riešiť a bezpečnostný proces[8] sa spúšťa od začiatku a týka sa celej organizácie.

Hoci to na prvý pohľad vyzerá ako zbytočná formalita, ak má mať snaha o systematické riešenie KIB (ktorá pravdepodobne povedie aj k rozsiahlym zmenám v organizácii) nádej na úspech, musí vedenie organizácie jednoznačne deklarovať podporu KIB a vytvárať podmienky pre úspešný priebeh celého bezpečnostného procesu. Bez toho, aby boli zamestnanci presvedčení, že vedenie organizácie považuje KIB za úlohu s vysokou prioritou, nebudú jej, najmä v prípadoch ak im bude komplikovať život, venovať potrebnú pozornosť. Vedenie organizácie sotva bude mať čas a potrebné znalosti na tvorbu bezpečnostnej stratégie a písanie bezpečnostnej politiky. Po vyjadrení podpory KIB preto vedenie musí vytvoriť[9] pracovnú skupinu dostatočne kvalifikovaných a kompetentných ľudí, ktorí na základe zadania vedenia pripravia stratégiu KIB a napíšu bezpečnostnú politiku organizácie. Bezpečnostnú politiku organizácie vedenie organizácie najprv schváli[10] a potom vydáva vo forme interného záväzného dokumentu. Úlohou bezpečnostnej politiky je povedať každému zamestnancovi organizácie čo môže, čo nesmie, čo musí a za čo je zodpovedný pri práci s IKT. Bezpečnostná politika by mala byť preto napísaná tak, aby jej tí, ktorých sa týka, rozumeli a musí byť dostupná všetkým, od ktorých sa očakáva, že ju budú musieť dodržiavať, teda minimálne zamestnancom príslušnej organizácie a v primeranej miere aj zamestnancom tretích strán, ktorí s IKT organizácie nejakým spôsobom prichádzajú do kontaktu. Vedenie organizácie v dokumente Bezpečnostná politika

a) deklaruje dôležitosť KIB pre organizáciu, podporu vedenia organizácie pri zaisťovaní potrebnej úrovne KIB v organizácii a pripravenosť vytvoriť pre to podmienky;

b) definuje, na čo sa Bezpečnostná politika vzťahuje (oblasť pôsobnosti, (scope) Bezpečnostnej politiky), hlavné aktíva, hlavné bezpečnostné ciele organizácie v KIB a úroveň KIB, ktorú v organizácii považuje za primeranú,

c) stanoví zodpovednosť zamestnancov organizácie za presadzovanie a dodržiavanie Bezpečnostnej politiky (a dokumentov na ňu nadväzujúcich),

[6] manažmentu IB podľa noriem ISO/IEC 27001 a 27002, zohľadňujúceho aj legislatívne požiadavky na kybernetickú bezpečnosť

[7] z pedagogického hľadiska

[8] termín je prevzatý z BSI Štandardu [1] a označuje aktivity smerujúce k dosiahnutiu a trvalému udržaniu potrebnej úrovne KIB. V podstate zodpovedá 2. významu pojmu KIB, ako sme ju definovali v základných pojmoch. V materiáloch NIST sa ako synonymum pojmu bezpečnostný proces používa pojem bezpečnostný program.

[9] už v tejto fáze môže vedenie organizácie menovať manažéra KIB organizácie a poveriť ho aj organizačným zabezpečením prípravy bezpečnostnej stratégie. Samotná pracovná skupina by mala okrem manažéra KIB a informatikov obsahovať aj zástupcov organizačných útvarov, ktoré sú pre IB relevantné: personálne oddelenie, správa budov, právne oddelenie, oddelenie kontroly, príp. ďalších

[10] predtým ju aj opakovane môže vrátiť pracovnej skupine na dopracovanie

d) uvedie štruktúru bezpečnostných dokumentov nadväzujúcich na danú Bezpečnostnú politiku a ich obsah (špeciálne bezpečnostné politiky, alebo bezpečnostné štandardy, bezpečnostné praktiky—aké oblasti pokrývajú a akou formou budú vydané)

e) definuje na základe čoho sa bude informácia v organizácii klasifikovať[11],

f) definuje spôsob analýzy rizík (kvantitatívna/kvalitatívna) a hranicu akceptovateľného rizika v závislosti od úrovne IB, ktorú v organizácii považuje za primeranú,

g) stanoví

i zásady pre monitoring, kontrolu a audit informačných a komunikačných systémov organizácie

ii zásady riešenia bezpečnostných incidentov,

iii stratégiu pre zaistenie kontinuity činnosti IKS organizácie,

iv zásady pre správu bezpečnostnej politiky (ako často sa budú robiť pravidelné a z akých dôvodov mimoriadne revízie bezpečnostnej politiky).

Obsah bezpečnostnej politiky podľa ISO normy [6] je uvedený v prílohe 3.12.4.

Zhrnutie.

Vedenie organizácie zodpovedá o.i. aj za úroveň KIB v organizácii. Výnos MF SR o štandardoch pre ISVS stanovuje povinnosť zaviesť v organizáciách, ktoré majú ISVS, systém manažmentu KIB (ISMS). Vedenie organizácie vytvorí pracovnú skupinu, ktorá napíše bezpečnostnú politiku organizácie. Táto politika obsahuje stratégiu organizácie v KIB, stanovuje základné ciele KIB a je základom pre KIB v organizácii aj pre jej ISMS. Bezpečnostnú politiku vedenie vydá ako dokument, záväzný pre všetkých zamestnancov organizácie, externých pracovníkov a pracovníkov tretích strán, ktorí majú vplyv na IKT organizácie.

3.3 Riadenie KIB v organizácii

Bezpečnostná politika vytvára len rámec pre KIB v organizácii, ale nezaoberá sa spôsobmi ako dosiahnuť ciele, ktoré stanovila. Ak bezpečnostná politika nemá ostať len deklaráciou, na splnenie ňou definovaných úloh je potrebné vytvoriť primerané podmienky (personálne, organizačné, finančné a i.) zapojiť do jej realizácie zamestnancov organizácie, podrobne analyzovať bezpečnostné potreby organizácie a rozpracovať všeobecné ustanovenia bezpečnostnej politiky do konzistentného systému opatrení[12]. Na to, aby mal kto realizovať bezpečnostnú politiku, je v organizácii potrebné definovať bezpečnostné roly, stanoviť pre jednotlivé roly úlohy a zaradiť do nich vhodných ľudí. V informačne vyspelých krajinách vo väčších organizáciách rozlišujú desiatky špeciálnych bezpečnostných rolí (pozri napr. katalóg rolí v materiáli NIST [9]), v našich podmienkach budeme počet bezpečnostných rolí minimalizovať. Každá organizácia by však mala mať výkonného človeka, manažéra KIB, zodpovedného za riadenie KIB v organizácii. Manažér KIB plní podľa [1] nasledujúce úlohy:

[11] pozri časť Klasifikácia informácie a systémov

[12] postupnosť krokov pri implementácii bezpečnostnej politiky v organizácii nemusí byť totožná s poradí, v akom sú popisované v tejto práci

a) manažuje bezpečnostný proces a pracuje na úlohách, ktoré s ním súvisia,

b) pomáha vedeniu organizácie pri tvorbe (a správe) bezpečnostnej politiky,

c) koordinuje rozpracovanie bezpečnostnej politiky, čiastkových koncepcií, politík, návodov, pravidiel a metodických materiálov,

d) iniciuje a monitoruje implementáciu bezpečnostných opatrení,

e) vypracováva pre vedenie organizácie prehľady stavu KIB v organizácii,

f) koordinuje v organizácii projekty súvisiace s informačnou bezpečnosťou,

g) vyšetruje bezpečnostné incidenty, ku ktorým došlo v organizácii,

h) iniciuje a koordinuje vzdelávacie aktivity zamerané na zvýšenie bezpečnostného povedomia, znalostí a zručností KIB v organizácii.

Manažér KIB by mal byť zapojený aj do nových IKT projektov organizácie, aby mohol presadzovať zohľadňovanie bezpečnostných požiadaviek hneď od začiatku projektu (napr. vytvárania alebo obstarávania nového IS). Manažérom KIB nemôže byť hocikto. Aby dokázal úspešne plniť stanovené úlohy, mal by poznať organizáciu, jej informačnú a komunikačnú infraštruktúru, byť schopný pracovať v tíme a viesť tím, komunikovať s vedením organizácie, zamestnancami, predstaviteľmi a zamestnancami tretích strán, mať skúsenosti s manažmentom projektov a, samozrejme, mal by mať potrebné vedomosti z KIB, vrátane relevantných noriem a právnych predpisov. Funkcia manažéra KIB by sa nemala spájať s inými funkciami[13], pretože by

- mohlo dochádzať ku konfliktu záujmov (napr. informatika a manažéra KIB) a
- nemusel mať na plnenie úloh v KIB dosť času.

Manažér KIB je predovšetkým výkonná funkcia, ale niektoré výstupy jeho práce (koncepčné materiály KIB, prehľady stavu KIB v organizácii a najmä navrhované opatrenia) sa musia prerokovať vo vedení organizácie a po prípadných úpravách a schválení presadzovať z úrovne vedenia organizácie a na to kompetencie manažéra KIB nestačia. Preto by niektorý z členov vedenia organizácie mal explicitne zodpovedať za KIB v organizácii[14].

Rozsah úloh v KIB určite presiahne fyzické kapacity manažéra KIB. Podľa veľkosti, potrieb a možností organizácie bude do plnenia úloh KIB potrebné zapojiť aj ďalších zamestnancov; jedných na riešenie koncepčných, kontrolných a koordinačných úloh na úrovni celej organizácie (tím pre manažment KIB alebo bezpečnostné fórum podľa ISO normy [7]) a ďalších na praktické činnosti potrebné na zaisťovanie IB v organizačných útvaroch, systémoch, resp. projektoch organizácie. Zrejme len málo organizácií si bude môcť dovoliť vytvoriť tím pre manažment KIB zo špecializovaných odborníkov, ktorí sa riešeniu KIB v organizácii budú venovať na plný úväzok. Realistickejším riešením je nájdenie vhodných kandidátov spomedzi zamestnancov organizácie a rozšírenie ich pracovnej náplne o KIB, prípadne ich uvoľnenie od iných v povinností na určitú

[13] v malých organizáciách sa tomu pravdepodobne nedá vyhnúť, ale manažérovi KIB je možné prideľovať úlohy, pri plnení ktorých nenastáva konflikt záujmov

[14] tomuto vedúcemu zamestnancovi, sponzorovi KIB, by podliehal manažér KIB

dobu v prípade, keď organizácia potrebuje riešiť akútny problém (napr. vypracovanie Bezpečnostnej stratégie). Norma predpokladá vytvorenie koncepčno-riadiaco-koordinačného útvaru, bezpečnostného fóra. Jeho zloženie by mohlo byť podobné zloženiu pracovnej skupiny, ktorá pripravila Bezpečnostnú politiku organizácie. Okrem tohto virtuálneho manažérskeho tímu, bude organizácia pravdepodobne potrebovať špecializovaných manažérov KIB, ktorých úlohou je riadenie KIB v organizačných zložkách (veľkej) organizácie, zabezpečovanie primeraného riešenia bezpečnostných požiadaviek vo významných projektoch a riešenie bezpečnostných problémov dôležitých systémov. Tieto funkcie bude v organizácii tiež pravdepodobne možné riešiť rozšírením pracovných náplní existujúcich zamestnancov.

Zhrnutie.

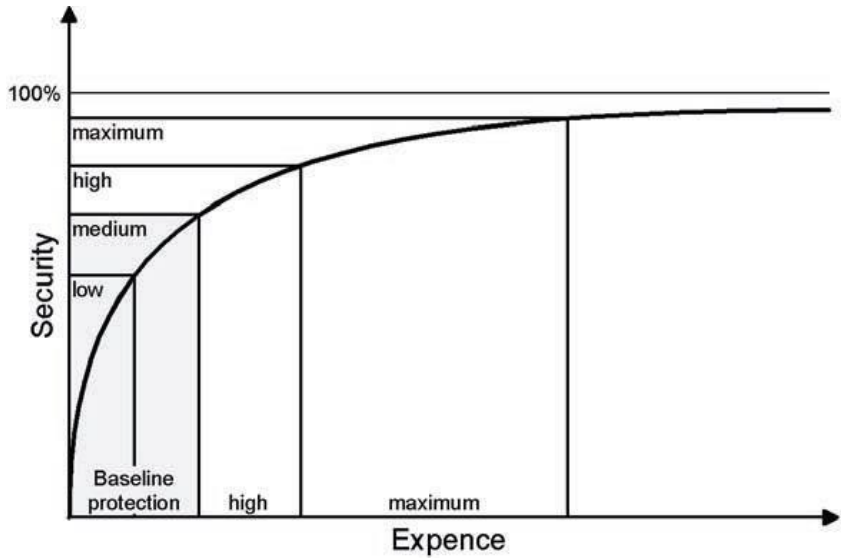
Bezpečnostnú politiku bude musieť niekto v organizácii zaviesť do života. Vedenie poverí niektorého člena vedenia zodpovednosťou za KIB (prepojenie vedenia a výkonnej zložky KIB) a ustanoví manažéra KIB ako výkonného zamestnanca pre oblasť KIB. Podľa veľkosti a charakteru organizácie ustanoví z riadiacich zamestnancov organizácie tím manažéra KIB (bezpečnostné fórum), ktorý bude riešiť koncepčné otázky KIB a lokálnych manažérov KIB na čiastočné úväzky, ktorí budú pomáhať manažérovi KIB a používateľom IKT riešiť bezpečnostné problémy v organizačných zložkách, resp. veľkých systémoch organizácie.

3.4 Finančné zdroje na KIB

Pri implementácii bezpečnostnej politiky musí organizácia rátať nielen s dostatočnými finančnými, ale aj s ľudskými a časovými zdrojmi. Je jednoduchšie odhadnúť na čo budú financie potrebné, ako ich výšku. Najmä zdôvodnenie výšky finančných nákladov spôsobuje problémy, pretože ak v organizácii nie je dostatočná úroveň KIB, tak skôr či neskôr dôjde k bezpečnostným incidentom, ktoré budú znamenať pre organizáciu nejakú stratu[15]; ale keď organizácia vynakladá dostatočné prostriedky na riešenie KIB, k incidentom nedochádza. A potom paradoxne vzniká otázka, či bolo na KIB potrebné vynaložiť a najmä v budúcnosti vynakladať také veľké prostriedky. Úroveň KIB v organizácii sa dá ťažko nejako kvantitatívne vyjadriť a ešte ťažšie sa predpovedá, či v budúcnosti organizácia bude cieľom nejakého útoku, alebo či bude postihnutá prírodnou katastrofou, zhoršenými spoločenskými podmienkami a aké budú mať tieto nepriaznivé okolnosti na ňu dopad.

Hoci sa KIB nedá exaktne hodnotiť pomocou štandardných ekonomických kritérií, dlhodobé sledovanie vzťahu medzi investíciami do KIB a úrovňou KIB (meranou frekvenciou výskytu a dopadom bezpečnostných incidentov) priniesli zaujímavé zistenia. Ukazuje sa, že (za predpokladu, že sú prostriedky na KIB optimálne použité) už s relatívne malými prostriedkami sa dá dosiahnuť základná úroveň KIB, ktorá predstavuje veľký pokrok oproti východiskovému stavu (bez riešenia KIB), ale potom sa zlepšovanie úrovne IB spomaľuje, až nakoniec dosiahne maximum, ktoré sa ani ďalšími investíciami do KIB už viac nedá zlepšiť, pozri graf na obr. 3.1., prevzatý z BSI štandardu [1]. Tento vzťah medzi nákladmi a úrovňou KIB treba zohľadňovať pri plánovaní prostriedkov pre KIB už pri tvorbe bezpečnostnej politiky organizácie, nakoľko nemá zmysel stavať si na začiatku príliš ambiciózne ciele, na dosiahnutie ktorých budú v realizačnej fáze chýbať prostriedky.

[15] výška strát spôsobených bezpečnostnými incidentmi môže slúžiť ako orientačná hodnota pre výšku investícií do KIB



Obr. 3.1: Vzťah medzi nákladmi na IB a úrovňou IB. [1]

Obmedzené zdroje na IB nemusia nutne znamenať, že vážne bezpečnostné problémy ostanú v organizácii nevyriešené. Mnohé bezpečnostné problémy majú našťastie viacero rôznych riešení a často je možné dosiahnuť väčší pokrok jednoduchšími organizačnými opatreniami, ako (napr.) zavedením nejakého nákladného technického riešenia. Tak napríklad prvým predpokladom dosiahnutia požadovanej úrovne KIB je normálne fungovanie IKT v organizácii. Ak má organizácia nevyhovujúcu štruktúru IKT a/alebo nedostatočne kvalifikovanú alebo preťaženú obsluhu IKT, tak kým nebudú vyriešené základné problémy prevádzky IKT, nemá zmysel prijímať ďalšie bezpečnostné opatrenia na riešenie bezpečnostných problémov vyššej úrovne [16].

Organizácia môže niektoré úlohy v KIB riešiť vlastnými pracovníkmi, ale pravdepodobne nebude mať dostatočné kapacity na to, aby riešila všetky bezpečnostné problémy vlastnými silami. Pri plánovaní prostriedkov na KIB bude potrebné zohľadniť aj prostriedky na zabezpečenie externých špecialistov, prípadne na outsourcing niektorých služieb (napr. PKI, nezávislý bezpečnostný audit a i.). Prostriedky je potrebné plánovať aj na činnosť manažéra KIB a zamestnancov, ktorí sa na plnení úloh v KIB podieľajú a na samotné monitorovanie KIB v organizácii. Tieto náklady sa organizácii môžu vrátiť, pretože napr. nezávislá kontrola prijatých opatrení môže odhaliť prípady, keď je cena opatrení príliš vysoká v porovnaní s hodnotou rizika (a cenou aktíva, ktoré majú chrániť), resp. aj v opačnom prípade, keď už opatrenie nie je dostatočne účinné a vďaka tomu je riziko príslušnej hrozby príliš vysoké a pre organizáciu neprijateľné.

Manažment KIB nie je izolovaný od ostatných činností organizácie. Po vyriešení počiatočných problémov (vypracovanie a implementácia bezpečnostnej politiky, zaradenie ľudí do bezpečnostných rôl, analýze rizík a implementácii bezpečnostných opatrení atď.), ktoré si vyžadujú vyššie počiatočné investície, by sa financovanie kybernetickej a informačnej bezpečnosti malo dostať do ustálenej podoby. Manažér KIB (v spolupráci s bezpečnostným fórom, ak v organizácii existuje) bude každoročne vypracúvať správu o stave KIB v organizácii a plán práce

[16] k výberu opatrení sa dostaneme po analýze rizík, v časti 3.12.1.

na ďalší rok. Tieto dokumenty predloží sponzor KIB do rokovania vedenia spolu s rozpočtom nákladov na KIB na ďalší rok. Keďže je veľmi pravdepodobné, že požadované prostrieky budú presahovať možnosti organizácie, návrh rozpočtu na KIB by mal byť štrukturovaný:

- prostriedky potrebné na udržanie/dosiahnutie minimálnej úrovne KIB,
- prostriedky potrebné na riešenie vleklých bezpečnostných problémov, ktoré organizácia dlhodobo tlačí pred sebou,
- rezerva pre mimoriadne situácie.

Riešenie KIB v organizácii si vyžaduje aspoň prostriedky na zachovanie minimálnej úrovne KIB, neposkytnutie prostriedov na riešenie vleklých problémov môže spôsobiť, že sa z nich stanú akútne bezpečnostné problémy a mimoriadne problémy bude možno potrebné riešiť ad-hoc.

Zhrnutie.

Na implementáciu bezpečnostnej politiky bude potrebné rátať s finančnými, materiálnymi a personálnymi zdrojmi. Úroveň KIB ani návratnosť investícií do KIB sa síce nedá presne merať, ale empirické skúsenosti ukazujú, že už s relatívne malými nákladmi sa dá dosiahnuť výrazné zlepšenie (obr. 3.1.). Dostupné zdroje je potrebné zohľadniť už pri tvorbe bezpečnostnej politiky a je potrebné rátať s tým, že nie všetky úlohy bude organizácia schopná riešiť sama. Na druhej strane, niektoré bezpečnostné opatrenia môžu odhaliť nedostatky, ktorých odstránením sa zvýši tak efektívnosť činnosti ako aj úroveň KIB organizácie. Plánovanie zdrojov na KIB by sa malo odvíjať od úloh, ktoré organizácia v KIB potrebuje riešiť a zosúladené so štandardnými procesmi plánovania činnosti organizácie (správa o činnosti, plán činnosti a rozpočet na ďalší rok).

3.5 Analýza rizík

Bezpečnostná politika stanovila hlavné ciele pre KIB organizácie, hranicu akceptovateľného rizika a spôsob analýzy rizík. Organizácia si teraz potrebuje spraviť podrobnejší prehľad o tom, čo konkrétne, pred čím a na akej úrovni potrebuje chrániť. Odpovede na tieto otázky dáva analýza rizík. Ak na to organizácia má dostatok vlastných kvalifikovaných ľudí, môže si ju robiť sama, v opačnom prípade na ňu využije (aj) externých odborníkov. Keďže organizácia potrebuje rozpracovať svoju bezpečnostnú stratégiu (Bezpečnostnú politiku), predpokladáme, že rozsah (scope) analýzy rizík bude totožný s oblasťou pôsobnosti Bezpečnostnej politiky. (V budúcnosti môže organizácia spraviť alebo nechať si spraviť analýzu rizík pre dôležitý systém, časť organizácie, resp. tematicky zameranú na nejaký druh údajov, napr. osobné údaje). V ďalšom budeme predpokladať, že manažér KIB zostavil na analýzu rizík pracovnú skupinu zloženú z kompetentných pracovníkov, schopných splniť zadanú úlohu.

3.5.1 Zber podkladov

Pracovná skupina, ktorá je poverená spraviť analýzu rizík, určí

1. všetky relevantné aktíva organizácie,

2. všetky relevantné hrozby[17] voči aktívam zo zoznamu vytvoreného v prvom kroku,
3. všetky bezpečnostné požiadavky vyplývajúce z právnych predpisov, vnútorných predpisov, zmlúv a podobných dokumentov organizácie,
4. všetky zraniteľnosti aktív[18] určených v prvom kroku,
5. už existujúce bezpečnostné opatrenia.

Pri tvorbe zoznamu aktív pracovná skupina zároveň zistí, kto je za dané aktívum zodpovedný (tzv. „vlastník aktíva“) a čo všetko na dané aktívum má nejaký vplyv (bezpečnostné prostredie aktíva). Hrozby voči aktívam doplní o hrozby voči bezpečnostnému prostrediu jednotlivých aktív, pretože tieto aktíva môžu byť poškodené aj nepriamo, narušením podmienok v ktorých fungujú. Právne predpisy, zmluvy, normy stanovujú bezpečnostné požiadavky na aktíva, ktorých nedodržanie môže viesť k bezpečnostným incidentom, alebo môže mať právne dôsledky (sankcie). Identifikácia existujúcich opatrení je dôležitá hneď z dvoch dôvodov—účinné opatrenie môže znižovať pravdepodobnosť naplnenia hrozby a jeho ignorovanie by mohlo viesť k chybnému hodnoteniu rizík. Po vyhodnotení rizík bude organizácia prijímať opatrenia a je možné, že niektoré z existujúcich opatrení bude potrebné nahradiť účinnejšími. V takom prípade nemá zmysel udržiavať duplicitné opatrenia.

3.5.2 Ohodnotenie rizík/výpočet hodnoty rizika

Po zozbieraní podkladov pracovná skupina vypočíta hodnoty jednotlivých identifikovaných rizík. Hodnota rizika sa najčastejšie vyjadruje ako stredná hodnota dopadu hrozby, t.j.

$$\text{hodnota rizika} = \text{pravdepodobnosť}^{19} * \text{dopad hrozby},$$

alebo na logaritmickej škále[20] :

$$\text{hodnota rizika} = \text{pravdepodobnosť} + \text{dopad hrozby},$$

Pri výpočte hodnoty rizika sa využívajú dva základné prístupy; kvantitatívny a kvalitatívny. Pri kvantitatívnom prístupe je hodnota rizika aj dopad vyjadrené číselne (dopad napríklad výškou finančnej straty, pravdepodobnosť číslom z intervalu $\langle 0, 1\rangle$), pri kvalitatívnom prístupe sa pravdepodobnosť, dopad aj hodnoty samotného rizika kategorizujú a vyjadrujú slovne. Hoci kvantitatívna metóda vyzerá na prvý pohľad exaktnejšie a objektívnejšie, používa sa len zriedka, pretože je problém presne určiť tak hodnotu dopadu ako aj pravdepodobnosti nejakej udalosti[21]. V ďalšom preto rozoberieme kvalitatívnu metódu odhadu (hodnôt) rizík.

[17] zoznam hrozieb je uvedený v prílohe Katalóg elementárnych hrozieb

[18] zoznam zraniteľností je uvedený v prílohe Zoznam zraniteľností

[19] rozumie sa pravdepodobnmosť naplnenia hrozby voči aktívu a podobne dopad danej hrozby na aktívum a/alebo organizáciu

[20] pripomíname, že $\log x.y = \log x + \log y$

[21] ako vyjadriť pravdepodobnosť udalosti, ktorá v organizácii ešte nikdy predtým nenastala? Je možné považovať ju za nulovú a hrozbou sa nezaoberať? Alebo ako sa dá exaktne vyjadriť hodnota nehmotných aktív, ako je know-how, dobré meno, alebo zdravie a spokojnosť zamestnancov?

Organizácia by mala mať vytvorené kritériá pre hodnotenie dopadu hrozby, postavené na závažnosti škôd a výške materiálnych strát, ktoré v dôsledku naplnenia hrozieb utrpí, zohľadňujúce podľa ISO normy [7]:

- úroveň klasifikácie postihnutých informačných aktív,
- závažnosť narušenie informačnej bezpečnosti (napr. strata dôvernosti, integrity a dostupnosti),
- narušenie operácií/činnosti (organizácie, alebo tretích strán),
- finančné straty,
- narušenie plánov a nesplnené termíny,
- poškodenie reputácie,
- porušenie právnych, zmluvných a regulačných požiadaviek.

Tento zoznam je potrebné doplniť o zdravie a život ľudí[22], lebo strata zdravia a ľudského života je z etického hľadiska nenahraditeľná, strata kvalifikovaného zamestnanca môže byť ťažko nahraditeľná a zranenie alebo smrť človeka môže mať negatívne dopady na organizáciu (reputácia, právne dôsledky).

Hrozby môžu mať rôzne formy dopadu (napr. záplava: utopenie človeka, poškodenie budovy, poškodenie zariadení, počítačov, prerušenie napájania, prerušenie komunikačných liniek, znemožnenie prístupu zamestnancov do budovy, znemožnenie príchodu zamestnanca do práce, znečistenie okolitého prostredia, poškodenie cestných komunikácií a pod.). Vyhneme sa rozoberaniu možných foriem dopadu a využijeme americký federálny štandard FIPS 199 [4], ktorý abstrahuje od zbytočných podrobností a vyjadruje rôzne formy dopadu hrozieb pomocou narušenia základných bezpečnostných požiadaviek na ochranu informácie (dôvernosť, integrita a dostupnosť) a definuje tri kvalitatívne úrovne dopadu:

nízky, ak strata dôvernosti, integrity alebo dostupnosti[23] má obmedzený negatívny vplyv na činnosť organizácie, jej aktíva alebo osoby[24]. Obmedzený negatívny dopad znamená, že strata dôvernosti, integrity alebo dostupnosti môže spôsobiť

- zníženie schopnosti organizácie v takej miere a na takú dobu, že organizácia je síce schopná plniť svoje primárne funkcie ale menej efektívne,
- málo závažné poškodenie aktív organizácie,
- malé finančné straty,
- malú ujmu osobám.

[22] sú relevantné najmä pre systémy v ktorých sa spracovávajú zdravotné informácie (nesprávna liečba v dôsledku narušenia integrity alebo dostupnosti údajov), riadiacich systémoch (napr. doprava, elektrárne, výrobné linky).

[23] tu aj v ďalších prípadoch sa rozumie „v dôsledku naplnenia hrozby“

[24] napr. narušenie súkromia

stredný, ak strata dôvernosti, integrity alebo dostupnosti má závažný negatívny vplyv na činnosť organizácie, jej aktíva alebo osoby. Závažný negatívny vplyv znamená, že strata dôvernosti, integrity alebo dostupnosti môže spôsobiť

- zníženie schopnosti organizácie v takej miere a na takú dobu, že organizácia je síce schopná plniť svoje primárne funkcie ale efektívnosť jej činnosti je výrazne redukovaná,
- značné poškodenie aktív organizácie,
- značné finančné straty,
- významnú ujmu osobám (ale nie závažné zranenia alebo straty na životoch).

vysoký (katastrofický) ak strata dôvernosti, integrity alebo dostupnosti má veľmi závažný až katastrofický negatívny vplyv na činnosť organizácie, jej aktíva alebo osoby. Veľmi závažný negatívny vplyv znamená, že strata dôvernosti, integrity alebo dostupnosti môže spôsobiť

- také škody, že organizácia nie je schopná vykonávať niektoré zo svojich primárnych funkcií,
- rozsiahle poškodenie aktív organizácie,
- veľké finančné straty, ktoré organizácia nie je schopná kompenzovať z vlastných zdrojov,
- veľkú až katastrofickú ujmu osobám (vrátane život ohrozujúcich zranení až smrti osôb).

V praxi je jednoduchšie stanoviť krajné hodnoty dopadu—vysoká hodnota dopadu je taká, ktorá by znemožnila plnenie základných úloh organizácie, ba až ohrozila jej existenciu; nízka hodnota dopadu je taká, že organizácia zaregistruje bezpečnostný incident, ten však nemá vplyv na plnenie základných úloh organizácie a dá sa riešiť bežnými prostriedkami (napr. preinštalovanie softvéru osobného počítača). Dopad vyšší ako nízky a nižší ako vysoký budeme chápať ako dopad strednej úrovne.

Druhým činiteľom ovplyvňujúcim výšku rizika je pravdepodobnosť naplnenia hrozby. Na hodnotu pravdepodobnosti (naplnenia hrozby voči konkrétnemu aktívu) vplýva o.i. existencia zraniteľností, prijaté opatrenia, prípadne potrebný útočný potenciál. Na ohodnotenie pravdepodobnosti budeme používať 4 stupňovú škálu a riziko budeme vyjadrovať slovne (nulové, nízke, stredné, vysoké), alebo sa na vyjadrenie jeho hodnoty použijeme číselnú škálu. Pravdepodobnosti, ktoré sú uvedené v tabuľke 3.1 je potrebné brať ako ilustratívny príklad, organizácia si môže sama určiť, čo považuje za vysokú, strednú a nízku úroveň pravdepodobnosti.

Metóda odhadovania rizika pre štvorúrovňovú škálu pravdepodobností a trojúrovňovú škálu dopadu je uvedená v tabuľke

Iné tabuľky pre odhad rizík sú uvedené v norme [7].

označenie	pomenovanie	poznámka
0	nulová	udalosť nenastane
1	nízka	udalosť nenastala, alebo sa vyskytla raz za niekoľko rokov
2	stredná	raz za rok
3	vysoká	niekoľkokrát mesačne/týždenne

Tabuľka 3.1: Kvalitatívne vyjadrenie pravdepodobnosti udalosti

3.5.3 Vyhodnotenie rizík

Odhad rizík ešte nemusí zohľadníť všetky okolnosti, ktoré sú pre určenie reálnej hodnoty rizika pre organizáciu podstatné. Na zoznam rizík sa musia pozrieť ľudia, ktorí vedia posúdiť, čo by narušenie konkrétneho aktíva pre organizáciu znamenalo, teda vedúci pracovníci a najmä vlastníci aktív. Títo na základe kritérií na ohodnotenie rizík (risk evaluation criteria), scenárov naplnenia hrozieb vyhodnotia riziká a pracovná skupina s ich pomocou vytvorí zoznam rizík usporiadaných podľa závažnosti. Tento zoznam obsahuje dve skupiny rizík: tie, ktorých hodnota presahuje hranicu akceptovateľného rizika a tie ostatné.

3.5.4 Ošetrenie rizík

Organizácia má zoznam rizík usporiadaných podľa závažnosti a teraz je potrebné rozhodnúť, čo s nimi bude robiť. Má štyri možnosti [7]:

1. **Redukcia rizika**. V tomto prípade organizácia prijíma opatrenia (technické, organizačné, personálne a iné) zamerané na zníženie pravdepodobnosti naplnenia a/alebo dôsledkov hrozby tak, aby sa hodnota výsledného rizika dostala pod úroveň akceptovateľného rizika. Rozsiahly zoznam opatrení obsahuje napríklad ISO norma [6].

2. **Zachovanie rizika** (risk retention): ak je úroveň rizika nižšia ako úroveň akceptovateľného rizika, organizácia nemusí prijímať žiadne opatrenia.

3. **Vyhnutie sa riziku**. Prichádza do úvahy vtedy, keď by opatrenia na redukciu rizika boli príliš nákladné, ale hodnota rizika je vyššia ako úroveň akceptovateľného rizika. Organizácia zmení podmienky, ktoré viedli k neprijateľne vysokému riziku, napríklad

dopad → pravdepodobnosť ↓	nízky	stredný	vysoký
nulová	nulové	nulové	nulové
nízka	nízke	nízke	stredné
stredná	nízke	stredné	vysoké
vysoká	stredné	vysoké	vysoké

Tabuľka 3.2: Kvalitatívne vyjadrenie hodnoty rizika

použitím iného riešenia (vykonávanie činnosti iným spôsobom, prenesenie činností do menej nebezpečného prostredia a pod.)

4. **Prenesenie rizika**. Organizácia môže preniesť riziko na iný subjekt[25] , ktorý ho dokáže efektívnejšie riešiť. (Príkladmi prenesenia rizika sú napr. zmluvy s dodávateľom o skrátenej dobe servisného zásahu, outsourcing problematických činností, poistenie).

Definitívne rozhodnutie o tom, čo sa bude robiť s identifikovanými rizikami musí prijať vedenie organizácie. Pracovná skupina nemá dostatočné kompetencie na presadenie navrhovaných opatrení a nemôže zastupovať organizáciu v rokovaniach s partnermi. Pre rokovanie vedenia pripraví dva dokumenty: Zoznam vyhodnotených rizík so zdôvodneniami k jednotlivým rizikám a Plán ošetrenia rizík. Plán obsahuje úplný zoznam identifikovaných rizík s návrhom, čo je potrebné s jednotlivými rizikami robiť. Ak vedenie organizácie schváli Plán ošetrenia rizík, tým vyjadrí súhlas s implementáciou navrhovaných opatrení a zároveň akceptuje zostatkové riziká.

3.6 Bezpečnostné opatrenia

> *It is estimated that ninety-nine per cent of all reported intrusions result through exploitation of known vulnerabilities or configuration errors, for which safeguards and countermeasures were available (NIST SP 800-53)*

Bezpečnostné opatrenia (safeguards, security controls, security measures) sú riešenia, ktorých zavedením (implementáciou) sa eliminuje riziko alebo aspoň zníži jeho úroveň (hodnota). Podľa prostriedkov, ktoré používajú sa opatrenia delia na [11]

a) technické,

b) organizačné a

c) prevádzkové.

Podľa toho, na ktorú fázu potenciálneho bezpečnostného incidentu spôsobeného naplnením hrozby pôsobia, delíme opatrenia na

a) preventívne,

b) detekčné a

c) korekčné.

[25] pripomíname, že prenesením rizika sa organizácia spravidla nezbavuje zodpovednosti za prípadný dopad hrozby, pretože klienti budú považovať problémy spôsobené prípadným bezpečnostným incidentom za chybu organizácie

Technické opatrenia sú založené na bezpečnostných funkciách realizovaných pomocou hardvérových komponentov, firmvéru a softvéru. Organizačné opatrenia sa realizujú pomocou politík, pravidiel, záväzných postupov, stanovení zodpovednosti, školení zamestnancov, zmlúv. Prevádzkové opatrenia zahŕňajú fyzickú ochranu IKT, podpornej infraštruktúry, ochranu prístupu, detekcie pohybu, detekcie požiaru a pod. Hoci sa opatrenia kategorizujú, pri návrhu opatrení na zmiernenie rizika sa kombinujú opatrenia všetkých troch kategórií.

Úlohou **preventívnych opatrení** je zamedziť vzniku bezpečnostného incidentu, alebo aspoň výrazne znížiť pravdepodobnosť naplnenia hrozby. Preventívne opatrenia sú zamerané buď na odstránenie zraniteľnosti, ktorú hrozba využíva, alebo v prípade, ak je nositeľom hrozby človek, na zníženie jeho útočného potenciálu:

- motivácie: napr. zvýšenie pravdepodobnosti jeho odhalenia a potrestania (odstrašenie),
- príležitosť: na prekonanie nových opatrení potrebuje podstatne väčšie zdroje,
- znalosti: odstránenie známych zraniteľností, ktoré umožňovali útoky.

Detekčné opatrenia predstavujú druhú úroveň ochrany aktív. Ich cieľom je odhaliť včas začínajúci bezpečnostný incident, signalizovať ho napr. operátorovi a zaznamenať údaje potrebné na analýzu vzniku a priebehu bezpečnostného incidentu. Príkladmi detekčných opatrení sú zariadenia na detekciu pohybu, dymu, IDS (intrusion detection systems, systémy na detekciu prieniku), monitorovacie programy, systémy na vytváranie záznamov auditu a pod. **Korekčné opatrenia** sú zamerané na zabezpečenie kontinuity činnosti: v prípade bezpečnostných incidentov na ich riešenie a na návrat aktíva do normálneho stavu. Príklady opatrení sú uvedené nižšie.

Posledným krokom pred výberom opatrení na ošetrenie neakceptovateľných rizík je analýza ekonomickej efektívnosti (cost/benefit) navrhovaných opatrení, ktorú pripravuje pracovná skupina. Vstupom pre analýzu ekonomickej efektívnosti je zoznam identifikovaných rizík. Ku každému riziku sú priradené možné opatrenia a analýza pozostáva z

a) určenia dopadu zavedenia nového alebo rozšírenia existujúceho opatrenia,

b) určenia dopadu toho, že sa nové opatrenie nezavedie alebo existujúce opatrenie nerozšíri,

c) odhadu nákladov na zavedenie nového alebo rozšírenia existujúceho opatrenia, napr.
   - kúpa technických zariadení a/alebo softvéru,
   - prípadné zníženie efektívnosti činnosti systému v dôsledku zavedenia opatrenia,
   - náklady spojené so zavedením dodatočných politík a procedúr,
   - náklady na personál potrebný na zavedenie nových opatrení (pracovný čas existujúcich zamestnancov, alebo náklady spojené s prijatím nových zamestnancov),
   - náklady na školenia zamestnancov,
   - náklady na údržbu;

d) porovnanie nákladov na zavedenie nového alebo rozšírenia existujúceho opatrenia a jeho prínosu vzhľadom na význam tých systémov a údajov pre organizáciu, ktorých ochrana sa daným opatrením zvýši (resp. u ktorých sa zníži úroveň rizika).

Záverečné rozhodnutie je na vedúcom zamestnancovi (alebo vedení) organizácie, ktorý musí posúdiť, či je v danom prípade riziko akceptovateľné alebo nie a či návrh na zavedenie nového opatrenia možno zamietnuť alebo nie. Pre rozhodovanie o zavedení nového opatrenia môžu pomôcť nasledujúce pravidlá

a) ak opatrenie redukuje riziko viac, než je potrebné, treba sa pozrieť, či neexistuje iné, lacnejšie riešenie,

b) ak je cena navrhovaného riešenia ako hodnota, o ktorú redukuje riziko, treba hľadať iné riešenie,

c) ako opatrenie neredukuje riziko dostatočne, treba sa pozrieť na ďalšie doplňujúce opatrenia alebo nejaké iné opatrenie,

d) ak navrhované opatrenie redukuje riziko dostatočne a je spomedzi možných opatrení najlacnejšie, treba ho použiť.

Zoznam opatrení[26], ktoré podľa [10] musí organizácia zaviesť na dosiahnutie základnej úrovne[27] bezpečnosti svojich IKT je uvedený v prílohe 3.12.1.

3.7 Spravovanie rizík

Organizácia zavedením nových alebo rozšírením existujúcich opatrení zmiernila riziká tým, že

a) odstránila niektoré zraniteľnosti aktív, čím sa zredukovala na nulu pravdepodobnosť naplnenia niektorých hrozieb, (preloženie serverov z prízemnej miestnosti na 2. poschodie odstránilo možnosť zaplavenia počítačov vodou z rozvodnenej rieky)

b) pridanie cieleného opatrenia znížilo kapacitu a motiváciu útočníka (zrušenie anonymného prístupu k systému, silná identifikácia a autentizácia používateľov, vytváranie záznamov auditu o činnosti v systéme)

c) znížil sa dopad negatívneho dopadu bezpečnostného incidentu na organizáciu (napr. zálohovaním údajov a možnosťou preniesť v krátkom čase činnosť z jedného systému na záložný systém).

Je veľmi pravdepodobné, že sa nepodarilo eliminovať všetky riziká. Riziká, ktoré ostali po prijatí nových a/alebo rozšírení existujúcich opatrení sa nazývajú *zostatkové* (*zvyškové*, alebo *reziduálne*) riziká, ktoré bude potrebné porovnať s hranicou akceptovateľného rizika. Ak je úroveň niektorého zostatkového rizika vyššia ako úroveň akceptovateľného rizika, organizácia má dve možnosti:

a) nájsť a implementovať vhodné opatrenia, ktoré by znížili úroveň „vysokých“ zostatkových rizík na úroveň akceptovateľného rizika,

[26] ide o vysokoúrovňové opatrenia, zoznam konkrétnych opatrení je uvedený napr. v ISO/IEC norme [6]
[27] základná úroveň neznamená nízku úroveň bezpečnosti, pozri Prílohu Klasifikácia informácie a systémov

b) prehodnotiť úroveň akceptovateľného rizika alebo podmienečne akceptovať „neriešiteľné“ riziko s povinnosťou monitorovať príslušné aktívum, aby sa včas zachytil začiatok prípadného bezpečnostného incidentu.

Dosiahnutie požadovanej úrovne KIB znížením rizík na akceptovateľnú úroveň nemusí mať dlhé trvanie. Podmienky, za ktorých organizácia robila analýzu rizík, sa neustále menia:

a) Mení sa samotná organizácia (organizačná štruktúra, technická infraštruktúra, zamestnanci, ich pracovné zaradenie, roly, vyvíja sa poslanie organizácie, mení sa citlivosť údajov a pod.). Tieto zmeny môžu spôsobiť, že sa menia aj predpoklady, z ktorých sa vychádzalo pri analýze rizík a teda závery analýzy rizík (najmä vyhodnotenie rizík) nemusia byť platné.

b) Menia sa technológie a v dôsledku toho sa objavujú nové zraniteľnosti, hrozby; staré opatrenia strácajú na účinnosti, resp. sú celkom neaktuálne, úroveň rizík sa môže meniť (zvyšovať).

Aby sa v dynamicky sa meniacom prostredí udržala požadovaná úroveň KIB v organizácii, organizácia musí priebežne monitorovať bezpečnostnú situáciu a v prípade veľkých zmien (organizačné zmeny, infraštruktúra, zmeny zákonov s veľkým dopadom na organizáciu[28] , veľké bezpečnostné incidenty a pod.) a v pravidelných časových intervaloch zopakovať analýzu rizík a aktualizovať prijaté opatrenia. Ak majú zmeny lokálny charakter (zavedenie nového systému), analýza rizík nemusí pokrývať celú organizáciu a môže sa zamerať len tie oblasti, ktorá boli zmenami dotknuté.

Zhrnutie. Po prijatí opatrení musí organizácia skontrolovať, či sa jej tým podarilo znížiť všetky riziká na prijateľnú mieru. Ak nie, musí hľadať iné riešenia. Ale ani uspokojivý stav nemusí trvať dlho a organizácia musí vyhodnocovať zmeny, ktoré môžu spôsobiť objavenie nových alebo nárast existujúcich rizík nad prijateľnú úroveň. Okrem analýz rizík vyvolaných veľkými zmenami odporúčame pravidelné posúdenie KIB, aby sa zamedzilo tomu, že časom nepozorovane vyprchala účinnosť prijatých opatrení.

3.8 Bezpečnostný audit

Systém opatrení, ktoré organizácia prijala po analýze rizík, nemusel splniť jej očakávania. Niektoré opatrenia mohli ostať len na papieri, iné mohli byť implementované len čiastočne, ďalšie stratili na účinnosti; problémy môžu byť aj v samotnom ISMS, nevyjasnených kompetenciách alebo chýbajúcich zdrojoch. Na odhaľovanie takýchto nedostatkov slúži audit. Audit vo všeobecnosti je nezávislá jednorazová kontrola, počas ktorej sa zisťuje súlad predmetu auditu s nejakým ideálnym stavom. V prípade bezpečnostného auditu organizácie budú predmetom auditu bezpečnostné opatrenia a činnosť ISMS. Audit opatrení ISMS je popísaný v norme ISO/IEC TR 27008 [8] z ktorej sme v tejto časti vychádzali.

Bezpečnostný audit sa v organizáciách vykonáva

[28] prijatie zákona o kybernetickej bezpečnosti, nariadení GDPR, eIDAS, novelizácia štandardov ISVS a pod.

a) v pravidelných časových intervaloch (napríklad každoročne). Cieľom pravidelného auditu je posúdiť, či nedošlo k zmenám, ktoré sa síce zatiaľ neprejavili, ale mohli znížiť účinnosť existujúcich opatrení a tým zvýšiť úroveň rizík. Pravidelný audit umožní včas odhaliť neúčinné opatrenia a dať podnet na nápravu. Závery auditu sú dôležitým podkladom pre pravidelné (výročné) hodnotenie stavu KIB v organizácii.

b) nepravidelne. Podnetom pre vykonanie mimoriadneho bezpečnostného auditu bývajú najčastejšie bezpečnostné incidenty (často sa opakujúce alebo s vážnymi dôsledkami pre organizáciu) ktoré naznačujú, že úroveň KIB v organizácii nie je dostatočná, alebo veľké zmeny, ktoré si vyžiadali prehodnotiť systém bezpečnostných opatrení. V takýchto prípadoch je úlohou bezpečnostného auditu posúdiť, či existujúce bezpečnostné opatrenia poskytujú požadovanú úroveň ochrany.

Špeciálnym prípadom auditu je tzv. certifikačný audit, ktorého úlohou je overiť, či je predmet auditu v súlade s nejakým štandardom (napr. či je ISMS organizácie v súlade s normou (ISO/IEC 27001). Certifikáciou sa budeme zaoberať v časti 3.10.

Iniciovanie a zdroje na audit. Povinnosť organizácie vykonávať pravidelne bezpečnostný audit je stanovená v bezpečnostnej politike[29] a audit by mal byť zaradený do plánu činnosti organizácie a mali by naň byť plánované prostriedky. Vykonanie mimoriadneho auditu bude iniciovať pravdepodobne manažér KIB, ktorý bude musieť požiadať vedenie o poskytnutie potrebných neplánovaných zdrojov. V ďalšom predpokladáme, že prípravu auditu a koordináciu súčinnosti audítorov a zamestnancov organizácie bude riadiť/vykonávať manažér KIB.

Príprava auditu. Manažér KIB zozbiera potrebné informácie o systémoch, ktoré sa majú posudzovať (technickú a prevádzkovú dokumentáciu, predchádzajúcu analýzu rizík, informácie o bezpečnostných incidentoch, plány auditu podobných systémov[30], výsledky predchádzajúcich auditov systémov organizácie, bezpečnostnú politiku, štandardy a praktiky pre relevantné systémy). Na základe predbežne zozbieraných informácií upresní rozsah a hĺbku auditu.

Výber audítorov. Na vykonanie auditu je potrebná odborná kvalifikácia, informačné zdroje a súčinnosť zamestnancov organizácie. Aby výsledky auditu neboli ovplyvnené záujmami audítorov, bezpečnostný audit nesmú vykonávať ľudia, ktorých sa podieľali na vytváraní systému alebo na činnosti, ktorá je predmetom posudzovania. Vykonaním auditu musí organizácia poveriť nezávislého audítora (audítorov), v prípade potreby aj externých. Keď budú audit vykonávať externí audítori, odporúčame zapojiť do audítorského tímu aj vlastných zamestnancov organizácie, aby sa naučili ako sa robí audit.

Audítori budú počas auditu potrebovať komunikovať so zamestnancami (riadiacimi pracovníkmi, informatikmi, používateľmi). Manažér KIB vopred informuje o pripravovanom audite zamestnancov, ktorých súčinnosť pri audite je potrebná a spolu s audítormi pripraví harmonogram auditu.

Príprava plánu auditu. Podrobný plán auditu už pripravujú audítori (rozsah, harmonogram, metódy, ktoré hodlajú použiť) a schvaľuje[31] ho manažér KIB.

[29] do tej sa premietajú aj prípadné povinnosti vykonávať audit vyplývajúce zo zákonov, zmlúv a iných záväzných dokumentov

[30] ak sú, pravda, dostupné

[31] audit zasiahne aj činnosť organizácie a jeho negatívne dopady je potrebné minimalizovať. Preto musí plán auditu schváliť na to oprávnený zamestnanec organizácie.

Vykonanie auditu. Počas samotného auditu audítori budú skúmať objekty (systémy, ich komponenty, opatrenia a pod.) aby zistili, či spĺňajú požiadavky, ktoré sú na ne kladené. Výsledkom posudzovania napr. opatrenia je

a) spĺňa, ak opatrenie v plnom rozsahu plní svoj účel;

b) spĺňa čiastočne, ak ešte nebolo plne implementované, jeho funkcionalita nie je úplná alebo nemá dostatočnú úroveň,

c) iné, ak opatrenie nebolo vôbec implementované, neplní požadované funkcie, alebo audítor nemal na jeho posúdenie potrebné informácie.

Výsledky typu b) a c) audítor musí zdôvodniť (a prípadne uviesť, či môžu spôsobiť narušenie dôvernosti, integrity alebo dostupnosti údajov), aby organizácia vedela, čo potrebuje spraviť na nápravu nedostatkov.

Posúdenie záverov auditu. Partnermi audítorov pri posudzovaní konkrétnych systémov, resp. opatrení, ktoré sa ich týkajú, sú riadiaci pracovníci, ktorí sú za tieto systémy zodpovední (vlastníci systémov). Títo dostanú predbežné výsledky auditu ešte pred tým, ako na ich základe napíšu audítori záverečnú správu a majú možnosť odstrániť zistené nedostatky. Ak sa tak stalo, audítori v záverečnej správe uvedú zistenia, ktoré sa týkajú stavu po odstránení nedostatkov.

Záverečná správa. Odovzdaním záverečnej správy sa pre audítorov audit končí. Zistenia, ktoré záverečná správa obsahuje, spracujú zodpovední pracovníci (manažér KIB, majitelia systémov, informatici) rovnako ako závery analýzy rizík. Posúdia riziká vyplývajúce zo zistených nedostatkov a navrhnú riešenia. Keďže nedostatky v opatreniach znamenajú, že

- sa vynakladajú prostriedky organizácie na nedostatočne účinné opatrenia a
- aktíva organizácie nie sú dostatočne chránené;

záverečnú správu auditu a navrhovaný postup na odstránenie zistených nedostatkov prerokováva vedenie organizácie.

Zhrnutie. Audit je nezávislé posúdenie skutkového stavu oproti nejakému štandardu. V organizácii slúži bezpečnostný audit na posúdenie stavu KIB. Organizuje ho manažér KIB, vykonávajú nezávislí auditori. Bezpečnostný audit môže byť zameraný na riadenie KIB v organizácii (ISMS) a/alebo účinnosť bezpečnostných opatrení. Na audite sa podieľajú aj zamestnanci organizácie; záverečnú správu auditu prerokováva vedenie organizácie.

3.9 Normy

Zaistiť primeranú úroveň IB v organizácii nie je už na prvý pohľad vzhľadom na rozsah, zložitosť a rýchle zmeny IKT jednoduchá úloha. Ak by každá organizácia mala riešiť svoje bezpečnostné problémy vlastnými silami, bola by to pre väčšinu z nich neriešiteľná úloha. Organizácie však našťastie používajú štandardné technické prostriedky so štandardným programovým vybavením. Aj tých niekoľko špecifických aplikácií, ktoré si pre svoje potreby organizácie nechali vytvoriť, využíva štandardné vývojové prostriedky a prevádzkuje sa na štandardných IKT. Prevažná väčšina IKT a programového vybavenia v organizáciách je teda štandardná a má rovnaké

bezpečnostné problémy, ktoré je možné riešiť štandardnými prostriedkami. V priebehu uplynulých 2-3 desaťročí štátne, súkromné, akademické, odborné a iné organizácie vyvinuli značné úsilie o štandardizáciu IB/KIB, výsledkom ktorej je množstvo noriem, technických správ, *de-facto* štandardov, odporúčaní a návodov. Na Slovensku za normalizáciu zodpovedá Úrad pre normalizáciu, metrológiu a skúšobníctvo SR. Úrad však (spoň v oblasti informačnej bezpečnosti) nevyvíja vlastné normy; bezpečnostné normy, ktoré obsahuje STN, sú prebraté prevažne z ISO. ISO normy pre oblasť manažmentu IB sú sústredené v rade ISO/IEC 270xx. Stručne popíšeme tie, ktoré sú prakticky použiteľné pre riadenie KIB v organizácii

ISO/IEC 27000 Information security management systems - Overview and vocabulary. Norma obsahuje prehľad ISO noriem venovaných manažmentu IB a výklad základných pojmov, ktoré sa v normách radu ISO/IEC 270xx používajú. (Najdôležitejšie z nich sú zaradené do výkladového slovníka uvedeného v prílohe tejto knihy).

ISO/IEC 27001:2018 - Information security management systems - Requirements. Toto je relatívne stručná norma obsahujúca požiadavky, ktoré musia spĺňať systémy manažmentu IB (ak majú získať certifikáciu podľa ISO/IEC 27001). Tieto požiadavky sú podrobnejšie rozpracované v norme

ISO/IEC 27002:2013 - Code of practice for information security management. Táto norma obsahuje okolo 120 opatrení, ktoré je potrebné zaviesť na naplnenie požiadaviek stanovených v norme ISO/IEC 27001. Ak by aj organizácia nemala ambície nechať svoj systém manažmentu IB certifikovať podľa ISO/IEC 27001, mala by dobre poznať ISO/IEC 27002, pretože táto norma je základom pre záväzné bezpečnostné štandardy ISVS [13].

ISO/IEC 27005:2018 - Information security risk management. Toto je veľmi užitočná a praktická norma, ktorá popisuje správu rizík, vrátane podrobného postupu pri analýze rizík.

ISO/IEC TS 27008:2019 - Information technology – Security techniques – Guidelines for the assessment of information security controls Norma má formu technickej správy a obsahuje podrobný návod, ako pripraviť audit bezpečnostných opatrení ISMS. Predmetom posudzovania môže byť aj samotný ISMS organizácie; o tom, ako pripraviť a vykonať audit ISMS pojednáva čerstvo aktualizovaná norma ISO/IEC 27007:2020 Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing.

ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity - pomerne všeobecná norma, popisujúca v skutočnosti bezpečnosť Internetu. V súčasnosti sa pripravuje revízia normy, ktorá by mala[32]

- vysvetliť vzťahy medzi bezpečnosťou Internetu, webu, počítačových sietí a kybernetickou bezpečnosťou,
- poskytnúť prehľad bezpečnosti Internetu,
- identifikovať zainteresované strany a ich roly v bezpečnosti Internetu,
- poskytnúť vysokoúrovňový návod riešenia bežných otázok bezpečnosti Internetu,

[32] https://www.iso27001security.com/html/27032.html

- referencovať opatrenia v pripravovanej novej verzii normy ISO/IEC 27002.

ISO/IEC 27103:2018 Information technology – Security techniques – Cybersecurity and ISO and IEC Standards Prehľadová norma popisujúca použitie noriem ISO/IEC 270xx na riešenie problémov kybernetickej bezpečnosti. V podstate premieta kybernetickú bezpečnosť do informačnej bezpečnosti.

ISO normy sú niekedy príliš všeobecné, nie sú voľne dostupné a detailne rozoberajú problémy, ktoré sú zaujímavé len pre úzky okruh špecialistov. Pre praktické použitie môžu byť užitočné normy amerického NIST a nemeckého Spolkového úradu pre informačnú bezpečnosť, BSI.

Americký NIST (National Institute of Standards and Technology - Národný inštitút pre štandardy a technológie) zodpovedá zo zákona za vývoj štandardov, techník a návodov na zaistenie informačnej bezpečnosti IKS (s výnimkou systémov pracujúcich s klasifikovanou informáciou) v amerických štátnych inštitúciách a agentúrach. Hoci je právne prostredie a organizácia amerických inštitúcií iné ako na Slovensku, viaceré z amerických štandardov a množstvo metodických materiálov NIST je použiteľných aj v slovenských podmienkach. Obmedzíme sa opäť na dokumenty súvisiace s manažmentom IB. Základom pre manažment informačnej bezpečnosti je bezpečnostná kategorizácia informačných systémov, ktorá je definovaná v nasledujúcich dvoch federálnych štandardoch:

FIPS 199 Standards for Security Categorization of Federal Information and Information Systems definuje spôsob klasifikácie informácie a systémov, v ktorých sa táto informácia spracováva, založený na ohodnotení dopadov, spôsobených narušením dôvernosti, integrity a dostupnosti informácie. Na tento štandard nadväzuje

FIPS 200 Minimum Security Requirements for Federal Information and Information Systems, ktorý popisuje, ako na základe klasifikácie systémov stanoviť bezpečnostné požiadavky zodpovedajúce požadovanej úrovni ich ochrany. Prístupy uvedené v týchto dvoch amerických štandardoch sú podrobnejšie popísané v prílohe 3.12.5 na strane 54.

NIST vydáva takmer 30 rokov metodické materiály z IB v sérii Special publications 800. Vyššie uvedené federálne štandardy (vytvorené NIST) sú podrobnejšie rozpracované v metodickej publikácii

NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categorization Levels Obsahuje návod na zaradenie informácie a systémov do bezpečnostných kategórií.

Ďalšie dokumenty popisujú postup, ako konkretizovať bezpečnostné potreby systému a vybrať pre ne vhodné riešenia:

NIST SP 800 - 30 Risk Management Guide for Information Technology Systems pokrýva rovnakú problematiku ako ISO/IEC 27005 - správu rizík. Podrobne popisuje najmä analýzu rizík a výber opatrení.

Metodický návod na správu bezpečnostných rizík v priebehu životného cyklu systému zohľadňujúci aj klasifikáciu systémov, je uvedený v publikácii **NIST SP 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems (A Security Life Cycle Approach).**

Jedným z kľúčových dokumentov SP 800, obsahovo podobným ISO/IEC 27002 je **SP 800-53 Recommended Security Controls for Federal Information Systems.** Obsahuje návod ako stanoviť bezpečnostnú kategóriu systému a podrobne špecifikovať bezpečnostné požiadavky na zachovanie dôvernosti, integrity a dostupnosti. Obsahuje aj tri minimálne súbory bezpečnostných opatrení pre systémy z bezpečnostných kategórií nízka, stredná a vysoká.

Na ňu nadväzuje publikácia **Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems,** ktorá sa zaoberá metódami posudzovania efektívnosti opatrení a tým poskytuje spätnú väzbu pre správu rizík.

Aktualizovaný dokument **NIST SP 800-34, Rev. 1, Contingency Planning Guide for Federal Information Systems,** obsahuje návod na prípravu, zavedenie, testovanie a udržiavanie plánov na zabezpečenie kontinuity činnosti organizácie.

Všetky uvedené dokumenty sú napísané tak, aby ich mohli čítať aj ľudia, ktorí sa nezaoberajú KIB. Sú však pomerne rozsiahle, dosť sa prekrývajú a z hľadiska vedúceho pracovníka obsahujú príliš veľa technických podrobností. NIST si toho bol zrejme vedomý a vydal pre vedúcich pracovníkov súbornú príručku manažmentu **IB NIST SP 800-100 Information Security Handbook: A Guide for Managers.** Hoci v slovenských podmienkach určite nebude možné realizovať niektoré jej odporúčania v plnom rozsahu (personálne zabezpečenie KIB, dokumentovanie KIB), poskytuje pohľad na KIB z hľadiska vedúceho pracovníka, ktorý v špecializovaných dokumentoch chýba.

Nemecký BSI vypracoval koncepciu ochrany IKT založenú na tom, že väčšinu systémov tvoria štandardné systémy, ktoré pôsobia v podobných podmienkach. Tento predpoklad umožnil katalogizovať hrozby, zraniteľnosti aj opatrenia. Na základe týchto katalógov je možné dosiahnuť pomerne jednoducho základnú úroveň bezpečnosti (štandardných) systémov; podľa charakteru (typu, určenia, prostredia v ktorom pôsobí) je možné stanoviť pre systém relevantné hrozby a vybrať na ošetrenie rizík, ktoré z nich vyplývajú, štandardné opatrenia. Ak základná úroveň ochrany (Grundschutz) nepostačuje, pre systém je nutné spraviť analýzu rizík (zameranú však len na hrozby, ktoré nie sú dostatočne pokryté štandardnými opatreniami) a navrhnúť dodatočné opatrenia. Táto koncepcia je podporená všeobecne dostupným a pravidelne aktualizovaným katalógom hrozieb, zraniteľností a opatrení a štyrmi štandardami, ktoré sa oplatí prečítať:

BSI Standard 100-1 Information Security Management System (ISMS) definuje požiadavky na ISMS. Je plne kompatibilný s ISO/IEC 27001, ale je názornejší a lepšie čitateľný ako spomenutý ISO štandard.

BSI Standard 100-2 IT-Grundschutz Methodology podrobne vysvetľuje ako vytvoriť, uviesť do činnosti a prakticky „prevádzkovať“ ISMS v organizácii. Popisuje, ako napísať bezpečnostnú politiku, ako vybrať vhodné opatrenia, na čo si dávať pozor pri implementácii bezpečnostnej politiky a ako udržiavať požadovanú úroveň ISMS.

BSI Standard 100-3 Risk analysis on the basis of IT-Grundschutz rieši problém, ktorý sme už spomenuli vyššie: ako efektívne dopĺňať opatrenia poskytujúce základnú úroveň ochrany systému opatreniami, zaručujúcimi vyššiu úroveň ochrany.

Zatiaľ posledný z BSI štandardov venovaných IB je zameraný na kontinuitu činnosti.

BSI Standard 100-4 Business continuity management.

V roku 2017 vydal BSI inovované verzie prvých troch štandardov a v roku 2019 aj **IT-Grundschutz Compendium**, rozsiahlu príručku popisujúcu jednotlivé moduly Grundschutz. Je to dobrý referenčný dokument.

BSI štandardy predstavujú trochu odlišný prístup k zaisteniu IB v organizácii, ako americké federálne štandardy a dokumenty NIST. Sú však kompatibilné s ISO štandardami radu 270xx a ISMS vytvorený na základe BSI štandardov je možné certifikovať podľa ISO/IEC 27001.

Zhrnutie. Normy obsahujú koncentrované odborné know-how riešenia špecifických problémov. Vypracovávajú a posudzujú ich odborníci, sú pravidelne revidované a aktualizované. Súlad z normami je predpokladom technickej aj bezpečnostnej interoperability systémov. Slovensko preberá medzinárodné (ISO) a európske normy, vykonávacie predpisy k zákonom o kybernetickej bezpečnosti a IT vo VS vychádzajú z ISO noriem. ISO normy sú však pomerne drahé a pre neodborníka zložité. Existujú voľne dostupné metodické materiály amerického NIST-u a nemeckého BSI, v ktorých je podobná problematika spracovaná zrozumitelnejšie a v súlade s ISO normami.

3.10 Certifikácia

Certifikácia produktu, systému alebo kvalifikácie je posúdenie, do akej miery spĺňa posudzovaný objekt stanovené certifikačné kritériá. Ak posudzovaný objekt spĺňa certifikačné kritériá v dostatočnej miere, tak mu o tom príslušný certifikačný orgán môže vystaviť osvedčenie. V oblasti KIB sa certifikujú technické zariadenia, systémy a špecialisti v KIB. Technické zariadenia, systémy, v menšej miere softvérové riešenia sa certifikujú najčastejšie podľa ISO/IEC 15408 (Common Criteria).[33] (Objekt posudzovania norma Common Criteria nazýva TOE - Target Of Evaluation, my ho kvôli zjednodušeniu budeme označovať ako systém alebo produkt.) Základom certifikácie systému je tzv. protection profile, registrovaný bezpečnostný model systému. Pri hodnotení systému sa posudzuje, či spĺňa všetky bezpečnostné požiadavky (bezpečnostné funkcie) a na akej úrovni (bezpečnostné záruky). Common Criteria majú definovaných 7 hierarchicky usporiadaných úrovní bezpečnostných záruk (EAL - Evaluation Assurance Level) a teoreticky čím na vyššej úrovni je systém certifikovaný, tým vyššiu úroveň bezpečnostných záruk by mal poskytovať. Výhodou certifikácie systémov (podľa Common criteria) sú bezpečnostne kompatibilné systémy a garantovaná úroveň záruk. Certifikované systémy sa používajú najmä na implementáciu bezpečnostných funkcií, napr. šifrovacie moduly a bezpečné zariadenia na vytváranie elektronických podpisov. Pri rozhodovaní o kúpe nejakého certifikovaného produktu je však popri úrovni záruk (EAL) potrebné preskúmať aj protection profile, oproti ktorému bol produkt certifikovaný, aby sa nestalo, že produkt má síce vysokú úroveň záruk, ale jeho funkcionalita bola obmedzená do takej miery, že nemusí byť použiteľný pre potreby organizácie. Podrobnejšie o certifikácii systémov podľa Common Criteria pojednáva kapitola Architektúra, modely a hodnotenie.

Common Criteria neriešia bezpečnostné aspekty prevádzky certifikovaného systému. Kladú požiadavky na bezpečnostné prostredie systému, ale neuvádzajú bezpečnostné funkcie (opatrenia), pomocou ktorých je tieto požiadavky možné naplniť. Manažmentom IB (KIB) sa zaoberajú už spomínané normy radu ISO/IEC 270xx. Ak má organizácia zavedený ISMS v súlade s normou ISO/IEC 27001, môže si ho nechať oproti tejto norme certifikovať. Norma ISO/IEC

[33] tento rozsiahly štandard je voľne dostupný na https://www.commoncriteriaportal.org/

27007 sa zaoberá auditom ISMS a obsahuje aj zoznam otázok na certifikačný audit ISMS podľa ISO/IEC 27001.

Organizácia neraz potrebuje využiť služby externých špecialistov na KIB. Informačná bezpečnosť na Slovensku sa ešte v nedávnej minulosti študovala ako špecializácia informatiky, resp. v doktorandskom štúdiu. Hoci pred niekoľkými rokmi vznikli (na STU a UK) študijné programy informačnej bezpečnosti, nestíhajú kapacitne pokryť potreby praxe. Postgraduálny systém v minimalistickej forme (prax v KIB a individuálna príprava na základe poskytnutých materiálov a skúška v podobe testu) existuje na Slovensku vyše 20 rokov a takto sa dá získať medzinárodne uznávaná kvalifikácia v informačnej bezpečnosti zložením skúšok na CISA (certifikovaný audítor informačných systémov), CISM (certifikovaný manažér informačnej bezpečnosti), alebo širšie postavený certifikát CGEIT (Certified in the Governance of Enterprise IT[34]). Tieto tri certifikáty vystavuje ISACA - Medzinárodná asociácia pre audit informačných systémov, ktorá má organizáciu aj na Slovensku. Iné certifikáty (ako napr. CISSP) sa dajú získať v zahraničí. Ak organizácia potrebuje vykonať bezpečnostný audit, mala by hľadať certifikovaného auditora informačných systémov, CISA. Manažér IB by mal mať znalosti zodpovedajúce CISM, vo veľkých organizáciách by sa uplatnil človek so znalosťami CGEIT. Pripomíname, že získaním certifikátu sa človek nestáva odborníkom v danej oblasti, certifikát potvrdzuje, že na to má potrebnú prax a vedomosti.

Zhrnutie. Certifikácia je formálne potvrdenie toho, že predmet certifikácie spĺňa certifikačné kritériá. Technické systémy sa najčastejšie certifikujú vzhľadom na rozsah bezpečnostných funkcií a ich úroveň podľa kritérií odvodených z normy ISO/IEC 15408. Systémy manažmentu IB sa certifikujú oproti norme ISO/IEC 27001. Odbornú kvalifikáciu v informačnej bezpečnosti je možné formálne preukázať získaním niektorého z certifikátov CISA, CISM, CISSP, CGEIT a iných.

3.11 Ďalšie oblasti manažmentu kybernetickej a informačnej bezpečnosti

V tejto kapitole sme stručne opísali vybrané oblasti manažmentu kybernetickej a informačnej bezpečnosti. Ďalšie rozoberieme podrobnejšie v samostatných kapitolách tejto knihy.

[34] certifikovaný odborník pre riadenie podnikových IT

3.12 Prílohy

3.12.1 Opatrenia

Táto príloha obsahuje zoznam oblastí KIB a najdôležitejších bezpečnostných opatrení, ktoré musí organizácia prijať (alebo zdôvodniť, prečo ich nepotrebuje), aby zaistila základnú úroveň ochrany svojich IKT. Zoznam je prebratý z dokumentu NIST [10] a slúži ako kontrolný zoznam pre vedúcich pracovníkov a manažéra KIB organizácie. Konkrétne opatrenia na realizáciu úloh uvedených v tomto zozname a aávody na ich implementáciu možno nájsť v samotnom dokumente [10], ale aj napr. v ISO/IEC norme [6].

1. **Riadenie prístupu (Access Control (AC))** Organizácia musí zabezpečiť
   - aby prístup k systému mali len oprávnené osoby a iné zariadenia alebo systémy (externé počítače),
   - aby oprávnené osoby mohli pristupovať (priamo, alebo prostredníctvom iných systémov alebo procesov) len k tým zdrojom systému, na ktoré majú oprávnenia a vykonávať len tie činnosti, na ktoré sú oprávnené.
2. **Bezpečnostné povedomie a tréning (Awareness and Training (AT))** organizácia musí zabezpečiť
   - aby si manažéri a používatelia IKT systémov v organizácii boli vedomí a bezpečnostných rizík spojených s ich činnosťou a požiadaviek, ktoré pre nich vyplývajú v tejto súvislosti z príslušných zákonov, bezpečnostnej politiky a ďalšej vnútornej legislatívy organizácie, bezpečnostných štandardov a prevádzkového poriadku IKT systémov;
   - aby bol personál a používatelia primerane trénovaní na to, aby si dokázali plniť povinnosti podľa prvého bodu týkajúce sa bezpečnosti prevádzky a používania IKT systémov.
3. **Audit a dosledovateľnosť (Audit and Accountability (AU)):** Organizácia musí
   - vytvárať, chrániť a udržiavať záznamy auditu činnosti IKT systému v rozsahu potrebnom na to, aby bolo možné monitorovať, analyzovať, vyšetrovať a nahlasovať protizákonné, neoprávnené alebo neprimerané aktivity v IKT systéme,
   - zabezpečiť, aby jednotlivé aktivity v IKT systéme boli jednoznačne spojené s používateľmi, ktorí ich vykonali a tak títo používatelia mohli byť braní na zodpovednosť za svoju činnosť v systéme.
4. **Certifikácia, akreditácia a bezpečnostné ohodnotenie (Certification, Accreditation, and Security Assessments (CA))** Organizácia musí
   - periodicky vyhodnocovať bezpečnostné opatrenia v IKT systémoch organizácie, aby určila, či sú opatrenia účinné,
   - vypracovať a implementovať plány činnosti zamerané na opravu nedostatkov a redukciu alebo odstránenie zraniteľností v IKT systémoch organizácie

- povoliť/schváliť prevádzku IKT systémov organizácie a pripojenie externých systémov k nim,
- neustále monitorovať bezpečnostné opatrenia na ochranu IKT systémov, aby zaistila ich stálu účinnosť.

5. **Manažment konfigurácie (Configuration Management (CM))** Organizácia musí
   - zaviesť a udržiavať základné konfigurácie IKT systémov a katalógy IKT systémov (hw, sw, firmware a dokumentácia) organizácie počas ich životných cyklov,
   - zaviesť a presadzovať nastavenia bezpečnostnej konfigurácie IKT produktov používaných v IKT systémoch organizácie
6. **Havarijné plánovanie (Contingency Planning (CP)):** Organizácia musí
   - vypracovať, udržiavať a efektívne implementovať plány reakcie organizácie na mimoriadne situácie, zálohovacie procedúry a plány obnovy pre IKT systémy organizácie, aby zaistila dostupnosť kritických informačných zdrojov a kontinuitu operácií v mimoriadnych situáciách.
7. **Identifikácia a autentifikácia Identification and Authentication (IA):** Organizácia musí
   - identifikovať používateľov IKT systémov, zariadení, procesov konajúcich v záujme po-užívateľov; a overiť identity týchto používateľov, procesov alebo zariadení ešte pred tým ako im povolí prístup k IKT systémom organizácie
8. **Reakcia na incidenty (Incident Response (IR))** Organizácia musí
   - pre IKT systémy organizácie vytvoriť operačné kapacity na riešenie bezpečnostných incidentov, ktoré sú schopné vykonávať adekvátnu prípravu zamestnancov, detekciu, analýzu, ohraničenie bezpečnostného incidentu, obnovu IKT systému po incidente a primerané reakcie používateľov na incident,
   - vystopovať pôvod incidentu, zdokumentovať ho a nahlasovať príslušným riadiacim pracovníkom organizácie, prípadne úradom.
9. **Údržba (Maintenance (MA))** : Organizácia musí
   - vykonávať aktuálnu (podľa potreby) a periodickú údržbu IKT systémov organizácie,
   - zabezpečovať efektívny dohľad nad nástrojmi, technikami, mechanizmami, ktoré sa používajú pri údržbe a personálom ktorý údržbu vykonáva.
10. **Ochrana médií (Media Protection (MP))** Organizácia musí
    - chrániť pamäťové média tak papierové ako aj digitálne (elektronické),
    - omedziť prístup k informáciám uloženým na pamäťových médiách IKT systému len pre oprávnené osoby,
    - zničiť pamäťové médiá pred ich vyradením alebo bezpečne odstrániť údaje z pamäťových médií pred ich opätovným použitím.

11. **Fyzická ochrana a ochrana prostredia (Physical and Environmental Protection (PE))** Organizácia musí

    - obmedziť fyzický prístup k IKT systémom, zariadeniam a do ich operačného prostredia len na oprávnené osoby,
    - chrániť fyzické zariadenia a podporovať infraštruktúru IKT systémov,
    - poskytovať pre IKT systémy podporné zariadenia potrebné pre ich prevádzku,
    - chrániť IKT systémy proti prírodným hrozbám a hrozbám z prostredia,
    - zaistiť primerané environmentálne opatrenia v zariadeniach v ktorých sú umiestnené IKT systémy.

12. **Plánovanie (Planning (PL)):** Organizácia musí

    - vyvinúť, zdokumentovať, periodicky aktualizovať a implementovať bezpečnostné plány pre IKT systémy organizácie, ktoré popisujú použité alebo plánované bezpečnostné opatrenia pre IKT systémy a pravidlá správania jednotlivcov, pristupujúcich k IKT systémom.

13. **Personálna bezpečnosť (Personnel Security (PS))** Organizácia musí

    - zabezpečiť, aby jednotlivci ktorí zastávajú zodpovedné funkcie v organizácii (vrátane tretích strán poskytujúcich služby organizácii) boli dôveryhodné osoby a spĺňali bezpečnostné kritériá stanovené pre dané funkcie,
    - zaistiť, aby informácie a IKT systémy organizácie boli chránené počas personálnych zmien a po nich, ako sú ukončenie pracovného pomeru alebo zmena pracovného zaradenia,
    - zaviesť a uplatňovať formálne sankcie voči zamestnancom, ktorí konali v rozpore s bezpečnostnou politikou alebo bezpečnostnými procedúrami organizácie.

14. **Ohodnotenie rizík (Risk Assessment (RA)):** Organizácia musí

    - periodicky ohodnocovať riziká voči aktivitám organizácie (vrátane poslania organizácie, funkcií, ktoré plní, imidžu alebo reputácie), aktívam organizácie, a jednotlivcom, ktoré vyplývajú z činnosti IKT systémov organizácie a s nimi súvisiaceho spracovania, ucho-vávania alebo prenosu informácie.

15. **Obstarávanie systémov a služieb (System and Services Acquisition (SA)):** Organizácia musí

    - vyhradiť dostatočné zdroje na primeranú ochranu IKT systémov organizácie,
    - používať v priebehu celého životného cyklu systému také procesy, ktoré zohľadňujú bezpečnostné aspekty systému,
    - dodržiavať obmedzenia na inštaláciu a používanie softvéru
    - zaistiť, aby tretie strany pri poskytovaní služieb organizácii používali adekvátne bezpečnostné opatrenia na ochranu informácie, aplikácií a/alebo služieb ktoré organizácii poskytujú.

16. **Ochrana systému a komunikácie (System and Communications Protection (SC))** Organizácia musí

    - monitorovať, kontrolovať a chrániť komunikáciu organizácie (t.j. informácie vysielanú alebo prijímanú IKT systémami organizácie) na vonkajších hraniciach a kľúčových vnútorných hraniciach informačných systémov,

    - uplatňovať pri vývoji a prevádzke IKT systémov také návrhy architektúry, techniky vý-voja softvéru a inžinierske princípy, ktoré podporujú informačnú bezpečnosť v IKT systémoch organizácie.

17. **Integrita systému a informácie (System and Information Integrity (SI))** Organizácia musí

    - včas identifikovať, nahlasovať[35] a korigovať chyby v údajoch a v IKT systémoch organizácie,

    - na vhodnom mieste IKT infraštruktúry organizácie (centrálne a/alebo distribuovane) zabezpečovať ochranu IKT systémov pred škodlivým softvérom,

    - monitorovať bezpečnostné výstrahy a odporúčania systému a primerane na ne reagovať.

[35] pre nahlasovane odhalených zraniteľností, chýb, príznakov bezpečnostných incidentov alebo iných bezpečnostne relevantných udalostí by mali byť stanovené kontaktné osoby (vedúci, správca systému, manažér IB), ktorým má zamestnanec, ktorý problém odhalil, informáciu podať

3.12.2 Katalóg hrozieb

Zoznam hrozieb bol prevzatý z webovej stránky Spolkového úradu pre informačnú bezpečnosť, BSI. A označuje Availability (dostupnosť), C Confidentiality (dôvernosť), I Integrity (integritu).

Tabuľka 3.3: Katalóg hrozieb

kód	**hrozba**	**dopad**
T.1	Požiar	I,A
T.2	Nepriaznivé klimatické podmienky	I,A
T.3	Voda	I,A
T.4	znečistenie, prach. korózia	I,A
T.5	Prírodné katastrofy	A
T.6	Katastrofy životného prostredia	A
T.7	veľké udalosti v prostredí/okolí (demonštrácie, nepokoje)	C,I,A
T.8	zlyhanie alebo prerušenie dodávky energie	I,A
T.9	zlyhanie alebo prerušenie komunikačných sietí	I,A
T.10	zlyhanie alebo poškodenie zdrojov energie	A
T.11	zlyhanie alebo prerušenie poskytovania služieb	C,I,A
T.12	interferujúca radiácia	I,A
T.13	zachytenie kompromitujúceho vyžarovania	C
T.14	zachytenie informácie/špionáž	C
T.15	odpočúvanie	C
T.16	krádež zariadení, pamäťových médií alebo dokumentov	C,A
T.17	strata zariadení, pamäťových médií alebo dokumentov	C,A
T.18	zlé plánovanie alebo nedostatok adaptácie	C,I,A
T.19	prezradenie citlivej informácie	C
T.20	informácie z nespoľahlivého zdroja	C,I,A
T.21	manipulácia s hw a sw	C,I,A
T.22	manipulácia s informáciou	I
T.23	neoprávnený prístup k IKT systémom	C,I,A
T.24	zničenie zariadení alebo pamäťových médií	A
T.25	zlyhanie zariadení alebo systémov	C,I,A
T.26	nesprávne fungovanie zariadení alebo systémov	C,I,A
T.27	nedostatok zdrojov	A
T.28	zraniteľnosti alebo chyby sw	C,I,A
T.29	porušenie zákonov alebo predpisov	C,I,A
T.30	neoprávnené používanie alebo správa zariadení a systémov	C,I,A
T.31	nesprávne používanie alebo správa zariadení a systémov	C,I,A
T.32	zneužitie oprávnení	C,I,A

T.33	absencia personálu	A
T.34	útok	C,I,A
T.35	prinútenie, vydieranie, korupcia	C,I,A
T.36	krádež identity	C,I,A
T.37	popretie činnosti	C,I
T.38	zneužitie osobných údajov	C
T.39	škodlivý sw	C,I,A
T.40	odmietnutie služby	A
T.41	sabotáž	A,I
T.42	sociálne inžinierstvo	C,I
T.43	opakované posielanie správ	C,I
T.44	neoprávnený vstup do priestorov	C,I,A
T.45	strata údajov	A
T.46	strata integrity citlivej informácie	I

3.12.3 Zoznam zraniteľností

V tejto časti je uvedený zoznam zraniteľností prevzatý z normy [7] doplnený o niektoré zraniteľnosti uvedené v dokumente [11]. Podrobný zoznam zraniteľností možno nájsť v [3]. Pre každú zraniteľnosť sú na ilustráciu uvedené hrozby (hrozba), ktoré môžu danú zraniteľnosť využiť. Úplný zoznam hrozieb schopných využiť uvedené zraniteľnosti je vo väčšine prípadov podstatne rozsiahlejší.

Tabuľka 3.4: Zoznam vybraných zraniteľností

kód	zraniteľnosť	hrozba
Prostredie a infraštruktúra		
Z.1.1	nedostatočná fyzická ochrana budov, dverí, okien	neoprávnený prístup, krádež
Z.1.2	zanedbanie alebo nedostatočná úroveň fyzického riadenia prístupu do budovy alebo miestností	neoprávnený prístup, zámerné poškodenie, krádež
Z.1.3	nestabilná elektrická sieť	výpadok zdrojov energie
Z.1.4	umiestnenie v oblastiach ohrozených záplavami	záplava
Hardvér		
Z.2.1	neexistuje harmonogram periodickej výmeny	zhoršovanie kvality pamäťových médií
Z.2.2	citlivosť na kolísanie napätia	výpadok napätia, prepätie, kolísanie napätia
Z.2.3	citlivosť na výkyvy teplôt	teplotné extrémy
Z.2.4	citlivosť na vlhkosť, prašnosť, znečistenie	nadmerná prašnosť (vietor, stavebné práce)
Z.2.5	citlivosť na elektromagnetické žiarenie	elektromagnetické žiarenie
Z.2.6	nedostatočná údržba alebo chybná inštalácia pamäťových médií	chyba údržby, nedostatok pamäťových kapacít, nedostupnosť zdrojov
Z.2.7	chýba efektívne riadenie zmien konfigurácie	chyba obsluhy

kód	zraniteľnosť	hrozba
	Programové vybavenie (softvér	
Z.3.1.	nejasná alebo neúplná špecifikácia pre vývojárov	chyba obsluhy
Z.3.2.	žiadne alebo nedostatočné testovanie programového vybavenia	zlyhanie softvéru
Z.3.3.	komplikované používateľské rozhranie	chyba obsluhy
Z.3.4.	chýbajúce alebo nedostatočné mechanizmy pre identifikáciu a autentizaciu	predstieranie cudzej identity
Z.3.5.	nedostatočný alebo chýbajúci záznam auditu	použitie softvéru neoprávneným spôsobom
Z.3.6.	všeobecne známe vady programového vybavenia	použitie softvéru neoprávneným spôsobom
Z.3.7.	nechránené tabuľky hesiel	predstieranie cudzej identity
Z.3.8.	slabý manažment hesiel (slabé heslá, ukladanie nešifrovaných hesiel, rovnaké heslá pre rozličné účely, nedostatočne časté menenie hesiel)	predstieranie cudzej identity
Z.3.9.	nesprávne pridelenie prístupových práv	použitie softvéru neoprávneným spôsobom
Z.3.10.	nekontrolované sťahovanie a používanie softvéru	zlomyseľný softvér
Z.3.11.	opustenie pracovnej stanice bez odhlásenia	
Z.3.12.	chýba efektívne riadenie zmien	zlyhanie softvéru
Z.3.13.	nedostatočná alebo chýbajúca dokumentácia	chyba obsluhy
Z.3.14.	chýbajú záložné kópie (údajov, programového vybavenia)	zlomyseľný softvér, požiar
Z.3.15.	vyradenie alebo opätovné používanie pamäťových médií bez poriadneho vymazania údajov	použitie softvéru neoprávneným spôsobom, únik údajov (narušenie dôvernosti údajov)
Z.3.16.	povolená nepotrebná služba	použitie softvéru neoprávneným spôsobom, neoprávnený prístup do systému

Z.3.17.	nedokončený alebo nový softvér (neúplné alebo neadektvítne testovanie)	zlyhanie softvéru,použitie softvéru neoprávneným spôsobom
Z.3.18.	široko distribuovaný softvér	strata integrity sw počas distribúcie
	Komunikácia	
Z.4.1.	nechránené komunikačné linky	odpočúvanie, prerušenie linky
Z.4.2.	zlé prepojenie káblov	infiltrácia komunikácie
Z.4.3.	nedostatky v identifikácii odosielateľa a prí-jemcu	predstieranie cudzej identity
Z.4.4.	prenos hesiel v otvorenej forme	prístup k sieti pre neoprávneneho používateľa
Z.4.5.	nedostatočné/chýbajúce potvrdenie zaslatia alebo prijatia správy	popretie pôvodu alebo prijatia
Z.4.6.	používanie modemov (dial up)	prístup neoprávneného používateľa do systému/siete
Z.4.7.	nechránený prenos citlivých správ	odpočúvanie
Z.4.8.	neadekvátna správa siete (routing)	preťaženie siete
Z.4.9.	nechránené pripojenie k verejnej sieti	použitie softvéru neoprávne-ným spôsobom
Z.4.10.	nedostatočne bezpečná architektúra siete	prienik do siete
	Dokumenty	
Z.5.1.	nechránené úložisko	krádež, narušenie dôvernosti
Z.5.2.	nedostatočná starostlivosť pri vyraďovaní dokumentov	krádež, narušenie dôvernosti
Z.5.3.	nekontrolované kopírovanie	narušenie dôvernosti krádež

kód	zraniteľnosť	hrozba
	Personál	
Z.6.1.	absencia personálu	nedostatok personálu
Z.6.2.	práca externých pracovníkov alebo upratovavacieho personálu bez dohľadu	krádež, neoprávnený prístup do systému
Z.6.3.	nedostatočný bezpečnostný tréning	chyba obslužného personálu
Z.6.4.	nedostatočné bezpečnostné povedomie chyby	používateľov
Z.6.5.	nesprávne použitie sw alebo hw	chyba obslužného personálu
Z.6.6.	nedostatočné alebo chýbajúce monitorovacie mechanizmy	použitie sw neoprávneným spôsobom
Z.6.7.	nedostatočné alebo chýbajúce politiky upra-vujúce korektné používanie telekomunikač-ných prostriedkov a výmeny správ	použitie sietí neautorizova-ným spôsobom
Z.6.8.	nedostatočné procedúry pri získavaní pra-covníkov	úmyselné poškodenie systé-mu, chyba obsluhy
	Procedurálne zraniteľnosti	
Z.7.1	chybajúca autorizácia prostriedkov na spracovanie informácie	úmyselné poškodenie systé-mu
Z.7.2	nedostatočný formálny proces schvaľovania verejne dostupnej informácie	vstup poškodených údajov
Z.7.3	chýbajúci formálny proces revízie prístupových práv	neoprávnený prístup
Z.7.4	chýba politika o používaní mobilných počítačov a podobných zariadení	krádež, neoprávnený prístup do systému
Z.7.5	chýbajú formálne procedúry riadenia ISMS dokumentácie	vstup poškodených údajov
Z.7.6	chýbajú formálne procedúry kontroly/sledovania záznamov ISMS	vstup poškodených údajov
Z.7.7	chýbajú formálne procedúry registrovania a odregistrovania používateľov	neoprávnený prístup
Z.7.8	chýba kontrola aktív umiestnených mimo budovy	krádež
Z.7.9	chýba dohoda o úrovni služieb (Service Level Agreement)	hyba údržby

Z.7.10	chýba "politika čistého stola a čistej obrazovky"	krádež informácie, neoprávnený prístup k systému, narušenie dôvernosti
Z.7.11	chýbajúce alebo nedostatočné ustanovenia v zmluvách so zákazníkmi alebo tretími stranami	neoprávnený prístup, chyba údržby, chyba sw
Z.7.12	chýbajúce alebo nedostatočné ustanovenia o bezpečnosti v zmluvách so zamestnancami	podvod, krádež
Z.7.13	chýbajú plány kontinuity činnosti	technické zlyhanie
Z.7.14	chýba náležité vymedzenie zodpovednosti za informačnú bezpečnosť	odmietnutie zodpovednosti
Z.7.15	chýba politika pre používanie elektronickej pošty	únik citlivej informácie, nesprávne smerovanie správ
Z.7.16	chýbajú procedúry identifikácie a ohodnotenia/odhadu rizika	neoprávnený prístup k systému
Z.7.17	chýbajú procedúry pre narábanie s klasifikovanou informáciou	hyba používateľa, únik citli-vých informácií
Z.7.18	chýbajú procedúry upravujúce narábanie s informáciami, na ktoré sa vzťahuje ochrana duševného vlastníctva	krádež informácie, právny postih
Z.7.19	chýbajú procedúry na oznamovanie bezpečnostných slabín	používanie systému a sietí neoprávnenýcm spôsobom
Z.7.20	chýbajú procedúry zavádzania sw do bežiacich systémov	chyba obsluhy
Z.7.21	chýba procedúra riadenia zmien	chyba údržby
Z.7.22	chýba procedúra monitorovania prostriedkov/zariadení na spracovanie informácie	neoprávnený prístup
Z.7.23	nerobí sa pravidelný audit (dohľad, kontrola)	neoprávnený prístup
Z.7.24	nerobia sa pravidelné revízie manažmentu (systému)	zneužitie zdrojov
Z.7.25	nie je zavedený monitorovací mechanizmus pre narušenia bezpečnosti	úmyselné poškodenie systému
Z.7.26	chýba stanovenie zodpovednosti za informačnú bezpečnosť v pracovnej náplni	chyby používateľov

Z.7.27	hlásenia o závadách nie sú zaznamenané v logoch administrátora a operátora	chyba obsluhy
Z.7.28	nie je definovaný disciplinárny proces pre prípad bezpečnostného incidentu	krádež informáce, neoprávnený prístup, používanie sw neoprávneným spôsobom
Zraniteľnosti v aplikáciách		
Z.8.1	nesprávne nastavenie parametrov	omyl používateľa
Z.8.2	použitie aplikačných programov na chybné údaje (napr. neaktuálne)	nedostupnosť údajov
Z.8.3	neschopnosť vytvoriť prevádzkové správy	neoprávnený prístup
Z.8.4	nesprávne údaje	omyl používateľa
Všeobecné zraniteľnosti		
Z.9.1.	single point of failure (úzke miesto, alebo kritický prvok systému)	zlyhanie systému, úmyselné poškodenie
Z.9.2.	nedostatočná údržba	zlyhanie hw, sw

3.12.4 Obsah bezpečnostnej politiky

V bezpečnostnej politike organizácie (vydanej vedením organizácie) musí byť stanovený záväzný základný rámec pre kybernetickú a informačnú bezpečnosť organizácie. Podľa ISO normy [6] bezpečnostná politika by mala povinne obsahovať (resp. rámcovo upravovať):

a) deklaráciu vedenia organizácie o význame ochrany informácie, identifikácii hlavných aktív a stanovení cieľov informačnej bezpečnosti v organizácii a podpore vedenia organizácie pri ich napĺňaní,

b) vymedzenie oblasti použiteľnosti danej bezpečnostnej politiky (z čoho bezpečnostná politika vychádza a na čo všetko sa vzťahuje),

c) štruktúru bezpečnostných dokumentov nadväzujúcich na danú bezpečnostnú politiku a ich obsah (špeciálne bezpečnostné politiky, alebo bezpečnostné štandardy, bezpečnostné praktiky - aké oblasti pokrývajú a akou formou budú vydané)

d) stanovenie zodpovednosti zamestnancov organizácie za presadzovanie a dodržiavanie bezpečnostnej politiky (a dokumentov na ňu nadväzujúcich),

e) klasifikáciu informácie (na základe čoho sa bude informácia v organizácii klasifikovať)

f) spôsob analýzy rizík a hranica akceptovateľného rizika,

g) monitoring, kontrola, audit IKS,

h) riešenie bezpečnostných incidentov,

i) zaistenie kontinuity činnosti IKS organizácie,

j) správa bezpečnostnej politiky (ako často sa budú robiť pravidelné a z akých dôvodov mimoriadne revízie bezpečnostnej politiky).

Ak by bezpečnostná politika mala byť podrobnejšia, mala by stanoviť aj zásady pre

a) riadenie prístupu (k údajom a službám IKS organizácie),

b) dosledovateľnosť (accountability)—pre aké činnosti,

c) záznamy auditu (o čom sa budú vytvárať, kto a ako ich bude spracovávať),

d) outsourcing služieb súvisiacich s vývojom a prevádzkou IKS,

e) vývoj softvéru a obstarávaním IKT,

f) zálohovanie údajov a softvéru (čo a ako často),

g) kontinuitu činnosti (Business continuity planning)—identifikácia systémov kritických pre organizáciu a povinnosť vypracovať a implementovať havarijné plány,

h) vyraďovanie pamäťových médií,

i) likvidácia papierových dokumentov,

j) prístup na Internet a používanie elektronickej pošty,

k) „vlastníctvo informácií“—komu patria jednotlivé údaje, práva a povinnosti z toho vyplývajúce,

l) vynášanie IKT zariadení mimo priestorov (opravy),

m) používanie prenosných zariadení a práca na diaľku,

n) ochranu pred škodlivým softvérom,

o) šifrovú ochrana informácie,

p) bezpečnosť pracovných staníc (minimálna požadovaná úroveň),

q) ochranu súkromia

r) disciplinárne pokračovanie v prípade porušenia pravidiel stanovených bezpečnostnou politikou,

s) dosiahnutie/udržiavanie súladu s legislatívou (najmä v prípade medzinárodných organizácií, pôsobiacich v prostredí s rozdielnou legislatívou)

t) prípadne iné, ktoré organizácia považuje za potrebné.

a zásady stanovené v bezpečnostnej politike prípadne rozpracovať do podoby špecifických politík.

3.12.5 Klasifikácia informácie a systémov

Klasifikácia informácie a systémov umožňuje zjednodušiť manažment kybernetickej a informačnej bezpečnosti v organizácii tým, že namiesto toho, aby sa každý prípad (údaj, resp. systém) posudzoval a jeho ochrana riešila zvlášť, definujú sa klasifikačné kritériá, na základe ktorých je možné rozdeliť údaje do (bezpečnostných) tried s rovnakými bezpečnostnými potrebami. Existuj katalógy štandardných bezpečnostných opatrení (v Nemecku tzv. Grundschutzbuch BSI) a pre jednotlivé triedy sú stanovené súbory štandardných bezpečnostných opatrení, garantujúcich požadovanú úroveň ochrany údajov[36]. (Klasifikácia systémov je odvodená od klasifikácie údajov, ktoré sa v nich spracovávajú.) Stanovenie bezpečnostných opatrení pre údaje sa potom robí tak, že sa informácia podľa klasifikačných kritérií zaradí do niektorej triedy a na jej ochranu sa použijú opatrenia zodpovedajúce danej triede. (Ak by na údaje boli kladené špeciálne bezpečnostné požiadavky z hľadiska obsahu alebo úrovne ochrany, na ktoré nestačia takéto „konfekčné“ bezpečnostné riešenia, bude potrebné spraviť analýzu rizík, vybrať a použiť vhodné opatrenia na ochranu údajov s neštandardnými bezpečnostnými potrebami zvlášť. V nemeckom štandarde [2] sa uvádza, že katalógové riešenia podľa metodiky štandardu [1] pokrývajú 80% prípadov.) Pozrieme sa na klasifikáciu údajov/informácie a systémov podrobnejšie. Budeme vychádzať z amerických noriem [4],[5] ale na záver ukážeme, že navrhované riešenia sú zovšeobecnením klasických klasifikačných schém.

Požiadavky na ochranu údajov sa v konečnom dôsledku redukujú na základné bezpečnostné požiadavky (dôvernosť, integrita, dostupnosť, autentickosť, súkromnosť a i.) alebo nejakú ich kombináciu. Vyberieme tri základné bezpečnostné požiadavky dôvernosť, integrita a dostupnosť a pre každú z nich stanovíme štyri hierarchicky klasifikačné stupne, vychádzajúc z hodnoty dopadu v dôsledku narušenia príslušnej bezpečnostnej požiadavky (vysvetlíme to na príklade dôvernosti, pre integritu a dostupnosť budeme postupovať rovnako):

1. NA (not aplicable, nepoužiteľné) - ak sa požiadavka na dôvernosť nedá na údaje aplikovať,
2. nízky—ak je dopad narušenia dôvernosti údajov nízky,
3. stredný—ak je dopad narušenia dôvernosti údajov stredný,
4. vysoký—ak je dopad narušenia dôvernosti údajov vysoký.

Úroveň dopadu sa vyjadruje rovnako, ako pri analýze rizík. Pre každý z klasifikačných stupňov vyberieme (existujú štandardne preddefinované súbory, ktoré môžeme prebrať bez zmeny, alebo upraviť podľa potreby) súbor bezpečnostných opatrení primeraný klasifikačnému stupňu. Takto vzniknú po tri súbory bezpečnostných opatrení pre dôvernosť, integritu a dostupnosť. (Pre stupeň NA nie sú predpísané žiadne opatrenia). Klasifikáciu údajov budeme robiť nasledovne:

keďže je pravdepodobné, že údaje, ktoré sa používajú v rovnakom prostredí na podobný účel, budú mať aj podobné bezpečnostné požiadavky, budeme klasifikovať typy údajov, ktoré majú podobný charakter (osobné údaje, zdravotné údaje, ekonomické údaje, programy, konfiguračné parametre, kryptografické kľúče, heslá, autentizačné údaje a pod.). Tento prístup

[36] v Nemecku spomínaný BSI Grundschutzbuch [1], v USA požiadavky na ochranu štátnych informačných systémov (obdoba ISVS) [10], [12] a na Slovensku upravujú klasifikáciu informácie a kategorizáciu viaceré zákony, najpodrobnejšie sú bezpečnostné požiadavky (na ISVS) rozpísané vo vyhláške [13]

nevylučuje možnosť dodatočnej klasifikácie konkrétnych údajov, ktoré sa nepodarilo zaradiť do žiadneho typu. Každému typu informácie/údajov priraďujeme trojicu [4]

$$\mathrm{SC}_{\text{typ informácie}} = ((\text{dôvernosť, dopad}), (\text{integrita, dopad}), (\text{dostupnosť, dopad}))$$

kde SC označuje security category, bezpečnostnú kategóriu a hodnota dopadu je prvok množiny nízka, stredná, vysoká, alebo NA (nepoužiteľná). Pre lepšie pochopenie označenia uvedieme niekoľko príkladov. Uvažujme informáciu, ktorú organizácia vystavuje na svojej webovej stránke. Takúto informáciu označíme ako verejnú informáciu a priradíme jej ohodnotenie:

$$\mathrm{SC}_{\text{verejná informácia}} = ((\text{dôvernosť, NA}), (\text{integrita, stredná}), (\text{dostupnosť, stredná}))$$

Pre zdravotnú informáciu (zdravotná dokumentácia pacienta)

$$\mathrm{SC}_{\text{zdravotná informácia}} = ((\text{dôvernosť, vysoká}), (\text{integrita, vysoká}), (\text{dostupnosť, stredná}))$$

Systém klasifikujeme na základe klasifikácie všetkých typov informácie, ktoré sa v ňom spracovávajú. Taktiež mu priraďujeme trojzložkový vektor:

$$\mathrm{SC}_{\text{informačný systém}} = ((\text{dôvernosť, dopad}), (\text{integrita, dopad}), (\text{dostupnosť, dopad}))$$

kde sa ako hodnota dopadu pre dôvernosť systému berie maximum z hodnôt dopadu pre dôvernosť jednotlivých typov informácií, ktoré sa v ňom spracovávajú. Podobne pre výpočet úrovne hodnôt integrity a dostupnosti. Na rozdiel od klasifikácie údajov sa hodnota NA pri klasifikácii systémov nepoužíva a namiesto nej sa používa hodnota „nízka“. Ak sa v systéme spracováva zdravotná a verejná informácia s ohodnotením podľa predchádzajúceho príkladu, tak jeho bezpečnostná klasifikácia bude

$$\mathrm{SC}_{\text{informačný systém}} = ((\text{dôvernosť, vysoká}), (\text{integrita, vysoká}), (\text{dostupnosť, stredná})).$$

Poznámky.

1. Hoci existuje viacero bezpečnostných požiadaviek, najčastejšie sa na klasifikáciu informácie používa tradične dôvernosť. Informačná bezpečnosť sa však definuje ako dosiahnutie potrebnej úrovne dôvernosti, integrity a dostupnosti údajov (IKT a služieb). Pri analýze rizík sa zohľadňujú aj iné bezpečnostné požiadavky (nepopretie prijatia, pôvodu, súkromnosť, dosledovateľnosť, anonymita, pseudonymita, a i.) a to znamená, že údaje je potrebné skúmať (klasifikovať) aj z hľadiska iných bezpečnostných požiadaviek, ako je dôvernosť. Keby sa však údaje/informácia klasifikovali podľa viacerých bezpečnostných požiadaviek, vznikli by dva problémy:

   a) niektoré bezpečnostné požiadavky sú protirečivé (dosledovateľnosť a anonymita), medzi inými sú silné väzby (autentickosť a integrita), čo by bolo pri návrhu klasifikácie potrebné jednoznačne vyriešiť.

b) už pri troch bezpečnostných požiadavkách a štyroch úrovniach dopadu dostávame $4^3 = 64$ možných kombinácií hodnôt. Pre n bezpečnostných požiadavkách a štyroch úrovniach dopadu máme 4^n možných kombinácií, ktoré by vzhľadom na možné vzťahy medzi jednotlivými požiadavkami bolo treba riešiť jednotlivo. Takáto klasifikačná schéma by však bola obrovská a prakticky nepoužiteľná.

c) čo s opatreniami? Ako sa bude líšiť opatrenie na zaistenie napr. integrity na strednej úrovni od opatrenia na zaistenie integrity na vysokej úrovni? A čo s opatreniami rozličnej úrovne pre také špecifické požiadavky ako je pseudonymita, zaistenie súkromnosti?

Obmedzenie množiny bezpečnostných požiadaviek použitých na klasifikáciu na tri (trojica CIA: confidentiality, integrity, availability) má niekoľko dôvodov:

a) snaha obmedziť počet tried a veľkosť klasifikačnej schémy (hoci aj 64 tried sa môže zdať veľa),

b) relatívna nezávislosť dôvernosti, integrity a dostupnosti, ktorá umožňuje pre jednotlivé stupne ochrany napr. dôvernosti stanoviť požadovanú úroveň záruk nezávisle od ostatných bezpečnostných požiadaviek. To znamená, že bude potrebné vypracovať požiadavky na opatrenia, ktoré zaručia dostatočnú ochranu dôvernosti informácie v prípade, keď je dopad narušenia jej dôvernosti nízky, stredný a vysoký. Podobne pre integritu a dostupnosť. Vďaka relatívnej nezávislosti dôvernosti, integrity a dostupnosti stačí vypracovať 9 súborov požiadaviek na opatrenia, namiesto 64, čo je ešte zvládnuteľné.

2. Ak nestačí kategorizácia podľa typu údajov (napr. v prípade utajovaných skutočností), je možné rozdeliť kategóriu údajov na podkategórie (v prípade utajovaných skutočností na vyhradené, dôverné, tajné a prísne tajné) a stanoviť úroveň bezpečnostných požiadaviek pre tieto podkategórie.

3. Americký štandard [4] chápe integritu širšie, ako sme ju definovali my v úvodnej časti. Z pragmatických dôvodov zahŕňa do integrity aj autentickosť a nepopretie pôvodu. Táto definícia je trocha nekonzistentná (dá sa použiť pre údaje, ale nie pre fyzické systémy), ale pri štúdiu amerických noriem treba mať na pamäti tento rozdiel.

4. Vektorové ohodnotenie bezpečnostnej kategórie typu informácie je v prípade potreby možné nahradiť skalárnym, t.j. jednou hodnotou. Ostatné hodnoty sa nastavia na NA. To umožňuje vyjadriť existujúce klasifikačné schémy postavené na jednom kritériu (bezpečnostnej požiadavke) pomocou vektorovej klasifikačnej schémy. Na druhej strane, vektor (dôvernosť, integrita, dostupnosť) je možné rozšíriť o ďalšie zložky. Ak by sme napríklad chceli rozlišovať integritu a autentickosť, ale zaradiť autentickosť medzi klasifikačné kritériá, údajom a systémom budeme priraďovať štvoricu hodnôt (dôvernosť, integrita, dostupnosť, autentickosť) na škále NA, nízka, stredná, vysoká.

5. Štandard [4] rieši klasifikáciu informácií a systémov. Naň nadväzujúci štandard [5] popisuje výber opatrení potrebných na zaistenie potrebnej úrovne ochrany informácií spracovávaných v systéme.

3.12.6 Príklad bezpečnostnej politiky

Ako sme uviedli v tejto kapitole, koncepcia informačnej bezpečnosti organizácie má podobu bezpečnostnej politiky. Viacero zákonov priamo alebo nepriamo požaduje od organizácie (povinnej osoby) vytvorenie (a dodržiavanie) bezpečnostnej politiky alebo podobného dokumentu. Najpodrobnejšie je obsah bezpečnostnej politiky špecifikovaný vo vyhláške [13]. Bezpečnostné štandardy pre ISVS sú kompatibilné s normou ISO/IEC 27002. Bezpečnostná politika podľa [13] spĺňa aj požiadavky stanovené inými zákonmi, resp. môže byť základom, ktorý sa dá doplniť tak, aby spĺňal špecifické požiadavky iných zákonov. V tejto časti uvedieme príklad bezpečnostnej politiky fiktívnej organizácie (s veľmi zjednodušenou organizačnou štruktúrou) a ilustrujeme na nej, ako sa tvorí bezpečnostná politika[37].

3.12.7 Fiktívny úrad

Predpokladáme, že naša organizácia je nejaký Fiktívny úrad (FÚ) s celoslovenskou pôsobnosťou, ktorý

a) je zriadený špeciálnym Zákonom o Fiktívnom úrade (ZFU)

b) má fiktívnu agendu, ktorá sa delí na čiastkové fiktívne agendy FA-1, FA-2,...

c) spravuje Centrálny register (CR), v ktorom sa spracovávajú referenčné údaje pre FA-1; CR je prvkom kritickej infraštruktúry

d) okrem CR má niekoľko ďalších informačných systémov IS-2, IS-3,... ktoré slúžia čiastkové fiktívne agendy FA-2, FA-3,...

e) informačné systémy sú prevádzkované na niekoľkých počítačových systémoch, ktoré sú spojené vnútornou počítačovou sieťou,

f) počítačové systémy, na ktorých sú prevádzkované informačné systémy CR, IS-2, IS-3,... sú sústredené vo výpočtovom stredisku a zamestnanci k nim pristupujú pomocou vnútornej siete a osobných počítačov,

g) všetky informačné systémy FÚ a osobné počítače zapojené do vnútornej siete, na ktorých sa spracováva agenda FÚ tvoria informačný systém FÚ (IS FÚ),

h) v IS FÚ sa spracovávajú citlivé údaje, osobné údaje, ekonomické údaje, ale nie utajované skutočnosti

i) informačný systém, v ktorom sa spracovávajú utajované skutočnosti je izolovaný od ostatných systémov FÚ

j) IS FÚ je pripojený na Internet aj na neverejnú sieť

k) FÚ poskytuje informácie a služby štátnym orgánom, súkromným a verejným inštitúciám, občanom, zahraničným subjektom

l) FÚ

[37] Fiktívny úrad využijeme aj v ďalších príkladoch

   a) poskytuje informácie anonymným používateľom prostredníctvom webovej stránky,
   b) komunikuje s klientmi pomocou elektronickej pošty
   c) poskytuje transakčné služby pomocou vlastného portálu

m) FÚ sa delí na sekcie, každú sekciu vedie riaditeľ, FÚ vedie generálny riaditeľ (GR)

n) GR má útvar GR, do ktorého patrí aj bezpečnostný manažér FÚ

o) GR a riaditelia sekcií tvoria vedenie FÚ

p) Bezpečnostnú politiku prerokováva a schvaľuje vedenie FÚ

q) FÚ má sekciu IT, ktorá sa stará o prevádzku IKT FÚ,

r) vlastníkmi IS, v ktorých sa spracovávajú jednotlivé agendy sú riaditelia sekcií zodpovední za príslušné agendy (personálna, ekonomická, FA-1,...)

s) FÚ má jedného špecialistu na kybernetickú a informačnú bezpečnosť, ktorým je manažér KIB FÚ. Každá sekcia má zamestnanca, ktorý plní úlohy v KIB pre danú sekciu. Týchto zamestnancov budeme nazývať manažérmi KIB sekcií. Ich činnosť v KIB riadi manažér KIB FÚ.

t) FÚ má ustanovenú osobu zodpovednú za ochranu osobných údajov.

Bezpečnostná politika Fiktívneho úradu

Existuje viacero legislatívnych a štandardizačných dokumentov upravujúcich obsah Bezpečnostnej politiky. Vzhľadom na to, že sme pri popise manažmentu informačnej bezpečnosti v organizácii v tejto kapitole vychádzali z medzinárodných noriem ISO, budeme sa pri tvorbe bezpečnostnej politiky pridržiavať normy ISO/IEC 27002. Vytvoríme stručnú bezpečnostnú politiku, ktorá predpokladá vytvorenie ďalších dokumentov (špecializovaných bezpečnostných politík alebo bezpečnostných štandardov FÚ). Dobrý príklad podrobnejšej bezpečnostnej politiky čitateľ nájde v Bezpečnostnej politike MV SR[38]. Nasledujúci text je usporiadaný takto:

- najprv je uvedená konkrétna požiadavka normy ISO/IEC 27002 (Príloha 3.12.4., Obsah Bezpečnostnej politiky),
- potom je kurzívou uvedený text Bezpečnostnej politiky FÚ, ktorým je naplnená daná požiadavka (v hranatej zátvorke je uvedené, čo treba konkretizovať),
- napokon je uvedený komentár k predchádzajúcej časti Bezpečnostnej politiky FÚ.

[38] Nariadenie Ministerstva vnútra Slovenskej republiky z 23. marca 2012, o bezpečnostnej politike Ministerstva vnútra Slovenskej republiky pre oblasť informačných systémov

Bezpečnostná politika Fiktívneho úradu s komentármi

> deklaráciu vedenia organizácie o význame ochrany informácie, identifikácii hlavných aktív a stanovení cieľov kybernetickej a informačnej bezpečnosti v organizácii a podpore vedenia organizácie pri ich napĺňaní,

Vedenie Fiktívneho úradu, ďalej len FÚ, považuje informácie za kľúčový zdroj, bez ktorého FÚ nemôže plniť svoje poslanie. Je si vedomé významu informácií, systémov, pomocou ktorých sa spravovávajú, povinností, ktoré mu vyplývajú zo zákonov ***[vymenovať zákony]****, hrozieb, ktoré môžu narušiť spracovanie informácií vo FÚ a dôsledkov, ktoré by naplnenie týchto hrozieb mohlo mať (pre FÚ aj SR). Kľúčovými aktívami FÚ z hľadiska informačnej bezpečnosti sú*

1. *aktíva IS FÚ (hardvér, programové vybavenie, databázy, aplikácie, sieťový a komunikačný softvér)*
2. *údaje, ktoré sa v IS FÚ spracovávajú,*
3. *zamestnanci, ktorí sa starajú o prevádzku IS FÚ,*
4. *zamestnanci, ktorí vykonávajú činnosti na plnenie agendy FÚ pomocou IS FÚ,*
5. *komunikačná infraštruktúra,*
6. *podporná technická infraštruktúra IS FÚ,*
7. *finančné zdroje FÚ a*
8. *dobré meno FÚ.*

Vedenie FÚ považuje dosiahnutie a udržanie dostatočnej úrovne kybernetickej a informačnej bezpečnosti vo FÚ za nevyhnutný predpoklad toho, aby FÚ mohlo plniť svoje úlohy, stanovuje dosiahnutie a udržanie dostatočnej úrovne informačnej bezpečnosti vo FÚ svoju prvoradú prioritu a za povinnosť každého zamestnanca FÚ (vrátane vedúcich zamestnancov) podieľať sa primerane svojmu pracovnému zariadeniu na zaistení informačnej bezpečnosti FÚ. Základné ciele FÚ v oblasti kybernetickej a informačnej bezpečnosti sú

1. *dodržiavanie zákonov a iných všeobecne záväzných právnych predpisov a z nich vyplývajúcich povinností FÚ v oblasti kybernetickej a informačnej bezpečnosti,*
2. *zabezpečenie nepretržitej spoľahlivej prevádzky IS FÚ,*
3. *poskytovanie spoľahlivých a dôveryhodných služieb zamestnancom FÚ a iným oprávneným osobám v stanovenom rozsahu a kvalite aj v prípade narušenia IS FÚ,*
4. *minimalizácia rizík ohrozenia aktív IS FÚ,*
5. *minimalizácia finančných strát v dôsledku narušenia informačných aktív FÚ,*
6. *ochrana dobrého mena FÚ.*

Vedenie FÚ sa zaväzuje/je pripravené na dosiahnutie vyššie uvedených cieľov vo FÚ vytvárať primerané podmienky.

Komentár.

Bezpečnostná politika musí mať vo FÚ dostatočnú váhu. Preto musí obsahovať časť, ktorá všeobecne definuje význam kybernetickej a informačnej bezpečnosti pre FÚ. Vhodné miesto na všeobecnú deklaráciu je úvodná časť bezpečnostnej politiky.

Všimnime si, že preambula obsahuje

1. deklaráciu kybernetickej a informačnej bezpečnosti ako prioritnej úlohy, ktorú bude vedenie organizácie presadzovať
2. deklaráciu povinnosti zamestnancov podieľať sa na zaistení kybernetickej a informačnej bezpečnosti
3. prísľub vedenia vytvárať pre stanovené úlohy aj podmienky

Tieto deklarácie tvoria všeobecný rámec, ktorý bude potrebný v bezpečnostnej politike, alebo dokumentoch, ktoré na ňu nadväzujú, podrobnejšie rozpracovať.

Zmyslom existencie FÚ je to, že vykonáva funkcie, ktoré sú potrebné pre chod spoločnosti. Na vykonávanie týchto funkcií potrebuje spracovávať nejaké údaje. Tieto sme v prípade FÚ rozdelili na referenčné údaje, ktoré spracováva v Centrálnom registri a ostatné údaje.

Ostatné údaje môžu súvisieť priamo s poslaním, ktoré FÚ plní voči spoločnosti, alebo jeho vnútorným chodom (mzdová, osobná agenda, prevádzka IKT, správa budov a pod.)

Kľúčovými aktívami sú tie, bez ktorých by FÚ nebol schopný plniť svoje (spoločenské) poslanie. Dajú sa určiť tak, že sa preberú jednotlivé aktíva FÚ a overí sa, či by FÚ mohol plniť svoje poslanie pri výpadku jednotlivých aktív. Aktíva sa dajú rozdeliť na aktíva IS FÚ (technické prostriedky, programové vybavenie, databázy, aplikácie, údaje, vnútorná sieť), aktíva potrebné na činnosť IS FÚ (obslužný personál, používatelia, priestory, infraštruktúra) a ostatné, ktoré sa priamo nedajú zaradiť do predchádzajúcich kategórií (finančné prostriedky, organizačná štruktúra organizácie, budovy, dobré meno organizácie a pod.)

Pri vymenovaní kľúčových aktív v bezpečnostnej politike nemožno ísť do veľkých podrobností. Bezpečnostná politika je vysokoúrovňový dokument, ktorý by mal mať dlhodobú platnosť a meniť by sa mal len pri veľkých zmenách (napr. zmena poslania, organizačnej štruktúry FÚ). Podrobnejšiu inventarizáciu aktív bude potrebné spraviť pri analýze rizík a možnosť prehodnotiť aktíva organizácie dáva aj audit.

Ďalšou povinnou časťou Bezpečnostnej politiky podľa normy ISO/IEC 27002 je stanovenie bezpečnostných cieľov FÚ. V Bezpečnostnej politike je vhodné stanoviť ich všeobecne tak, aby pokrývali bezpečnostné potreby FÚ; zabezpečiť spoľahlivé fungovanie IS FÚ tak, aby FÚ mohol plniť svoje funkcie, chránil svoje dobré meno a jeho IS fungoval v súlade so zákonmi.Tieto ciele bude potrebné konkretizovať; napr. spoľahlivá prevádzka IS znamená o.i. zaistenie primeraného prostredia pre IS FÚ, kvalifikovanú obsluhu, ochranu prístupu pred nepovolanými osobami, dostatočnú úroveň bezpečnostného povedomia zamestnancov a pod.

vymedzenie oblasti použiteľnosti danej bezpečnostnej politiky (z čoho bezpečnostná politika vychádza a na čo všetko sa vzťahuje),

Tento dokument je Bezpečnostnou politikou Fiktívneho úradu (ďalej len FÚ). Vzťahuje sa na všetky informácie, ktoré FÚ spracováva v papierovej, elektronickej alebo inej forme, na všetky informačné a komunikačné zariadenia a iné prostriedky, prostredníctvom ktorých sa informácia FÚ spracováva a na všetkých zamestnancov FÚ a v primeranej miere aj na zamestnancov tretích strán a občanov/klientov, ktorí k týmto informáciám majú prístup. Bezpečnostná politika je vypracovaná v súlade s požiadavkami ***[Zákona o ITVS, Zákona o ochrane osobných údajov, Zákona o kritickej infraštruktúre, Zákona o kybernetickej bezpečnosti, iného zákona]*** *a nevzťahuje sa na utajované skutočnosti. Bezpečnostná politika tiež zohľadňuje platné normy a bezpečnostné požiadavky vyplývajúce zo zmluvných záväzkov FÚ.*

Komentár.

Ďalšia časť Bezpečnostnej politiky stanovuje oblasť jej pôsobenia, t.j. na čo sa bezpečnostná politika FÚ vzťahuje. V pokračovaní úvodnej časti sa vymedzuje rozsah pôsobnosti Bezpečnostnej politiky. V uvedenom príklade je rozsah pôsobnosti maximálny. Výnimkou sú utajované skutočnosti, ktoré si vyžadujú inú úroveň ochrany, iné typy opatrení (personálnych, režimových) a preto sa spravidla spracovávajú v oddelenom systéme. Všimnite si, že nezávisí na forme, v akej sa informácia vo FÚ vyskytuje; ak si informácia zasluhuje ochranu, tak je potrebné ju chrániť v priebehu celého jej životného cyklu, bez ohľadu na to, v akej forme je zaznamenaná. Spracovanie informácie (resp. údajov, v podobe ktorých je informácia zaznamenaná) znamená spracovanie v širokom zmysle, t.j. získavanie/vytváranie, prenos, transformáciu, uchovávanie, využívanie, archivovanie, ničenie informácie. Takto definovaný rozsah bezpečnostnej politiky znamená, že sa bezpečnostná politika vzťahuje na IS FÚ a jeho okolie, t.j. tie subjekty, objekty a vzťahy v FÚ, ktoré majú vplyv na bezpečnosť IS FÚ. Všeobecnejšia definícia oblasti pôsobnosti bezpečnostnej politiky by už zahrnula celý FÚ, vrátane činností a aspektov, ktoré bezpečnosť IS a jeho aktív ovplyvňujú len sprostredkovane. Pri formulovaní bezpečnostnej politiky by pomohlo, keby FÚ mal vytvorený ISMS (Information security management system, Systém riadenia informačnej bezpečnosti), pretože ak by ho mal, bezpečnostná politika by sa oň mohla oprieť.

Bezpečnostná politika tiež deklaruje súlad s normami (zmyslom toho je kompatibilita bezpečnostnej úrovne IS FS s porovnateľnými systémami a interoperabilita). Zohľadnenie bezpečnostných požiadaviek je obojstranné, na jednej strane predpokladá, že ak FÚ uzatvára zmluvu napr. o poskytovaní služieb s nejakou treťou stranou, tak požiadavky tejto zmluvy nemôžu byť v rozpore s bezpečnostnou politikou FÚ; t.j. FÚ nesmie porušiť bezpečnostné požiadavky tretej strany a nesmie pripustiť, aby spolupráca s treťou stranou narušila bezpečnosť IS FS. Tieto záväzky sa musia premietnuť do zmlúv s dodávateľmi, resp. poskytovateľmi služieb.

> štruktúru bezpečnostných dokumentov nadväzujúcich na danú bezpečnostnú politiku a ich obsah (špeciálne bezpečnostné politiky, alebo bezpečnostné štandardy, bezpečnostné praktiky - aké oblasti pokrývajú a akou formou budú vydané)

Všeobecné ustanovenia Bezpečnostnej politiky FÚ sú/budú podrobnejšie rozpracované v Bezpečnostných štandardoch FÚ[39]*. Postup pri uplatňovaní bezpečnostných požiadaviek Bezpečnost-*

[39]Bezpečnostné štandardy sú k Bezpečnostnej politike v podobnom vzťahu ako vykonávacie predpisy ku zákonu.

ných štandardov v konkrétnych podmienkach bude rozpracovaný v Bezpečnostných praktikách. FÚ vydá formou záväzných dokumentov Bezpečnostné štandardy pre oblasti

1. *riadenia kybernetickej a informačnej bezpečnosti*
2. *personálnej bezpečnosti*
3. *fyzickej a objektovej bezpečnosti*
4. *bezpečnosti prevádzky*
5. *klasifikácie informácie*
6. *ochrany prístupu*
7. *spolupráce s externými subjektmi*
8. *komunikácie prostredníctvom Internetu a Neverejnej siete*
9. *havarijného plánovania a plánovania kontinuity činnosti*
10. *obstarávania a vývoja systémov*
11. *vytvárania bezpečnostného povedomia a vzdelávania v KIB*

Komentár.

Bezpečnostná politika FÚ je len základom bezpečnostnej dokumentácie FÚ. Ak má byť dlhodobo platná, nemôže zachádzať do podrobností, ktoré podliehajú zmenám. Na druhej strane, na zaistenie požadovanej úrovne kybernetickej a informačnej bezpečnosti vo FÚ všeobecné deklarácie nestačia. Preto ciele, povinnosti a vzťahy definované Bezpečnostou politikou musia byť rozpracované podrobnejšie. V Bezpečnostnej politike sú definované oblasti, ktoré FU považuje za tak dôležité z bezpečnostného hľadiska, že sa nimi bude zaoberať podrobnejšie. V Bezpečnostnej politike FÚ sú uvedené oblasti podľa normy ISO/IEC 27002.

> stanovenie zodpovednosti zamestnancov organizácie za presadzovanie a dodržiavanie bezpečnostnej politiky (a dokumentov na ňu nadväzujúcich)

Každý zamestnanec, ktorý pracuje s IS FÚ, alebo nejakým spôsobom ovplyvňuje jeho činnosť, je povinný oboznámiť sa s Bezpečnostnou politikou, dodržiavať jej ustanovenia a konať tak, aby nenarušil bezpečnosť IS FÚ. Podľa postavenia vo FÚ a vzťahu k IS FÚ sú jednotliví zamestnanci FÚ zaradení do niektorej z nasledujúcich rôl:

- *vedúci zamestnanec*
- *informatik*
- *manažér/špecialista KIB*
- *používateľ*

Vedúci zamestnanci a manažér KIB sú do rôl zaradení na základe funkcií, ktorú vo FÚ vykonávajú, ostatných zamestnancov zaraďuje do rolí riaditeľ sekcie (v prípade útvaru GR, generálny riaditeľ), do pôsobnosti ktorého patria, na základe ich pracovnej náplne. Riaditeľ, ktorý zamestnanca do roly zaradil, je povinný pri zmene pracovného zaradenia prehodnotiť aj zaradenia zamestnanca do roly. Každý zamestnanec musí mať v pracovnej zmluve stanovený aj záväzok dodržiavať Bezpečnostnú politiku. FÚ pri zaradení zamestnanca do roly zabezpečí jeho preškolenie na úrovni, zodpovedajúcej roly, do ktorej bol zaradený a zaradí ho do pravidelného vzdelávania KIB.

Komentár.

Aby si zamestnanec mohol plniť svoje pracovné povinnosti pomocou IS FÚ a nenarušil pritom jeho bezpečnosť, musí vedieť, čo a ako má robiť. Školiť zvlášť každého zamestnanca a individuálne mu stanoviť oprávnenia by bolo časovo náročné a zbytočné. Vo FÚ existujú skupiny zamestnancov, ktorí majú zhruba rovnaké požiadavky na IF FÚ a oprávnenia vo vzťahu k IS FÚ. Zamestnancov s rovnakými potrebami a postavením voči IS FÚ zaradíme do tej istej bezpečnostnej roly. Keďže vo FÚ je potrebné rozlišovať len 4 základné roly, stanovovanie oprávnení pre činnosť v IS FÚ, školenia zamestnancov sa vo FÚ výrazne zjednodušia. Bezpečnostná politika definuje aj spôsob zaraďovania zamestnancov do rolí a stanovuje zodpovedným zamestnancom povinnosť prehodnotiť v prípade potreby zaradenie zamestnanca. Plnenie povinností v informačnej bezpečnosti považuje FÚ za tak dôležité, že každého zamestnanca bude pravidelne vzdelávať primerane jeho potrebám a tieto povinnosti explicitne uvedie v jeho pracovnej náplni/zmluve. Takýto písomný záväzok je dôležitý napr. v prípade, keby sa vo FÚ uplatňovala prísna ochrana dôvernosti údajov a v Bezpečnostnej politike by bolo uvedené ustanovenie, že zamestnanec môže používať zdroje FÚ, vrátane Internetu a elektronickej pošty len na pracovné účely. V takom prípade by prezeranie stránok na Internete, posielanie súkromných mailov z úradnej adresy (zistiteľné bez čítania obsahu) bolo možné kvalifikovať ako porušenie pracovnej disciplíny a vyvodzovať z toho voči zamestnancovi dôsledky.

klasifikáciu informácie (na základe čoho sa bude informácia v organizácii klasifikovať)

FÚ vypracuje a zavedie do používania klasifikačnú schému pre klasifikáciu údajov a systémov. Klasifikačnými kritériami pre klasifikáciu údajov sú dôvernosť, integrita, dostupnosť a autentickosť. Úroveň bezpečnostnej klasifikácie informácie závisí od závažnosti dôsledkov, ktoré môže mať narušenie dôvernosti, integrity, dostupnosti a autentickosti údajov. Bezpečnostná klasifikácia systému je daná maximálnymi požiadavkami na ochranu dôvernosti, integrity, dostupnosti a autentickosti všetkých údajov, ktoré sa v ňom spracovávajú. GR a riaditelia sekcií zabezpečia, aby boli všetkým aktívam, ktoré sú v ich pôsobnosti a sú nevyhnutné pre činnosť FÚ, priradení vlastníci. Vlastníci aktív spolu s manažérom KIB klasifikujú aktíva a zabezpečia im ochranu primeranú ich klasifikácii.

Komentár.

Klasifikácia údajov a systémov je prostriedkom ako zredukovať námahu pri stanovovaní bezpečnostných požiadaviek na ochranu údajov a systémov a zaistiť porovnateľnú úroveň ochrany

aktív, ktoré majú rovnaké bezpečnostné potreby. Bezpečnostná politika FÚ definuje štyri základné bezpečnostné požiadavky na ochranu informácie. Informácia sa nebude klasifikovať po položkách, ale po typoch (napr. ekonomické údaje, osobné údaje, utajované skutočnosti, zverejnené údaje a pod.) a pre každý typ informácie sa definujú potreby jej ochrany z hľadiska dôvernosti, integrity, dostupnosti a autentickosti. Klasifikácia informácií a systémov vychádza z amerických štandardov FIPS 199 a 200 a je podrobne popísaná v ďalšej prílohe tejto kapitoly. Bezpečnostná politika FÚ zároveň definuje, kto by mal klasifikovať informácie a systémy. Podrobnosti bude upravovať bezpečnostný štandard.

spôsob analýzy rizík a hranica akceptovateľného rizika,

Pri analýze rizík vyplývajúcich z hrozieb voči aktívam IS FÚ sa postupuje podľa normy ISO/IEC 27005. Riziká sa hodnotia kvalitatívne na štvorstupňovej škále (nulové, nízke, stredné, vysoké). Pre FÚ je hranica akceptovateľného rizika stanovená na úrovni „nízke riziko“.

Komentár.

Uvedená ISO norma je venovaná správe rizík a podrobne popisuje analýzu rizík. Bezpečnostná politika konkretizuje, že vo FÚ sa bude robiť kvalitatívna analýza rizík a že FÚ považuje stredné a vysoké riziko za neprijateľné. Pri analýze rizík podľa ISO/IEC 27005 vo FÚ bude potrebné vyriešiť aj iné problémy, o ktorých sa v Bezpečnostnej politike nehovorí (napr. granularita=úroveň podrobnosti pri definovaní aktív, výber hrozieb, ohodnotenie dopadu a i.)

monitoring, kontrola, audit IKS,

Každý vlastník aktív je povinný kontrolovať stav aktív, za ktoré zodpovedá a účinnosť opatrení, prijatých na ich ochranu. Prístup k citlivým údajom FÚ a iné bezpečnostne relevantné aktivity v IS FÚ sú viazané na predchádzajúcu úspešnú identifikáciu a autentizáciu osoby, overenie toho, či má na prístup k údajom či iné aktivity v IS FÚ oprávnenie; sú monitorované technickými a logickými prostriedkami a je o nich vytváraný záznam auditu. K záznamu auditu nemajú prístup osoby, ktoré činnosti dokumentované v záznamoch auditu vykonávali. Záznamy auditu kontroluje audítor. Pri konfigurovaní, spúšťaní, údržbe systému a iných zásahoch do centrálneho registra musia byť prítomní aspoň dvaja operátori/správcovia systému a o vykonaných zásahoch musia vyhotoviť záznam. Manažér KIB kontroluje stav a úroveň ochrany IS FÚ.

Komentár.

Cieľom takto definovaných povinností je zaistiť, aby boli pokryté všetky zraniteľnosti, aby boli bezpečnostné opatrenia poriadne implementované a správne používané a aby sa dokumentovali udalosti, pri ktorých môže dôjsť k bezpečnostnému incidentu. Bezpečnostná politika rieši aj kontrolu činnosti privilegovaných používateľov (princíp štyroch očí), oddelenie právomocí (správca systému, audítor), ochranu záznamov auditu pred narušením zo strany privilegovaného používateľa a definuje kontrolu ako povinnosť manažéra KIB.

riešenie bezpečnostných incidentov,

Riešenie bezpečnostných incidentov vo FÚ riadi/koordinuje manažér KIB FÚ. Každý zamestnanec organizácie je povinný nahlásiť [svojmu priamemu nadriadenému, manažérovi KIB sekcie, manažérovi KIB FÚ] bezpečnostný incident vo FÚ, hneď, ako spozoroval jeho príznaky. Rovnako je každý zamestnanec povinný oznámiť ***[svojmu priamemu nadriadenému, manažérovi KIB sekcie, manažérovi KIB FÚ]*** *odhalenú, predtým neznámu zraniteľnosť aktíva IS FÚ. Každý zamestnanec je povinný v prípade potreby pomôcť pri riešení bezpečnostného incidentu, riadiac sa pri tom pokynmi manažéra KIB (FÚ alebo sekcie). Manažér KIB FÚ vyhodnocuje hlásenia o bezpečnostných incidentoch, koordinuje alebo priamo riadi ich riešenie, informuje dotknuté osoby (vrátane CSIRT.sk, operátorov, prípadne polície). Po uzavretí bezpečnostného incidentu je manažér KIB FÚ/sekcie povinný vyhotoviť záznam o bezpečnostnom incidente, v prípade závažného incidentu analyzovať príčiny a priebeh bezpečnostného incidentu, účinnosť prijatých opatrení, informovať o zistených skutočnostiach [riaditeľa sekcie, ak išlo o lokálny incident, GR, ak išlo o incident zasahujúci celý FÚ] a v prípade potreby navrhnúť úpravu alebo doplnenie bezpečnostných opatrení; v závažných prípadoch navrhnúť (manažér KIB FÚ) aj revíziu Bezpečnostnej politiky FÚ. Ak bezpečnostný incident spôsobil nedbanlivosťou alebo úmyselne zamestnanec FÚ, manažér KIB FÚ/sekcie, dá podnet na začatie disciplinárneho konania voči tomuto zamestnancovi. Informácie o bezpečnostných incidentoch vo FÚ sú považované za citlivé informácie a zamestnanci FÚ sú povinní zachovávať mlčanlivosť. O rozsahu informácií o bezpečnostnom incidente vo FÚ, ktoré FÚ poskytne verejnosti, čase a spôsobe zverejnenia informácií rozhoduje GR FÚ.*

Komentár.

Niektoré bezpečnostné incidenty zistia skôr zamestnanci ako manažéri KIB. (Možno aj preto, že niektoré z nich sami spôsobili.) V záujme FÚ je zistiť čo najskôr, že sa vyvíja nejaký bezpečnostný incident, pretože ak zasiahne včas, tak sa mu možno podarí incident lokalizovať a minimalizovať jeho negatívne dopady. Vo FÚ sa informácia o všetkých bezpečnostných incidentoch posiela manažérovi KIB FÚ. Toto riešenie má tú výhodu, že je možné stanoviť priority pri súčasnom výskyte viacerých bezpečnostných incidentov, odhaliť súvislosti medzi zdanlivo nezávislými incidentmi a koordinovať postup pri ich riešení. Nevýhodou môže byť zahltenie bezpečnostného manažéra FÚ nepodstatnými informáciami a oneskorené riešenie bezpečnostných incidentov. Namiesto takého centralistického riešenia by mohli byť incidenty nahlasované (a aj riešenie zabezpečené) podľa charakteru a závažnosti incidentu (prasknuté vodovodné potrubie - správa budov, alebo externá havarijná služba). O závažných bezpečnostných incidentoch by mal byť informovaný manažér KIB FÚ aj v prípade, ak sa jeho účasť pri riešení nevyžaduje. (Problémom je stanoviť hranicu medzi závažnými a nepodstatnými incidentmi). Incident môže zasiahnuť celý FÚ a mať negatívne dôsledky pre tretie osoby. Aby sa minimalizoval dopad incidentu na dotknuté osoby, FÚ je povinný poskytnúť im informácie potrebné na to, aby ochránili svoje systémy a informačné aktíva pred dopadmi bezpečnostného incidentu vo FÚ. Bezpečnostné incidenty signalizujú, že ochrana FÚ nie je dostatočná, alebo jeho zamestnanci nevedia, čo majú robiť a preto robia chyby, alebo sa FÚ stal terčom cielených útokov. Ani jedna z týchto možností nie je pre FÚ priaznivá a preto musí manažér KIB FÚ analyzovať závažné a evidovať nepodstatné bezpečnostné incidenty, aby dokázal zistiť ich príčinu a navrhnúť potrebné riešenia. Tieto môžu viesť až ku zmenám bezpečnostnej politiky FÚ.

Ak je pôvodcom bezpečnostných incidentov zamestnanec FÚ, manažér KIB FÚ (v prípade potreby aj za pomoci externého experta) musí pripraviť podklady pre disciplinárne konanie

voči pôvodcovi bezpečnostného incidentu. Podobne v prípade, keď sa podarí jednoznačne identifikovať externého útočníka a FÚ naň podá trestné oznámenie.

Bezpečnostné incidenty vzbudzujú veľkú pozornosť médií a verejnosti. Ich rozmazávanie v bulvárnych médiách nepomôže zvýšiť bezpečnosť IS FÚ, ale môže ohroziť dobré meno FÚ. Preto Bezpečnostná politika stanovuje spôsob, ako informovať verejnosť o bezpečnostnom incidente vo FÚ, aby sa minimalizovala negatívna publicita.

Riešenie bezpečnostných incidentov môže byť v Bezpečnostnej politike popísané aj podstatne stručnejšie (základné povinnosti zamestnanca, manažéra KIB pri riešení bezpečnostných incidentov, vyhodnotenie bezpečnostných incidentov, informovanie vedenia, verejnosti, dôsledky pre pôvodcu bezpečnostného incidentu a pod.) a podrobnosti budú popísané v štandarde FÚ pre riešenie bezpečnostných incidentov vo FÚ.

zaistenie kontinuity činnosti IKS organizácie,

Údaje a systémy FÚ sú klasifikované aj z hľadiska dostupnosti. Všetky informácie potrebné pre činnosť FÚ (operačné systémy, databázy, programové vybavenie IS FÚ, údaje a i.) sú pravidelne zálohované. Frekvencia a spôsob vytvárania záloh, uchovávanie záloh musí umožniť obnovenie činnosti FÚ podporovanej IS FÚ do času stanoveného pri klasifikácii informácií a systémov. Zálohovanie údajov a programového vybavenia musí byť vykonávané tak, aby sa minimalizoval jeho vplyv na činnosť IS FÚ. Zálohované údaje a programové vybavenie musia byť uložené mimo priestorov, v ktorých je umiestnený IS FÚ a musia byť chránené na úrovni zodpovedajúcej ich klasifikácii. Pre tie systémy IS FÚ, ktoré si vyžadujú nepretržitú prevádzku, FÚ vytvorí záložné kapacity na pracovisku v meste NN. FÚ vypracuje a zavedie havarijné plány a plány obnovy činnosti pre kľúčové komponenty IS FÚ.

Komentár.

Vytváranie a udržiavanie záložných kapacít FÚ je nákladné. Časté zálohovanie všetkých systémov a údajov môže obmedzovať výkonnosť IS FÚ a odčerpáva kapacity FÚ. Preto je rozsah, frekvencia a spôsob zálohovania (plné zálohy, inkrementálne) odvodený od cieľa, ktorý FÚ chce dosiahnuť s tými zdrojmi, ktoré má k dispozícii. (Stanovenie priorít aj pre zálohovanie). Kópie údajov slúžia na to, aby bolo možné obnoviť systémy a údaje, ktoré boli poškodené pri bezpečnostnom incidente, alebo na spustenie náhradnej prevádzky. Pri rozsiahlom bezpečnostnom incidente (požiar, záplava) by mohli byť poškodené aj záložné kópie, preto ich je potrebné uchovávať na mieste, ktoré je fyzicky dostatočne vzdialené od sídla FÚ. Záložné kópie obsahujú údaje s rovnakou klasifikáciou ako originálne údaje, preto by mali byť aj chránené na rovnakej úrovni, ako originálne údaje. Záložné kópie musia byť testované na to, či sa z nich dá systém a údaje obnoviť. Zvládnutie havárie, prírodnej pohromy si vyžaduje cieľavedomý koordinovaný postup, ktorý sa nedá vymyslieť a realizovať v okamihu negatívnej udalosti. Tam, kde by výpadok alebo narušenie systémov mohlo mať pre FÚ neprijateľné následky, sa musí FÚ pripraviť (materiálne, technicky, organizačne, personálne) na riešenie kritickej situácie. Havarijné plány rozoberajú možné scenáre katastrof a konanie FÚ v jednotlivých prípadoch (cieľom je ochrana životov, zdravia osôb a minimalizácia strát FÚ) a plány obnovy obnovenie činnosti FÚ.

správa bezpečnostnej politiky (ako často sa budú robiť pravidelné a z akých dôvodov mimoriadne revízie bezpečnostnej politiky).

Bezpečnostná politika FÚ je platná od 15.10.2020 a účinná od 1.1.2021. GR FÚ každoročne do 1. marca predloží vedeniu FÚ správu o stave informačnej bezpečnosti vo FÚ za predchádzajúci rok a prípadný návrh na zmeny Bezpečnostnej politiky FÚ. Ak sa v priebehu roka vyskytnú vážne dôvody na zmeny Bezpečnostnej politiky (zmena organizačnej štruktúry FÚ, nové povinnosti FÚ vyplývajúce z legislatívy, veľké zmeny IS FÚ, závažné bezpečnostné incidenty a pod.), GR FÚ predloží návrh na úpravy Bezpečnostnej politiky FÚ na najbližšom zasadnutí vedenia FÚ.

Komentár.

FÚ potrebuje aktuálnu bezpečnostnú politiku, ktorá bude reflektovať skutočný stav KIB FÚ, podmienok vo FÚ, požiadaviek na FÚ a hrozieb voči aktívam FÚ. Preto je v samotnej Bezpečnostnej politike FÚ definovaný postup pravidelného aj mimoriadneho posudzovania Bezpečnostnej politiky. Aby mala Bezpečnostná politika FÚ primeranú váhu, jej „vlastníkom“ je vedenie, resp. GR FÚ. Reálne sa však o správu Bezpečnostnej politiky FÚ stará manažér KIB FÚ.

Literatúra

[1] *BSI Standard 100-2 IT-Grundschutz Methodology, v.1.0.* Bonn: Bundesamt fűr Sicherheit in der Informationstechnik, 2005 (citované na stranách: 20, 21, 23, 24, 54).

[2] *BSI Standard 100-3 Risk Analysis based on IT-Grundschutz, v.2.0.* Bonn: Bundesamt fűr Sicherheit in der Informationstechnik, 2005 (citované na strane 54).

[3] *Common Vulnerabilities and Exposures.* 2019. URL: https://cve.mitre.org/data/downloads/index.html (citované na strane 47).

[4] *FIPS 199 Standards for Security Categorization of Federal Information and Information Systems,* U.S. Department of commerce & NIST, 2003 (citované na stranách: 27, 54–56).

[5] *FIPS 200 Minimum Security Requirements for Federal Information and Information Systems.* U.S. Department of commerce & NIST, 2006 (citované na stranách: 54, 56).

[6] *ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls.* Angl. 2. vyd. ISO a IEC, okt. 2013. 80 strán (citované na stranách: 21, 29, 32, 41, 52).

[7] *ISO/IEC 27005:2018 Information technology – Security techniques – Information security risk management.* Angl. 3. vyd. ISO a IEC, júl 2018. 56 strán (citované na stranách: 22, 27–29, 47).

[8] *ISO/IEC 27008 Information technology – Security techniques – Guidelines for auditors on information security management systems controls.* ISO (citované na strane 33).

[9] *Information Security Training Requirements: A Role- and Performance-Based Model.* NIST Special publications 800-16r1. Draft. Washington: U.S. Government Printing Office, 2014 (citované na strane 21).

[10] *Security and Privacy Controls for Federal Information Systems and Organizations.* NIST Special publications 800-53. Draft. Washington: U.S. Government Printing Office, 2017 (citované na stranách: 32, 41, 54).

[11] Stoneburner, G., Goguen. A. a Feringa, A. *Risk Management Guide for Information Technology Systems*. NIST Special publications 800-30. Washington: U.S. Government Printing Office, 2001 (citované na stranách: 30, 47).

[12] *Assessing Security and Privacy Controls in Federal Information Systems and Organizations, Building Effective Assessment Plans*. NIST Special publications 800-53a. Draft. Washington: U.S. Government Printing Office, 2014 (citované na strane 54).

[13] *Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z.z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy*. 2020 (citované na stranách: 17, 36, 54, 57).

[14] *Zákon č. 95/2019 Z.z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov*. 2019 (citované na stranách: 17, 19).

Kapitola 4

Architektúry a modely informačných systémov

Jaroslav Janáček

Informačné systémy, či už ide o malé informačné systémy prevádzkované na jednom počítači alebo komplexné distribuované systémy, sa skladajú z viacerých významných komponentov. Veľká časť týchto komponentov nie je špecifických pre konkrétny informačný systém, ale má všeobecný charakter. Ich úlohou je poskytnúť iným komponentom rôzne služby pomocou svojich rozhraní. Príkladom takých všeobecných komponentov je hardvér a operačný systém. Takýto prístup má viacero výhod, napr.:

- Nie je potrebné pre každý informačný systém nanovo vymýšľať riešenie pre štandardné problémy, keďže štandardné problémy typicky rieši nejaký štandardný komponent a riešenie poskytuje ako svoju službu.
- Rôzne informačné systémy môžu zdieľať všeobecné komponenty, čo umožňuje napr. použitie toho istého počítača na rôzne účely – nemusíme kvôli novému informačnému systému vždy obstarať aj nový hardvér.
- Ak sa zachová rozhranie, je možné jednotlivé komponenty nahradiť inými bez toho, aby to malo vplyv na iné časti systému. Napr. aplikačné programy pristupujú k údajom uloženým na disku prostredníctvom služieb operačného systému, ktorý pre ukladanie údajov poskytuje abstrakciu – súbory. Keď zmeníme spôsob uloženia údajov na disku, je potrebné zmeniť príslušný komponent operačného systému, no z pohľadu aplikačných programov sa nič nezmení.

Jednotlivé komponenty navzájom nevyužívajú svoje služby chaoticky, ale môžeme v nich identifikovať typicky niekoľko vrstiev. Najnižšou vrstvou je vrstva hardvéru. Súčasťou hardvéru sú, jednoducho povedané, všetky fyzické súčasti informačného systému, teda všetko, čo je možné chytiť do ruky. V hardvéri sú skutočne uložené všetky údaje, s ktorými informačný systém pracuje. V hardvéri sa tiež skutočne realizujú všetky operácie s údajmi.

Nad vrstvou hardvéru sa nachádza vrstva operačného systému. Operačný systém plní rad dôležitých úloh ako pre funkčnosť, tak aj pre bezpečnosť informačného systému. Jednou z

jeho dôležitých úloh je poskytnúť vyšším vrstvám abstrakciu rôznych častí hardvéru ako svoje služby, ktoré môžu komponenty na vyšších vrstvách využívať bez toho, aby museli poznať detaily o použitom hardvéri.

Nad vrstvou operačného systému sa nachádza aplikačná vrstva. V nej sa nachádzajú komponenty špecifické pre konkrétny informačný systém, ako aj ďalšie všeobecné komponenty – rôzne pomocné programy a tzv. knižnice. Knižnice sú komponenty využívané rôznymi programami na riešenie rôznych čiastočných problémov na aplikačnej vrstve, ktoré sa často opakujú. Takisto knižnice zvyčajne sprostredkovávajú programom jednotný prístup k službám operačného systému spôsobom, ktorý nie je závislý na konkrétnom operačnom systéme, ale môže byť spoločný pre viacero rôznych operačných systémov.

V zložitejších informačných systémoch sa často medzi aplikačnú vrstvu a vrstvu operačného systému vkladá ešte databázová vrstva. Jej úlohou je poskytnúť zložitejšie funkcie na prístup k veľkému množstvu štruktúrovaných údajov, čím komponenty na aplikačnej vrstve odbremení od problému, ako ukladať a manipulovať s veľkým množstvom údajov.

Vrstvy, ktoré sme spomenuli vyššie patria medzi najvýznačnejšie vrstvy, ktorých odlíšenie je potrebné aj z pohľadu bezpečnosti. Samé sú však často vnútorne členené na ďalšie vrstvy, alebo sa aspoň skladajú z mnohých spolupracujúcich komponentov. V nasledujúcich častiach sa podrobnejšie pozrieme na význam, štruktúru a vybrané vlastnosti jednotlivých vrstiev.

4.1 Hardvér

Hardvér informačného systému sa skladá z viacerých častí. Z laického pohľadu zvonku typicky vidíme samotný počítač a k nemu pripojené rôzne vstupné a výstupné zariadenia (klávesnica, myš, monitor, tlačiareň, skener, ...). V prípade notebookov sú viaceré tieto zariadenia spojené do jedného fyzického celku, čo umožňuje ľahšie prenášanie, no z hľadiska ich významu a funkčnosti sa prakticky nelíšia od ich samostatných verzií, ktoré poznáme zo stolných počítačov alebo serverov.

Vnútri počítača sa nachádza viacero dôležitých častí:

- základná doska (motherboard)
- procesor (CPU),
- operačná pamäť,
- pevné disky a/alebo SSD,
- CD/DVD mechaniky,
- rozširujúce karty (napr. grafická karta, sieťová karta, radič diskov, ...).

Základná doska je centrálny komponent, ktorý slúži predovšetkým na to, aby prepojil navzájom ďalšie komponenty. Na tento účel obsahuje jeden niekoľko typov tzv. *zbernice*. Zbernica je elektronický systém umožňujúci prenos príkazov a údajov medzi k nej pripojenými zariadeniami. V súčasnosti sa v bežných počítačoch stretneme najmä so zbernicami typu PCI a PCI-Express. Špeciálne zbernice sa používajú na komunikáciu medzi procesorom(mi) a pamäťou. Každá zbernica obsahuje špeciálne konektory, do ktorých sa pripájajú jednotlivé zariadenia.

Súčasťou základnej dosky sú aj ďalšie komponenty, ktoré vytvárajú rozhrania pre pripájanie iných zariadení k počítaču – či už externých (napr. klávesnice, myši, monitor, ...), alebo interných (napr. pevné disky). Na pripájanie rôznych zariadení sa používajú rôzne rozhrania. Z tých dnes najčastejšie sa vyskytujúcich môžeme spomenúť napr.:

- USB – používa sa dnes na pripájanie väčšiny externých zariadení k počítačom,
- PS/2 – staršie rozhranie na pripojenie klávesnice a myši,
- VGA, HDMI, DisplayPort – slúžia na pripojenie monitora,
- IDE, SATA – bežné rozhrania pre pripojenie diskov a CD/DVD mechaník v kancelárskych počítačoch,
- SCSI, SAS – bežné rozhrania pre pripojenie diskov a CD/DVD mechaník v serveroch.

Procesor je centrálna časť počítača, ktorá riadi celý počítač a vykonáva väčšinu výpočtov a iných operácií s údajmi. Počítač obsahuje aspoň jeden procesor, no môže ich byť aj viac. Dnešné procesory sa navyše skladajú z viacerých tzv. *jadier*, ktoré v podstate predstavujú samostatné procesory uzavreté v jednom spoločnom obale. Procesor sa vnútorne skladá z viacerých častí, z ktorých najdôležitejšie sú:

- aritmeticko-logická jednotka,
- riadiaca jednotka,
- registre.

Aritmeticko-logická jednotka procesora je sústava obvodov, ktoré realizujú elementárne aritmetické a logické operácie, ako napr. sčítanie, odčítanie, násobenie, delenie alebo porovnávanie čísel. Registre predstavujú veľmi rýchlu a malú pamäť na údaje, s ktorými môže aritemticko-logická jednotka pracovať. Riadiaca jednotka riadi činnosť procesora na základe *programu*. Program je postupnosť *inštrukcií*. Riadiaca jednotka postupne číta jednotlivé inštrukcie programu a pomocou ďalších častí procesora zabezpečuje ich vykonanie. Jednotlivé inštrukcie predstavujú pokyny na vykonanie elementárnych operácií ako napr. skopírovať údaje medzi miestom v pamäti a registrom, vykonať aritmetickú operáciu s hodnotami v dvoch registroch, začať vykonávať inú časť programu, a pod. Z takýchto elementárnych operácií sa v konečnom dôsledku skladajú všetky programy, ktoré určujú činnosť procesora, a tým aj celého informačného systému.

Aby riadiaca jednotka procesora mohla čítať a vykonávať inštrukcie programu, tieto musia byť zapísané v tzv. *strojovom kóde*. V tejto podobe majú inštrukcie podobu postupnosti čísel, podľa ktorých riadiaca jednotka rozhodne čo a s čím má spraviť. Táto podoba nie je zrozumiteľná človeku. Strojovému kódu najbližšia forma, ktorá je zrozumiteľná (príslušne kvalifikovanému) človeku je program napísaný v tzv. *jazyku assemblera*. V jazyku assemblera jednotlivým inštrukciám zodpovedajú niekoľko-písmenové skratky. V jazyku assemblera sa však bežne píšu len relatívne malé časti programov, ktoré buď obsahujú špeciálne inštrukcie, alebo pri ktorých je extrémne dôležitá napr. rýchlosť alebo presné načasovanie jednotlivých operácií. Obyčajne sa programy píšu vo *vyšších programovacích jazykoch*, ako sú napr. C, C++, C#, Java a iné. V

týchto jazykoch je možné programy písať človeku podstatne bližším štýlom, čo výrazne napomáha ich zrozumiteľnosti. Programy napísané vo vyšších programovacích jazykoch sa následne prekladajú do strojového kódu pre príslušný procesor alebo (napr. v prípade jazyka Java) do univerzálneho strojového kódu pre tzv. *interpreter*. Interpreter je program, ktorý vykonáva program zapísaný v nejakom univerzálnom strojovom kóde na konkrétnom procesore.

Operačná pamäť počítača (často nie celkom správne označovaná ako RAM) slúži na dočasné uloženie údajov a programov v počítači, aby s nimi mohol procesor pracovať. Typická veľkosť operačnej pamäte v bežných kancelárskych počítačoch a notebookoch sa v súčasnosti pohybuje na úrovni niekoľko gigabyte-ov (GB), v serveroch od niekoľkých GB po rádovo stovky GB. Údaje môžu byť uložené v operačnej pamäti len kým je počítač zapnutý, po vypnutí napájania sa postupne stratia. Z bezpečnostného hľadiska je dôležitý fakt, že strata obsahu operačnej pamäte nie je okamžitá. Pri izbovej teplote je obsah môže vydržať niekoľko sekúnd až minút, v nízkych teplotách aj niekoľko hodín.

Okrem operačnej pamäte počítač obsahuje aj pamäte, ktoré si svoj obsah zachovávajú aj bez napájania a slúžia na uloženie základných programov, ktorých úloha je po zapnutí počítača vykonať základné testy a inicializáciu jednotlivých častí počítača a následne spustiť operačný systém.

Pevné disky v počítači slúžia na trvalejšie ukladanie programov a údajov. V súčasnosti je väčšina pevných diskov založená na princípe ukladania údajov v podobe zmagnetizovaných oblastí na rotujúcej kovovej platni. Takto uložené údaje vydržia dlhodobo bez potreby napájania. Pevné disky sú však pomerne chúlostivé zariadenia, ktoré môžu byť ľahko poškodené napr. prudkými pohybmi počítača počas prevádzky disku. Keďže obsahujú pohybujúce sa mechanické časti (napr. platne otáčajúce sa rýchlosťou od 5000 do 15000 otáčok za minútu a čítacie a zapisovacie hlavy), časom sa opotrebujú a pokazia. Preto nemožno predpokladať, že údaje uložené na pevnom disku vydržia neobmedzene dlho. Z bezpečnostného hľadiska je tiež dôležité povedať, že dokonalé vymazanie údajov z pevného disku je veľmi problematické až nemožné. Aj po niekoľkonásobnom prepísaní oblasti pevného disku je stále možné pomocou špeciálnych prístrojov zrekonštruovať pôvodný obsah.

Čoraz častejšie sa dnes klasické pevné disky nahrádzajú SSD[1]. SSD neobsahujú žiadne pohyblivé časti, čo významne prispieva k ich odolnosti voči mechanickému poškodeniu. Na rozdiel od klasických pevných diskov na ich funkciu ani životnosť nemá vplyv pohybovanie s počítačom, preto sa najprv uplatnili v notebookoch a iných penosných zariadeniach. Ich ďalšou výhodou je vysoká rýchlosť zápisu a najmä čítania v porovnaní s klasickými pevnými diskami. Z tohto dôvodu sa dnes uplatňujú aj v stolných počítačoch a serveroch. Nevýhodou SSD je obmedzený počet záspisov do jedného bloku, ktorý dokážu realizovať. Základom SSD je pamäť typu flash, ktorá zvládne od niekoľko tisíc po cca stotisíc vymazaní a zápisov. Maximálny počet závisí od použitej technológie, a tá má významný vplyv aj na cenu – preto v praxi nájdeme lacné SSD určené pre bežných spotrebiteľov s malým maximálnym počtom záspisov ako aj podstatne drahšie SSD pre použitie v serveroch, ktoré vydržia väčší počet zápisov. Na zmiernenie tohto problému sa v SSD využívajú techniky na vyrovnávanie počtu zápisov do jednotlivých blokov – opakovaný zápis do rovnakého logického bloku sa realizuje často do rôznych skutočných (fyzických) blokov flash pamäte. Vďaka tomu SSD dosahujú použiteľné parametre ako náhrada diskov. V každom prípade, ak sa SSD použije spôsobom, kedy bude množstvo zápisov veľké,

[1] Solid-State Disk

dôjde časom k jeho znefunkčneniu a bude potrebná jeho výmena (a, samozrejme, dôjde k strate na ňom uložených údajov). Typickým príkladom je použitie SSD ako cache v diskových poliach – vďaka rýchlosti je to užitočné riešenie, ktoré pomáha zvýšiť výkon diskového poľa – no treba tu počítať s obmedzenou životnosťou a potrebou SSD v takomto diskovom poli vymieňať. Životnosť SSD pre praktické účely sa bežne udáva v podobe množstva údajov, ktoré je možné na SSD zapísať, kým pravdepodobne dôjde k zlyhaniu nejakého bloku – často sa označuje ako TBW (Terabytes Written). Ďalšou záludnosťou SSD je bezpečné vymazávanie údajov. Keďže opakované zápisy na rovnaké miesto v skutočnosti zvyčajne nevedú k fyzickému vymazaniu/prepísaniu daného miesta, tak bežné nástroje na bezpečné mazanie (prepisovanie) diskov nie sú pri SSD použiteľné (resp. vôbec nemusia zabezpečiť skutočné vymazanie citlivých údajov). Mnohé SSD dnes preto disponujú funkciou *Secure Erase*, ktorá umožňuje vymazať celé SSD. Alternatívou je predchádzať potrebe mazania údajov z SSD napr. použitím šifrovania údajov (v prípade dobrého riešenia sú údaje bez dešifrovacieho kľúča bezcenné).

Rozširujúce karty umožňujú pridávať počítaču ďalšiu funkcionalitu. Typickými príkladmi môžu byť grafické karty umožňujúce počítaču vytvárať signál pre monitor alebo sieťové karty umožňujúce pripojenie k počítačovej sieti. Dnes je bežné, že priamo základná doska obsahuje komponenty, ktoré časť takej funkcionality poskytujú, preto v dnešných počítačoch typicky nie je potrebné použiť toľko rozširujúcich kariet ako v minulosti. Z hľadiska funkčnosti však nie je dôležité, či je komponent poskytujúci rozširujúcu funkcionality integrovaný priamo na základnej doske alebo je na rozširujúcej karte. V oboch prípadoch je to zariadenie pripojené k niektorej zbernici na základnej doske.

Niektoré počítače, typicky notebooky, majú aj zvonku dostupné konektory, do ktorých je možné za behu pripojiť špeciálny typ rozširujúcej karty (PCMCIA, CardBus, ExpressCard). To umožňuje rozširovanie funkčnosti notebooku, no ako zároveň vytvára zraniteľnosť. Taká karta sa v konečnom dôsledku stáva zariadením pripojeným k zbernici, čo jej umožňuje priamo komunikovať napr. s operačnou pamäťou. Je preto možné vyrobiť takú kartu, ktorá napr. umožní z počítača získať kópiu operačnej pamäte (vrátane citlivých údajov, ktoré sa v nej môžu nachádzať).

Prenos údajov z a do zariadení pripojených k zbernici typicky prebieha jedným z troch spôsobov:

- pomocou na to špecificky určených inštrukcií procesor posiela a prijíma údaje do/zo zariadenia,
- procesor zariadenie používa spôsobom, ako keby to bola pamäť (tzv. pamäťovo mapované zariadenia),
- priamym prístupom do pamäte (DMA).

Pri prvých dvoch spôsoboch sa vždy jedná o prenos medzi zariadením a procesorom. To je nevhodné pre prenos veľkého množstva údajov, kedy by procesor mohol vykonávať nejakú užitočnejšiu činnosť. Tento problém sa odstraňuje pomocou priameho prístupu do pamäte (DMA), kedy procesor iba inicializuje prenos, určí na aké miesto v pamäti sa majú údaje zapísať alebo odkiaľ sa majú prečítať, a následne sa prenos deje po zbernici bez účasti procesora priamo medzi operačnou pamäťou a zariadením.

Procesor často potrebuje reagovať na externé udalosti – napr. prijatie údajov sieťovou kartou zo siete alebo dokončenie DMA prenosu zo zariadenia do pamäte. Aby nebolo potrebné neustále kontrolovať, či nejaká externá udalosť nastala alebo nie, procesory využívajú systém *prerušení*. Zariadenia pripojené na zbernicu majú možnosť signalizovať procesoru tzv. prerušenie. Riadiaca jednotka procesora medzi vykonávaním inštrukcií sleduje, či procesor nedostal žiadosť o prerušenie. Ak áno, tak pred vykonaním ďalšej inštrukcie najprv vykoná program, ktorý slúži na obsluhu príslušného prerušenia.

4.2 Operačný systém

Operačný systém (napr. rôzny Windows, Linux, UNIX, ...) predstavuje dôležitú vrstvu nad vrstvou hardvéru, ktorá umožňuje vyšším vrstvám používať počítač spôsobom, ktorý nie je závislý od konkrétnych technických detailov použitého hardvéru. Medzi základné úlohy operačného systému z pohľadu funkčnosti patria:

- správa procesov a procesora,
- správa pamäte,
- správa súborov,
- správa vstupno-výstupných a iných zariadení.

Informačné systémy plnia svoje úlohy vykonávaním programov. Program je vykonávaný v rámci *procesu*. Procesu musí operačný systém prideliť časť operačnej pamäte, do ktorej uloží inštrukcie programu, a kde sa tiež budú počas vykonávania programu ukladať spracovávané údaje. Všetky dnes bežné operačné systémy umožňujú z pohľadu používateľa vykonávať viacero procesov súčasne – tzv. *multitasking*. V skutočnosti nemôže byť naraz vykonávaných viac procesov, než má počítač procesorov (resp. jadier procesorov). Zdanlivé súčasné vykonávanie viacerých procesov sa dosahuje ich rýchlym striedaním, čiže prideľovaním a odoberaním procesora procesu. Toto prideľovanie a odoberanie procesora procesom je súčasťou správy procesov a procesora, a teda jednou z úloh operačného systému. Operačný systém sa tiež stará o vytváranie a rušenie procesov.

Operačný systém spravuje aj operačnú pamäť počítača. Prideľuje jednotlivým procesom bloky pamäte, ktoré proces môže používať. Všetky dnes bežné operačné systémy podporujú aj tzv. *virtuálnu pamäť*. Operačný systém vtedy „predstiera“, že má k dispozícii viac pamäte, než v skutočnosti operačnej pamäte v počítači je. Procesom prideľuje bloky (nazývané *stránky*) virtuálnej pamäte. Obsah stránky môže byť buď uložený v nejakom bloku skutočnej – *fyzickej* pamäte, alebo môže byť odložený na pevnom disku. Operačný systém spravuje *tabuľku stránok*, ktorá určuje, či a kde vo fyzickej pamäti sa nachádza príslušná stránka. Keď sa proces pokúsi pristúpiť k stránke, ktorá sa nenachádza vo fyzickej pamäti, procesor vygeneruje prerušenie, operačný systém nájde voľné miesto vo fyzickej pamäti, načíta doň obsah požadovanej stránky, upraví tabuľku stránok a vráti vykonávanie späť pôvodnému procesu. Keď sa vo fyzickej pamäti nenachádza voľné miesto na umiestnenie požadovanej stránky, operačný systém nejakú inú stránku z fyzickej pamäte odstráni (pričom jej obsah najprv uloží na disk).

Na dlhodobejšie ukladanie údajov slúžia najčastejšie pevné disky. Procesy však s priestorom na pevnom disku nemanipulujú priamo, ale prostredníctvom služieb operačného systému,

ktorý na tento účel poskytuje abstrakciu na ukladanie údajov, ktorú poznáme ako *súbory*. Na hardvérovej vrstve sú údaje napokon uložené v blokoch na disku. Operačný systém v rámci správy súborov pre každý súbor eviduje, v ktorých blokoch na disku sa nachádzajú jednotlivé časti údajov v súbore, prideľuje bloky súboru, keď je potrebné súbor zväčšiť, uvoľňuje bloky pri zmenšení veľkosti alebo vymazaní súboru. Súbory sú najčastejšie organizované v hierarchických štruktúrach – tzv. *adresároch* (nazývaných aj *priečinky*). Adresár môže obsahovať súbory ako aj ďalšie adresáre. Informácie o menách súborov a adresárov, ako aj ich ďalšie atribúty, operačný systém tiež ukladá vo vhodných štruktúrach na disku.

Operačný systém tiež zabezpečuje správu ďalších zariadení, napr. vstupné a výstupné zariadenia, pomocou ktorých môžu procesy interagovať s používateľom alebo inými systémami. Pri multitaskingu je zvyčajne potrebné zabezpečiť, aby so zariadením nemohli naraz komunikovať viaceré procesy. Inak by sa napr. mohlo stať, že pri tlačení na tlačiareň by sa pomiešali výstupy rôznych procesov. Úlohou operačného systému je preto zabezpečiť prideľovanie a odoberanie prístupu k zariadeniam jednotlivých procesom. Často je tiež riešením vytvorenie abstrakcie zariadenia – akéhosi virtuálneho zariadenia, ktoré môžu procesy voľne používať, pričom operačný systém zabezpečí prenos údajov medzi virtuálnym a skutočným zariadením vo vhodnom čase. Ako príklad si môžeme uviesť napr. klávesnicu a obrazovku. Operačný systém poskytuje vyššej vrstve abstrakciu obrazovky (napr. okno) a abstrakciu klávesnice a zabezpečuje, že obsah okna sa zobrazí na správnom mieste skutočnej obrazovky, a že vstup zo skutočnej klávesnice sa objaví na vstupe virtuálnej klávesnice toho procesu, ktorého okno je práve aktívne.

Operačný systém sám nie je jednoliatym komponentom, ale skladá sa z mnohých častí. Niektoré z nich sú nezávislé od konkrétneho hardvéru počítača, na ktorom operačný systém beží, no iné sú pre konkrétny hardvér špecifické. Tie špecifické komponenty, často nazývané *ovládače zariadení*, poskytujú zvyšku operačného systému jednotné rozhranie pre určitý typ zariadenia. Napr. sieťová karta je zariadenie, ktoré umožňuje odosielať a prijímať bloky údajov do/z počítačovej siete. Ale s rôznymi sieťovými kartami sa na hardvérovej vrstve komunikuje rôznym spôsobom – napr. niektorá používa DMA, iná špeciálne inštrukcie. Úlohou ovládača sieťovej karty je zvyšku operačného systému poskytnúť jednotné rozhranie pre zariadenie typu „sieťová karta“.

Operačný systém okrem vyššie uvedených úloh zohráva aj významnú úlohu pre bezpečnosť informačného systému. Zabezpečuje vzájomnú izoláciu procesov, aby sa procesy mohli navzájom ovplyvňovať len prostredníctvom kontrolovateľných mechanizmov. Taktiež zabezpečuje čiastočnú izoláciu procesov od hardvéru a umožňuje s hardvérom manipulovať len pomocou služieb operačného systému. Výnimkou je sprístupnenie tých častí hardvéru, ktorých používanie nemá dopad na globálny stav systému (napr. aplikačné procesy priamo využívajú bežné inštrukcie procesora).

Dôležitou bezpečnostnou funkciou operačného systému je aj riadenie prístupu. Všeobecnejším aspektom riadenia prístupu je venovaná samostatná kapitola. Pre účely riadenia prístupu operačný systém pre každý proces udržiava informáciu o používateľovi, ktorý je za tento proces zodpovedný, čiže v mene ktorého tento proces beží – vykonáva operácie. Keď proces využíva službu operačného systému, ktorá podlieha riadeniu prístupu (napr. prístup k súboru alebo k periférnemu zariadeniu), operačný systém vyhodnotí, či používateľ zodpovedný za tento proces má oprávnenie príslušnú operáciu vykonať alebo nie. Riadenie prístupu si vyžaduje identifikáciu a autentifikáciu používateľov, čo tiež patrí medzi bezpečnostné služby operačného systému (viac o identifikácii a autentifikácii v kapitole o riadení prístupu). Operačný systém tiež za-

bezpečuje vymazávanie zvyškových (reziduálnych) informácií, ktoré môžu zostať v pamäti po jej uvoľnení iným procesom alebo na disku po zmenšení alebo vymazaní súboru.

Pre lepšiu predstavu o riadení prístupu v operačných systémoch sa pozrieme na príklad dvoch typov bežne používaných operačných systémov – Windows a Linux/UNIX. V oboch systémoch je základom riadenia prístupu tzv. *voliteľné riadenie prístupu* (*discretionary access control*, *DAC*). Každý súbor a adresár (ďalej objekt) má svojho vlastníka, ktorý môže nastavovať prístupové práva k objektu. Systémy typu Linux/UNIX rozlišujú 3 práva na prístup k objektom – čítanie, zápis a spustenie programu/použitie adresára. Tieto práva môžu byť pridelené vlastníkovi objektu, jednej skupine používateľov a ostatným. Rozšírenie modelu prístupových práv v Linuxe známe ako *ACL* (*Access Control Lists*) umožňuje tieto práva prideľovať aj ďalším používateľom a viacerým skupinám. Systémy Windows majú jemnejšie delenie prístupových práv (umožňujú napr. rozlíšiť právo na vytváranie nových súborov a právo na vytváranie podadresárov, umožňujú nastaviť právo na vymazanie objektu, a pod.). Používajú tiež mechanizmus dedenia prístupových práv z adresára na podadresáre a súbory a umožňujú tiež určité právo explicitne zakázať. Práva môžu byť prideľované používateľom a skupinám používateľov. Ak je používateľ členom viacerých skupín, získava práva pridelené všetkým skupinám. Zakazovacie práva majú prednosť pred povoľovacími právami, ak sú pridelené na rovnakej úrovni adresárovej štruktúry. Avšak práva pridelené na úrovni bližšie k objektu majú vždy prednosť pred právami pridelenými na vyššej úrovni.

Voliteľné riadenie prístupu v operačných systémoch neumožňuje chrániť údaje, ku ktorým má používateľ prístup, proti nežiadúcemu prístupu škodlivého kódu – zlomyseľných programov (alebo programov, ktoré sa zlomyseľnými stanú v dôsledku zneužitia nejakej ich zraniteľnosti útočníkom). Mnohé funkcie operačného systému sú prístupné len používateľom s administrátorskými oprávneniami. Administrátorské oprávnenia tiež zväčša umožňujú jednoducho obísť prístupové práva k súborom. Veľkým problém nastáva, keď sa s oprávneniami administrátora vykonáva škodlivý kód, keďže takto získava úplnú kontrolu nad systémom. Z tohto dôvodu je nevhodné používať konto s administrátorskými oprávneniami na bežné činnosti. Žiaľ, je to pomerne častou zlou praktikou. V novších verziách systému Windows bol preto implementovaný mechanizmus *UAC* (*User Account Control*), ktorý ani používateľovi, ktorý je členom skupiny administrátorov, štandardne nepriznáva administrátorské oprávnenia, no umožňuje procesu získať tieto oprávnenia po interaktívnom potvrdení autentifikovaného administrátora.

V Linuxových systémoch museli byť niektoré programy vykonávané s administrátorskými oprávneniami často len kvôli pár operáciám. Aby nebolo nutné im poskytnúť plnú kontrolu nad systémom, je dnes možné takýmto programom explicitne prideliť vybrané oprávnenia prostredníctvom tzv. *capabilities*. Tým je možné znížiť množstvo programov, ktoré majú plnú kontrolu nad systémom.

Iným spôsobom, ako obmedziť možné dopady škodlivého kódu, je použitie *povinného riadenia prístupu* (*mandatory access control*, *MAC*). Pri povinnom riadení prístupu sú povolené operácie určené bezpečnostnou politikou, ktorú bežní používatelia a procesy nemôže modifikovať. Príkladom povinného riadenia prístupu v systémoch Windows je tzv. Mandatory Integrity Control (MIC). Tento subsystém umožňuje prideliť objektom a procesom úroveň integrity a zabraňuje procesom s nižšou úrovňou integrity modifikovať objekty s vyššou úrovňou integrity. Takto je možné napr. zabrániť tomu, aby chybný webový prehliadač ovplyvnený škodlivým kódom z Internetu prepísal dôležité súbory.

V systéme Linux je možné na povinné riadenie prístupu využiť jeden z dvoch rozšírených subsystémov – *SELinux* a *AppArmor*. SELinux umožňuje priradiť procesom a objektom tzv. typy a definovať, aké operácie môže proces určitého typu vykonať s objektom určitého typu. Subsystém AppArmor umožňuje vytvárať tzv. profily pre určité programy a v týchto profiloch obmedziť, k akým súborov a vybraným funkciám operačného systému má mať príslušný proces prístup. Oba tieto subsystémy umožňujú veľmi presne obmedziť možné dopady škodilvého kódu vykonaného v rámci určitého procesu.

4.3 Databázový systém

V informačných systémoch pracujúcich s väčším objemom štruktúrovaných údajov zvyčajne aplikačné procesy neukladajú údaje priamo do súborov pomocou služieb operačného systému, ale využívajú služby databázového systému. Databázový systém poskytuje aplikačnej vrstve služby na vkladanie, úpravu a vyhľadávanie v štruktúrovaných údajoch – v databázach. Aplikačná vrstva nemusí riešiť, ako údaje efektívne uložiť do súborov, ako v nich vedieť rýchlo vyhľadávať a pod., ale len pripraví tzv. dotazy v určenom jazyku (najčastejšie sa používa jazyk SQL), ktoré odošle databázovému serveru a následne si prevezme výsledky. Spôsob uloženia údajov je vnútornou záležitosťou databázového systému.

Databázové systémy zvyčajne podporujú tzv. transakčné spracovanie. Keď k databáze súčasne pristupuje viacero aplikačných procesov, často potrebujeme, každý z nich videl údaje v konzistentnom stave. Problém si môžeme demonštrovať na jednoduchom príklade. Majme v databáze tabuľku s počtom tovarov na sklade a majme aplikáciu, ktorá spracováva objednávky zákazníkov tak, že najprv skontroluje, či je na sklade aspoň požadované množstvo tovaru a, ak áno, počet kusov na sklade príslušne zníži a potvrdí objednávku. Keď budú bežať dva takéto aplikačné procesy naraz, môže sa stať, že oba zistia počet kusov na sklade skôr ako ho jeden z nich zníži, a teda oba úspešne potvrdia objednávky, no počet kusov na sklade sa dostane do záporných hodnôt (a, samozrejme, tovar na vybavenie objednávky nebude k dispozícii). Tento príklad je síce umelý, no reálne problémy s nekonzistenciou údajov v databázach sú často výrazne horšie. Riešením je práve transakčné spracovanie – aplikačný proces vykoná všetky súvisiace operácie ako súčasť jednej tzv. transakcie a databázový systém zabezpečí, že v prípade, že transakcia úspešne skončí, stav v databáze bude konzistentný, a že ak bude transakcia zrušená, stav v databáze ňou nebude ovplyvnený. V našom príklade by to mohlo dopadnúť tak, že by databázový systém zrušil transakciu jedného procesu v momente, keď by sa pokúsil modifikovať údaje, ktoré mu po tom, ako ich prečítal, už stihol modifikovať iný proces.

Databázové systémy tiež zabezpečujú riadenie prístupu k databáze a s tým súvisiacu identifikáciu a autentifikáciu. Vo vzťahu k operačnému systému beží databázový systém v mene na ten účel určeného používateľa (v tomto prípade používateľ nezodpovedá skutočnej osobe, ide o akéhosi virtuálneho používateľa na účely riadenia prístupu procesov, z ktorých sa skladá databázový systém). Aplikačné procesy sa identifikujú a autentifikujú pri využívaní služieb databázového systému, a ten následne povoľuje alebo zamieta jednotlivé operácie s údajmi v databáze. Riadenie prístupu v databázových systémoch umožňuje definovať práva na manipuláciu s databázami, tabuľkami, v niektorých databázových systémoch dokonca s jednotlivými stĺpcami tabuliek. Tým umožňuje pomerne presne definovať, aké operácie môžu jednotliví používatelia vykonať s rôznymi údajmi.

4.4 Virtualizácia, cloud

Spolu s narastajúcim výkonom hardvéru sa čoraz častejšie stáva, že počítače sú využité len na zlomok ich kapacity. To znižuje efektivitu ich využitia z priestorového, energetického aj finančného hľadiska. V súčasnosti veľmi populárnym (aj keď nie principiálne novým) riešením tohto problému je virtualizácia hardvéru. Pri virtualizácii sa medzi hardvérovú vrstvu a operačný systém vloží virtualizačná vrstva (tzv. *hypervízor*), ktorej úlohou je na jednom fyzickom hardvéri simulovať niekoľko samostatných počítačov. Týmto spôsobom je potom možné na jednom výkonnom fyzickom počítači mať niekoľko virtuálnych počítačov, pričom každý má svoj operačný systém. Výhodou virtualizácie je už spomenuté zvýšenie efektivity, keďže je zvyčajne efektívnejšie prevádzkovať jeden výkonnejší počítač ako veľa (aj keď o niečo menej výkonných) počítačov. Taktiež je výhodou, že keď potrebujeme nasadiť nový počítač, nie je potrebné kúpiť a sprevádzkovať nový hardvér, ale môžeme využiť voľnú kapacitu existujúceho. Vytvorenie nového virtuálneho počítača je záležitosť pár sekúnd až minút práce administrátora.

V súčasnosti je veľmi populárne využívanie *cloudových služieb*. Cloudové služby umožňujú objednať si prevádzkovanie softvéru, platformy, alebo aj celej virtuálnej infraštruktúry ako službu prevádzkovateľa cloudu. V praxi sa stretávame s viacerými typmi cloudových služieb:

- *SaaS – Software as a Service – softvér ako služba* je typ cloudovej služby, kedy poskytovateľ služby ponúka využitie nejakého konkrétneho softvéru ako službu. Typickými príkladmi sú e-mailový systém, systém na ukladanie a správu dokumentov, a pod. Pri tomto type cloudovej služby poskytovateľ zabezpečuje prevádzku celej infraštruktúry, na ktorej službu poskytuje. Zákazník môže nanajvýš nastavovať vybrané konfiguračné parametre poskytovanej služby (napr. pridávať či rušiť používateľov, nastavovať parametre antivírusovej a antispamovej kontroly, a pod.). Zákazník nepotrebuje správcu operačného systému, nerieši žiadnu inštaláciu na strane serverov, a pod.

- *PaaS – Platform as a Service – platforma ako služba* je typ cloudovej služby, kedy poskytovateľ služby ponúka využitie tzv. platformy na prevádzku nejakého informačného systému zákazníka. Pod platformou v tomto kontexte typicky rozumieme kombináciu webového servera, databázového servera a nejakého prostredia na prevádzku aplikačných komponentov informačného systému (napr. PHP, JSP, a pod.). Tento typ služby umožňuje zákazníkovi nasadiť na danej platforme vlastné komponenty a vytvoriť si (alebo si nechať vytvoriť) vlastnú webovú aplikáciu bez potreby starať sa o hardvér, operačný systém a systémové komponenty platformy. Využitie tohto typu cloudovej služby je náročnejšie ako využitie SaaS, ale poskytuje podstatne väčšiu flexibilitu.

- *IaaS – Infrastructure as a Service – infraštruktúra ako služba* je typ cloudovej služby, kedy poskytovateľ služby ponúka využitie (zvyčajne virtuálneho) hardvéru ako službu. Využitie tohto typu služby je v porovnaní s PaaS a SaaS najnáročnejšie, pretože správa všetkých vrstiev okrem hardvéru je na pleciach zákazníka. Zákazník si musí zabezpečiť správu operačného systému a všetkých komponentov svojho informačného systému na vyšších vrstvách. Význam služieb typu IaaS je predovšetkým v tom, že zákazník nepotrebuje vlastniť a prevádzkovať fyzický hardvér, ale môže si virtuálny hardvér objednávať podľa aktuálnej potreby. V jednoduchších prípadoch ide o prenájom virtuálnych počítačov s danými (často v určitých medziach prispôsobiteľnými) parametrami ako typ a počet procesorov, množstvo operačnej pamäte, diskový priestor, pripojenie do Internetu.

Pri pokročilejších cloudových službách typu IaaS je možné nakonfigurovať si celú komplexnú infraštruktúru pozostávajúcu z viacerých sietí, bezpečnostných prvkov (ako napr. firewall-y), dátových úložísk a virtuálnych počítačov. Pokročilé cloudové služby typu IaaS napr. ponúkajú dátové úložiská s rôznou úrovňou zabezpečenia proti strate dát v dôsledku technického zlyhania – od úrovne porovnateľnej s bežným diskovým poľom (RAID) až po úroveň viacnásobného uloženia na geograficky vzdialených lokalitách za účelom zaistenia dostupnosti dát aj v prípade významných katastrof.

Z hľadiska toho, aký je okruh zákazníkov, rozdeľujeme cloudy na:

- *verejný (public) cloud* – poskytuje služby komukoľvek,
- *súkromný (private) cloud* – poskytuje služby len jednému zákazníkovi / organizácii (prípadne nejakému zoskupeniu organizácií – napr. cloud pre štátnu správu jedného štátu).

Výhodou verejných cloudov je predovšetkým cena, keďže náklady na prevádzku cloudu môže poskytovateľ rozdeliť medzi väčší počet zákazníkov, a tiež dostupnosť rôznych komponentov. Výhodou súkromných cloudov je predovšetkým vyššia dosiahnuteľná úroveň bezpečnosti, keďže infraštruktúra nie je zdieľaná s verejnosťou, a môže byť teda lepšie chránená proti neoprávnenému prístupu. Súkromný cloud si môže organizácia pre svoje účely vybudovať sama (toto je vhodné najmä v prípade veľkých organizácií, kde potom jeden organizačný útvar zohráva rolu poskytovateľa cloudovej služby pre zvyšok organizácie), alebo môže byť poskytovateľom súkromného cloudu aj subjekt mimo organizáciu (v takom prípade často posyktovateľ cloudovej služby vyhradí časť infraštruktúry výlučne pre potreby jedného zákazníka). V praxi sa stretávame ešte s pojmom *hybridný cloud*. Ide o spojenie verejného a súkromného cloudu – niektoré časti informačného systému sú prevádzkované vo verejnom cloude, iné v súkromnom cloude (alebo na vlastnej infraštruktúre).

Pri úvahách o využití cloudových služieb je však okrem ceny (a jej porovnania s cenou obstarania a prevádzky vlastnej infraštruktúry) potrebné dôkladne posúdiť aj bezpečnostné riziká, ktoré využitie cloudových služieb so sebou prináša. Jedným dôležitým aspektom je fakt, že údaje budú v cloude uložené a spracovávané v prostredí, nad ktorým nemáme kontrolu. Ich ochrana pred neoprávneným prístupom je významne závislá na tom, ako dobre je infraštruktúra cloudu spravovaná jeho poskytovateľom. Nie je jednoduché (v praxi často ani možné) zabezpečiť ochranu dát spôsobom odolným voči potenciálnym nekalým úmyslom poskytovateľa cloudovej služby. Taktiež si je potrebné uvedomiť, že koncentrácia zaujímavých dát v cloude robí z tohto cloudu veľmi zaujímavý cieľ pre potenciálnych útočníkov, ktorí môžu byť schopní investovať viac prostriedkov do snahy o získanie neoprávneného prístupu než v prípade samostatného menšieho informačného systému. Na druhú stranu je pravdou aj to, že najmä v prípade menších, finančne, personálne a odborne poddimenzovaných organizácií môže byť úroveň zabezpečenia poskytovaná poskytovateľom cloudových služieb vyššia, než by si daná organizácia vedela zabezpečiť sama. Toto môže v niektorých prípadoch viesť aj k zaujímavým riešeniam, kedy napr. organizácia využije cloudové služby verejného cloudu na zvýšenie ochrany dát pred stratou (využitím úložiska s geograficky dislokovanými kópiami), ale ochranu dôvernosti týchto dát bude riešiť ich šifrovaním tak, aby poskytovateľ cloudovej služby buď vôbec nemal prístup k dešifrovaným dátam (teda dáta sa budú šifrovať, dešifrovať a spracovávať vo vlastnej infraštruktúre organizácie), alebo aby prístup k dešifrovaným dátam bol aspoň sťažený (napr. tým,

že kľúče nebudú trvale uložené v cloude, ale budú len v operačnej pamäti virtuálneho servera – toto riešenie stále umožňuje kľúče z operačnej pamäte extrahovať a zneužiť, ale je to podstatne náročnejšie ako len získať prístup k dátovému úložisku).

4.5 Model klient-server

Informačné systémy, ktoré umožňujú súčasnú prácu viacerým používateľom sú zvyčajne postavené na modeli *klient-server*. Základnou myšlienkou tohto modelu je centrálne spracovanie údajov časťou informačného systému nazývanou *server*, pričom komunikáciu medzi týmto serverom a používateľmi sprostredkovávajú ďalšie časti informačného systému, ktoré sa nazývajú *klienti*. Server je prevádzkovaný na jednom počítači a klienti sú prevádzkovaní na iných počítačoch, pri ktorých sedia používatelia. Klienti a server navzájom komunikujú prostredníctvom počítačovej siete.

Klientov rozdeľujeme na dva základné typy – tzv. *tenkí klienti* a *hrubí klienti*. Hrubý klient je pre informačný systém špecifický program bežiaci na používateľovom počítači, ktorý zabezpečuje vstup a výstup údajov ako aj predbežné alebo následné spracovanie pre/po prenesení údajov na server. Tenký klient je program bežiaci na používateľovom počítači, ktorý zabezpečuje v zásade len vstup a výstup údajov bez nejakého podstatného spracovania. Ako tenký klient sa v súčasnosti najčastejšie používa bežný webový prehliadač. To má veľkú výhodu v tom, že nie je potrebné na používateľov počítač inštalovať žiadny špeciálny program, vďaka čomu nie je ani dôležité, aký operačný systém je na používateľovom počítači použitý. Taktiež je často možné využiť to, že webový prehliadač je dnes bežnou súčasťou aj iných zariadení ako bežných počítačov – napr. tabletov, inteligentných mobilných telefónov, televízorov a pod. Vďaka tomu je možné s takýmto informačným systémom pracovať z veľkého množstva rôznych zariadení.

Z hľadiska bezpečnosti je dôležitá skutočnosť, že bezpečnostné funkcie ako napr. riadenie prístupu, autentifikácia a pod. musia byť realizované na serveri. Ak by boli realizované len na klientovi, nebolo by možné vylúčiť, aby útočník jednoducho použil vlastného upraveného klienta a realizoval tak nepovolené operácie.

4.6 Bezpečnostné funkcie vrstiev

Bezpečnosť informačného systému je komplexná záležitosť. Odhliadnime však teraz od právnych a organizačných aspektov a pozrime sa bližšie na technické otázky týkajúce sa toho, v ktorých vrstvách je možné realizovať bezpečnostné funkcie a mechanizmy, a aké predpoklady na to musia byť splnené.

Ak je nejaká bezpečnostná funkcia implementovaná na určitej vrstve, môže účinne poskytovať ochranu len proti útokom, ktoré sú vedené na tejto alebo vyššej vrstve. Keď napr. na aplikačnej vrstve implementujeme riadenie prístupu k údajom, tak toto môže byť účinné len proti útokom na aplikačnej vrstve. Ak by totiž útočník získal prístup k systému napr. na vrstve operačného systému, tak môže využiť rovnaké služby operačného systému, aké využíva aj príslušná aplikácia, a získať prístup k súborom s údajmi bez toho, aby použil akúkoľvek službu aplikácie. Analogicky, ak útočník získa prístup k údajom na úrovni hardvéru (napr. ukradne pevný disk z počítača), bez akýchkoľvek problémov môže obísť riadenie prístupu im-

plementované v operačnom systéme. Jedinou čiastočnou výnimkou je použitie kryptografických prostriedkov – napr. údaje zašifrované na aplikačnej vrstve môžu byť pred narušením dôvernosti účinne chránené aj proti niektorým útokom napr. na vrstve hardvéru.

Vo všeobecnosti môžeme povedať, že nevyhnutnými predpokladmi pre účinnú implementáciu bezpečnostných funkcií sú:

- bezpečnostnú funkciu nemôže byť možné obísť – teda útočník napr. nesmie mať možnosť využiť služby nižšej vrstvy na získanie prístupu k údajom,
- implementácia bezpečnostnej funkcie musí byť chránená proti neoprávnenej zmene, aby ju útočník nemohol pozmeniť tak, aby mu umožnila vykonať požadované operácie,
- údaje, ktoré bezpečnostná funkcia používa na rozhodovanie, musia byť chránené proti neoprávnenej zmene – napr. útočník nesmie mať možnosť zmeniť údaje obsahujúce informáciu o prístupových právach alebo heslo,
- dôverné údaje, ktoré bezpečnostná funkcia používa, musia byť chránené aj proti prezradeniu – napr. útočník nesmie mať možnosť zistiť heslá, ktoré sa používajú na autentifikáciu.

Berúc do úvahy vyššie uvedené predpoklady, pozrime sa teraz podrobnejšie na typické bezpečnostné funkcie jednotlivých vrstiev. Aplikačná vrstva typicky zabezpečuje riadenie prístupu k funkciám a údajom informačného systému pre používateľov aplikácie. Keďže aplikačná vrstva je špecifická pre konkrétny informačný systém, nie je tu problém zohľadniť sémantiku, čiže význam, jednotlivých údajov a aplikačných funkcií. V prípade použitia modelu klient-server aplikačná vrstva (presnejšie server) môže účinne zabezpečiť ochranu údajov proti útočníkovi využívajúcemu služby aplikačnej vrstvy a izolovať ho od možnosti použiť služby nižšej vrstvy. Nemôže však efektívne zabezpečiť vlastnú ochranu ani ochranu proti útočníkovi, ktorý má možnosť priamo využiť služby nižších vrstiev (pretože tu nie je splnený napr. predpoklad, že bezpečnostnú funkciu nie je možné obísť). Pokiaľ sa jedná jednoduchú aplikáciu (bez použitia modelu klient-server), je často problematické zabezpečiť, aby používateľ aplikácie nemal možnosť pristupovať aj k službám operačného systému.

Dôležitou úlohou operačného systému je zabezpečiť ochranu aplikačnej vrstvy (a teda aj jej bezpečnostných funkcií) pred neoprávnenou zmenou, ako aj zabezpečiť ochranu údajov aplikačnej vrstvy proti neoprávnenému prístupu inou cestou ako prostredníctvom aplikačnej vrstvy. Tým operačný systém vytvára predpoklady pre účinnú implementáciu bezpečnostných funkcií na aplikačnej vrstve. Ako sme už spomenuli v časti o operačnom systéme, na naplnenie týchto úloh operačného systému sa využívajú najmä izolácia procesov a riadenie prístupu. Opäť však platí, že operačný systém dokáže poskytovať ochranu proti útočníkovi, ktorý využíva služby operačného systému, no nedokáže efektívne poskytovať ochranu proti útočníkovi, ktorý má možnosť využiť priamo služby hardvéru. S vhodnou podporou od hardvéru však operačný systém izoluje procesy od priameho prístupu k hardvéru, čím ponecháva útočníkovi jedinú cestu na priamu manipuláciu s hardvérom, a to fyzický prístup alebo zásah do hardvéru. Keď odhliadneme od fyzického prístupu, tak vďaka izolácii procesov od hardvéru operačný systém môže účinne chrániť aj vlastnú implementáciu a vlastné údaje, ktoré jeho bezpečnostné funkcie využívajú.

Bez potrebnej podpory zo strany hardvéru by bol problém naplniť predpoklady na účinnú implementáciu bezpečnostných funkcií v operačnom systéme. Dnešný hardvér však poskytuje niekoľko bezpečnostných funkcií, ktoré tieto predpoklady umožňujú operačnému systému splniť. Základnými bezpečnostnými funkciami hardvéru sú:

- riadenie prístupu do pamäte,
- riadenie prístupu k zariadeniam,
- obmedzenie prístupu k *privilegovaným inštrukciám*.

Inštrukcie procesora, ktoré majú vplyv na systém ako celok (napr. zakazovanie prerušení, manipulácia s bezpečnostnými mechanizmami hardvéru, a pod.), sa nazývajú privilegované inštrukcie. Hardvér umožňuje privilegované inštrukcie vykonávať len operačnému systému (a prípadne operačným systémom určeným procesom) no nie bežným procesom.

Hardvér tiež poskytuje operačnému systému prostriedky na určenie toho, do ktorých častí pamäte môže jednotlivé procesy pristupovať. Taktiež umožňuje operačnému systému určiť, že len operačný systém alebo prípadne špeciálne určené procesy môžu manipulovať so zariadeniami.

Vďaka tomu si operačný systém môže ponechať kontrolu nad zariadeniami a celkovým stavom systému a účinne zabrániť procesom, aby mohli obísť bezpečnostné funkcie operačného systému.

Jedným z typických mechanizmov, ktorý býva v hardvéri na realizáciu spomenutých funkcií použitý sú tzv. *bezpečnostné okruhy* (*security rings*). Hardvér definuje niekoľko (typicky 2 až 4) okruhov, v rámci ktorých sa môžu vykonávať programy (čiže postupnosti inštrukcií). Vnútorný okruh má možnosť vykonávať všetky inštrukcie (teda aj privilegované) a smerom k vonkajším okruhom pribúdajú obmedzenia. Vonkajší okruh – typicky určený pre bežné programy na aplikačnej úrovni – neumožňuje vykonávanie žiadnych privilegovaných inštrukcií. Vnútorný okruh je určený pre operačný systém (resp. pre tzv. jadro operačného systému). Okruhy medzi vnútorným a vonkajším (ak sú podporované) môžu byť využité napr. pre ovládače zariadení v operačnom systéme.

Ďalším mechanizmom, slúžiacim na riadenie prístupu do pamäte je *stránkovanie*. Stránkovanie sme už spomenuli v súvislosti s virtuálnou pamäťou, no má aj úlohy v bezpečnosti. Hardvér umožňuje operačnému systému udržiavať samostatné tabuľky stránok pre jednotlivé procesy a definovať, či program vo vonkajšom okruhu môže k jednotlivým stránkam pristupovať a ako (čítanie, zápis, vykonávanie inštrukcií). Vďaka tomu môže operačný systém oddeliť pamäť prístupnú jednotlivým procesom a zabezpečiť tak ich vzájomnú izoláciu. Zároveň tak môže ochrániť vlastné údaje pred prístupom procesov.

Prístup k zariadeniam býva riešený buď tak, že je definované, ktorý okruh má prístup k hardvéru, a ktorý už nie, alebo procesor umožňuje operačnému systému definovať presne, ktorý proces môže k jednotlivým zariadeniam pristupovať. Vďaka tomu môže operačný systém izolovať procesy od priamej manipulácie napr. s pevným diskom, grafickou kartou a pod.

Žiadny z uvedených mechanizmov však nedokáže zabrániť manipulácii s hardvérom útočníkom, ktorý má fyzický prístup k hardvéru (teda ktorý môže napr. vybrať pevný disk z

počítača). Tu zohráva dôležitú úlohy fyzická bezpečnosť. Ak je aj málo pravdepodobné, že neoprávnená osoba počítač rozoberie, stále však zostáva niekoľko problémov, na ktoré je potrebné myslieť. Ako sme spomenuli v časti venovanej hardvéru, mnohé počítače majú možnosť rozširovať funkcionalitu hardvéru aj bez rozoberania a dokonca bez vypnutia. Typický príkladom sú spomenuté rozširujúce karty pre notebooky (CardBus, ExpressCard). Zasunutím vhodnej karty útočník získa prístup priamo na zbernicu a môže napr. pristupovať do operačnej pamäte bez vedomia operačného systému. Ďalším známym problémom bolo rozhranie FireWire (známe tiež ako IEEE 1394). Hoci sa najčastejšie používalo na pripájanie externých zariadení ako napr. digitálne kamery, v skutočnosti, na rozdiel od USB, sa jedná o rozhranie typu zbernica. Jeho prostredníctvom je možné napr. vykonávať aj DMA prenosy, a teda tiež získať prístup do operačnej pamäte bez vedomia operačného systému. Preto je vhodné toto rozhranie zablokovať (ak nie je potrebné) alebo venovať zvýšenú pozornosť fyzickej bezpečnosti.

Kapitola 5

Bezpečnosť ľudských zdrojov

Daniel Olejár

Ľudia sú súčasne najslabším aj najsilnejším prvkom IB v organizácii. Bez ich podpory a spolupráce s nimi sa nepodarí naplniť ciele bezpečnostnej politiky a bezpečnostné opatrenia sa minú účinkom. Vlastní zamestnanci organizácie sú jednou z najčastejších príčin bezpečnostných incidentov. Majú prístup k informačným systémom a informáciám organizácie a buď úmyselne, alebo z nevedomosti, nedbalosti či v dôsledku chyby môžu narušiť systémy alebo údaje organizácie. Ustanovenie manažéra KIB a vytvorenie „bezpečnostného manažmentu“ organizácie je nutnou, ale nie postačujúcou podmienkou úspešnej implementácie bezpečnostnej politiky. Nevyhnutným krokom k dosiahnutiu potrebnej úrovne IB v organizácii je zapojenie všetkých[1] jej zamestnancov, externých spolupracovníkov a zamestnancov tretích strán do procesu KIB. To však predpokladá, že organizácia definuje isté pravidlá správania, oboznámi s nimi zainteresovaných ľudí a bude ich dôsledne presadzovať. V prvej časti tejto kapitoly vychádzajúcej z normy [3] stručne rozoberieme bezpečnostné požiadavky na ľudí a čo by organizácia mala spraviť, aby ich ľudia pôsobiaci v organizácii poznali a dodržiavali. V druhej časti kapitoly sa budeme podrobnejšie zaoberať budovaním bezpečnostného povedomia a vzdelávaním zamestnancov.

5.1 „Životný cyklus“ zamestnanca

Organizácia si môže ušetriť množstvo problémov, keď sa bezpečnostnými požiadavkami na zamestnanca[2] zaoberá ešte pred jeho zamestnaním a nezamestná ľudí, ktorí nemajú potrebnú odbornosť alebo nie sú ochotní dodržiavať pravidlá organizácie. Potrebuje spomedzi kandidátov vybrať ľudí, ktorí [3]

a) rozumejú požiadavkám, ktoré na nich budú kladené,

b) majú predpoklady na úspešné plnenie pracovných úloh a

c) budú loajálni voči organizácii.

Aby organizácia spomedzi kandidátov na pracovnú pozíciu získala vhodného človeka

[1] ale primerane ich pracovnému zaradeniu a vzťahu k IKT

[2] rozumieme pod tým zamestnancov, zamestnancov tretích strán, externých spolupracovníkov

a) v zverejnenej špecifikácii pracovnej pozície jasne uvedie požiadavky na kandidáta (vrátane povinností v KIB, ktoré z pracovnej pozície vyplývajú) a podmienky zamestnania,

b) overí (rešpektujúc súkromie, ochranu osobných údajov a relevantnú legislatívu) či kandidáti vyššie uvedené požiadavky spĺňajú,

c) oboznámi prijatého zamestnanca (týka sa to aj zamestnanca tretej strany pristupujúceho k IKT organizácie) s rolou, do ktorej bol zaradený, povinnosťami a zodpovednosťou, ktoré mu z tejto roly vyplývajú (podmienky) a požiada ho, aby podpísal súhlas s týmito podmienkami[3].

Organizácia musí neustále vytvárať podmienky, aby si zamestnanci (a externí používatelia IKT organizácie) počas zamestnania boli vedomí povinností, ktoré v KIB majú a plnili ich. To znamená, že všetci zamestnanci (a externí používatelia IKT organizácie)

a) musia ešte pred tým, ako získajú prístup k citlivým informáciám a informačným systémom organizácie byť vhodnou formou dostatočne informovaní o bezpečnostných rolách, do ktorých sú zaradení a povinnostiach, ktoré im z tohto zaradenia vyplývajú,

b) dostanú návod, ako plniť povinnosti vyplývajúce zo zaradenia do bezpečnostnej roly,

c) by mali byť motivovaní, aby dodržiavali bezpečnostnú politiku organizácie,

d) by mali dosiahnuť úroveň bezpečnostného povedomia, zodpovedajúcu bezpečnostným rolám, do ktorých sú zaradení,[4]

e) dodriavali pravidlá organizácie, vrátane bezpečnostnej politiky a podmienok pracovnej zmluvy,

d) si na potrebnej úrovni udržiavali kvalifikáciu, znalosti a zručnosti.

Novoprijatý zamestnanec musí ešte pred tým, ako získa prístup k informáciám a systémom organizácie absolvovať úvodné školenie KIB, počas ktorého sa dozvie minimálne

a) o bezpečnostných politikách, cieľoch ktoré tieto politiky sledujú a povinnostiach, ktoré mu z nich vzhľadom na jeho pracovné zaradenie vyplývajú,

b) o organizácii KIB,

c) o bezpečnostných pravidlách, procedúrach, klasifikácii informácie a o narábaní s informáciami,

d) o nahlasovaní bezpečnostných incidentov a postupe pri ich riešení,

e) o disciplinárnych postihoch pri porušení povinností v IB.

[3] keďže podpísanie súhlasu je nutným predpokladom, aby zamestnanec mohol pristupovať k IKT organizácie a vykonávať úlohy, ktoré z jeho pracovného zaradenia vyplývajú, nepodpísanie súhlasu znemožňuje aby nastúpil na pozíciu, o ktorú sa uchádzal

[4] podrobnejšie rozoberieme v podkapitole 5.2

Úvodné školenie samozrejme nebude dlhodobo postačovať a organizácia by mala vytvoriť a zaviesť program (kontinuálneho) budovania/zvyšovania bezpečnostného povedomia zamestnancov, školení a vzdelávania v IB. Tejto problematike je venovaná podkapitola 5.2.

Negatívne stránky informačnej bezpečnosti. Niektoré bezpečnostné opatrenia môžu naraziť na odpor zamestnancov, pretože im sťažujú prácu alebo zasahujú do ich súkromia. V prvom prípade budú mať zamestnanci tendenciu vyhýbať sa opatreniam, aby si zjednodušili život (napr. viacnásobné prihlasovanie sa do systémov a aplikácií), čo sa dá riešiť vysvetlením zmyslu opatrení, kontrolou dodržiavania a uplatnením riešení, ktoré zmiernia negatívne dopady a príliš neoslabia účinnosť opatrení (napr. single sign on—jedno prihlásenie do systémov organizácie[5]). Druhý prípad je zložitejší. Organizácia vynakladá prostriedky na kúpu technických zariadení a aplikácií na to, aby pomocou nich dokázala lepšie plniť svoje úlohy. IKT sa však dajú použiť aj na účely, ktoré od poslania organizácie majú ďaleko (sťahovanie súborov z Internetu, využívanie elektronickej pošty na súkromné účely, hranie hier a pod.) Takéto činnosti v pracovnom čase znižujú výkon zamestnancov a môžu spôsobiť aj problémy organizácii (nelegálna činnosť vykonávaná pomocou počítačov organizácie). Jedným z možných riešení je stanoviť v bezpečnostnej politike zásadu:

> IKT organizácie sa môžu využívať len na pracovné účely. Iné použitie IKT je zakázané.

Takýto striktný zákaz si vyžaduje kontrolu, ktorú môžu zamestnanci považovať za neprimeraný zásah do súkromia (monitorovanie a zaznamenávanie aktivít na Internete, kontrola elektronickej pošty). Aj dokazovanie, že zamestnanec je zodpovedný napr. za poškodenie dobrého mena organizácie posielaním elektronickej pošty alebo diskusiou na sociálnych sieťach môže byť náročné. Miernejšou formou je explicitné vymedzenie zakázaných činností a kontrola záznamov o činnosti zamestnancov[6] v systéme v prípade, keď došlo k bezpečnostnému incidentu.

Napriek všetkým možným opatreniam môže nastať situácia, keď človek zlyhá a spôsobí bezpečnostný incident. Už v prípade chyby môže ísť o porušenie pracovných povinností nehovoriac už o nedbalosti alebo úmyselnom obchádzaní bezpečnostných opatrení, ktoré môžu mať prísnejšiu klasifikáciu (dokonca aj podľa trestného zákona). Pre takéto prípady by organizácia mala mať definovaný **disciplinárny proces** s postihmi, ktoré by odradili úmyselných porušovateľov organizáciou stanovených pravidiel. Postihy by však mali byť nastavené tak, aby neodradili zamestnancov, ktorí spôsobili bezpečnostný incident neúmyselne, priznať si chybu včas a nenechať problém narásť do veľkých rozmerov v nádeji, že sa na ich chybu alebo omyl nepríde.

(Nielen) z hľadiska bezpečnosti je pre organizáciu kritickým obdobím zmena pracovného zaradenia alebo ukončenie zamestnania. Pri zmene pracovného zaradenia sa menia oprávnenia a povinnosti zamestnanca a zamestanec môže organizácii spôsobiť problémy jednak tým, že nedokončí úlohy, ktoré plnil na predchádzajúcej pozícii a jednak môže získať (a zneužiť) neprimerané oprávnenia, ktoré získal tak, že si zachoval práva vyplývajúce z predchádzajúcej a pridal k nim práva vyplývajúce z jeho novej pracovnej pozície. Ukončenie zamestnania, ale aj preradenie na nižšiu pozíciu sa môže prejaviť v zhoršení vzťahu zamestnanca k organizácii

[5] ale nedá sa použiť vo všetkých systémoch, napr. tých, ktoré si vyžadujú silnú, viacfaktorovú identifikáciu a autentizáciu.

[6] z psychologického hľadiska takéto riešenie prijateľnejšie, ale má menší odradzujúci účinok.

a následne aktivitách poškodzujúcich organizáciu. V záujme organizácie je, aby ukončenie a zmeny zamestnania[7] prebiehali riadeným a dobre zdokumentovaným spôsobom. Pre takéto prípady musí mať organizácia pripravené postupy, ktoré zosúlaďujú právne kroky s opatreniami na minimalizáciu bezpečnostných rizík (zablokovanie prístupu dotknutej osoby do systémov, odovzdanie jej autentifikačných prostriedkov, výsledkov práce, zverenej techniky a pamäťových médií).

Zhrnutie.

Každý zamestnanec, ktorý pracuje s IKT musí vedieť, čo má robiť, čo nesmie a prečo. Povinnosti v IB musia byť súčasťou jeho pracovných povinností a pomocou školení sa naučí, ako ich plniť. Organizácia musí mať a uplatňovať postupy pre riešenie problematických situácií (výpoveď, zmena pracovného zaradenia) a zavedený korektný disciplinárny postup pre prípad, keď zamestnanec spôsobí bezpečnostný incident.

5.2 Budovanie bezpečnostného povedomia a vzdelávanie v KIB

Úspešné riešenie úloh, o ktorých sme hovorili v predchádzajúcich častiach, predpokladá, že všetci zamestnanci organizácie majú potrebné znalosti z IB pre plnenie svojich povinností a vedia ich v práci používať. To je ideálny stav, ku ktorému je potrebné sa dopracovať. Našťastie pre organizáciu, nemusia všetci jej zamestnanci byť odborníkmi v KIB. V tejto časti popíšeme systém (program) budovania bezpečnostného povedomia a prípravy ľudí na plnenie úloh v IB. Budeme vychádzať z metodiky materiálov NIST [5],[6] a [4].

Znalostné potreby v KIB tvoria vo väčšine organizácií trojúrovňovú pyramídu: na zaistenie potrebnej úrovne KIB organizácia potrebuje, aby

1. mali všetci zamestnanci (vrátane externých) dostatočnú úroveň bezpečnostného povedomia,
2. ľudia zaradení do bezpečnostných rôl mali znalosti, zručnosti a schopnosti potrebné na vykonávanie povinností, ktoré im z tohto zaradenia vyplývajú,
3. mala organizácia špecialistov v KIB, potrebných na manažment KIB, resp. riešenie špecifických úloh IB.

Základom tejto pyramídy je bezpečnostné povedomie (awareness). Cieľom aktivít zameraných na budovanie/zvyšovanie bezpečnostného povedomia je zmena/budovanie postoja ľudí ku KIB; a nie získanie konkrétnych vedomostí alebo zručností. Dostatočná úroveň bezpečnostného povedomia v organizácii znamená, že zamestnanci organizácie poznajú význam a potrebu KIB a uvedomujú si svoju spoluzodpovednosť za KIB v organizácii (prípadne aj širšiu—napr. na Internete). Na budovanie a udržiavanie bezpečnostného povedomia zamestnancov sa dajú využiť popularizačné prednášky, webové stránky, diskusné fóra, rozposielanie noviniek (newsletters), súťaže, e-maily, bannery, postery a i.

[7] primerane sa to vzťahuje na zamestnancov tretích strán pôsobiacich v organizácii, externistov a brigádnikov

Medzi budovaním bezpečnostného povedomia a špecifickou odbornou prípravou zameranou na ľudí zaradených do rôl, existuje medziúroveň, ktorú v dokumentoch [5],[6] označujú ako základy IB a bezpečnostnej gramotnosti (Security Basics and Literacy). Obsahom sú všeobecné poznatky z KIB, ktorých zvládnutie na jednej strane prispieva k prehĺbeniu bezpečnostného povedomia (ľudia majú konkrétnejšiu predstavu o problémoch a riešeniach KIB) a na druhej strane je predpokladom pre ďalšie špecializované vzdelávanie. Obsah Základov uvádzame v prílohe 5.3.1.

Druhú úroveň znalostnej pyramídy predstavuje odborná príprava ľudí ľudí zaradených do rôl. Ide o nešpecialistov v KIB a ich odborná príprava je zameraná na získanie vybraných špecifických znalostí a zručností, resp. rozvoj schopností potrebných na vykonávanie špecifických povinností vyplývajúcich z rôl, do ktorých sú v organizácii zaradení. Dokument [5] uvádza 7 generických a vyše 30 špecifických bezpečnostných rôl. Vypracovať obsah kurzov, študijné materiály pre tak veľký počet rôl nie je v našich podmienkach reálne. Preto sme dospeli k piatim základným kategóriám používateľov

1. laický používateľ IKT,
2. vedúci pracovník organizácie,
3. informatik, ktorý sa nešpecializuje v KIB,
4. manažér KIB,
5. lektor KIB.

Pre niektoré kategórie používateľov sme išli ešte o úroveň nižšie a definovali v nich roly, pre ktoré sme následne špecifikovali (podobným spôsobom ako v [5] a [6]) znalostné potreby. Na rozdiel od [5] sme pri špecifikácii znalostných potrieb jednotlivých rolí vychádzali z delenia KIB na oblasti podľa ISO normy [3]. Dôvodom je, že uvedená norma (a celá séria ISO/IEC 27xxx) sa v riadení informačnej bezpečnosti široko používa a premietla sa aj do slovenských legislatívnych noriem. Navyše, je obsahovo kompatibilná de-facto obsahovými štandardami IB—[1] a [2]. Navrhované obsahové rozdelenie KIB sme zachovali aj po vydaní novej verzie normy [3], v ktorej boli niektoré oblasti IB rozčlenené a preusporiadané.

Znalostné potreby ľudí zaradených do základných rôl sme obsahovo rozdelili na nasledujúce oblasti:

1. Legislatíva a štandardy IB
2. Riadenie KIB
3. Riadenie rizík
4. Obstarávanie, vývoj a zmeny IKT systémov
5. Fyzická bezpečnosť
6. Riadenie prístupu
7. Bezpečnosť komunikácie

8. Správa bezpečnostných incidentov
9. Prevádza IKT systémov a kontinuita činnosti
10. Audit informačnej bezpečnosti

Znalostné štandardy pre jednotlivé kategórie používateľov (a roly) sú uvedené v prílohe 5.2.

Vrcholom znalostnej pyramídy sú špecialisti KIB s vysokoškolským vzdelaním v KIB. Dokument [5] zdôrazňuje, že na rozdiel od špecializovanej odbornej prípravy zameranej na špecifickú oblasť, je štúdium KIB komplexné, integruje znalosti a zručnosti rôznych špecializácií do jedného celku, má teoretický základ a široký kontext a pripravuje odborníkov schopných riešiť nielen známe problémy štandardným spôsobom, ale nachádzať aj originálne riešenia, mať predstavu o budúcom vývoji a vedieť naň organizáciu včas pripraviť.[8]

Organizácia by potrebovala minimálne kalifikovaného manažéra kybernetickej a informačnej bezpečnosti a podľa zamerania a systémov, ktoré vlastní, možno aj iných špecialistov KIB. Hoci na niektorých slovenských univerzitách (minimálne UK Bratislava a STU Bratislava) sa informačná bezpečnosť vyše 20 rokov ponúka ako špecializácia v rámci informatických študijných programov a v posledných rokoch a týchto školách pripravili a otvorili (STU) aj samostatné akreditované študijné programy informačnej bezpečnosti, vysoké školy zatiaľ nepripravujú dostatočný počet potrebných špecialistov na informačnú bezpečnosť. Navyše, doterajšie skúsenosti s výučbou informačnej bezpečnosti ukázali, že študenti chápu problémy technického charakteru, ale majú problém s právnymi a manažérskymi otázkami, pre pochopenie ktorých im chýbajú skúsenosti z fungovania reálnych organizácií. Manažérov informačnej bezpečnosti, audítorov, špecialistov na ochranu osobných údajov, čiastočne vyšetrovateľov počítačovej kriminality bude asi potrebné pripravovať v postgraduálnom vzdelávaní.[9]

5.3 Príloha. Znalostné štandardy pre oblasť KIB

Prvá časť tejto prílohy obsahuje zoznam tém, vhodných na zvyšovanie bezpečnostného povedomia. V ďalších častiach sú uvedené charakteristiky rôl[10] a používateľov IKT a minimálne znalostné požiadavky na jednotlivé roly. Pri kategorizácii používateľov IKT a stanovení rôl sme vychádzali zo zloženia zamestnancov v organizáciách verejnej správy; v iných organizáciách bude možno iné zloženie zamestnancov, ale (až na špecifické prípady) by navrhované roly mali postačovať na zaradenie väčšiny zamestnancov.

5.3.1 Základy IB

Táto časť obsahuje zoznam tém[11], ktoré autori [6] považujú za vhodné zaradiť do programu zvyšovania bezpečnostného povedomia pre všetkých zamestnancov organizácie, resp. ako pre-

[8] The „Education“ level integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge, adds a multidisciplinary study of concepts, issues, and principles (technological and social), and strives to produce IT security specialists and professionals capable of vision and pro-active response.

[9] na prípravu postgraduálneho vzdelávania v IB je zameraný rozvojový projekt 002UK-2-1/2018, v rámci ktorého bola vytvorená aj táto učebnica

[10] rola, roly, skloňovanie podľa vzoru žena

[11] doplnených o niektoré aktuálne témy

rekvizity pre špecializované školenia. Na rozdiel od základných pojmov a oblastí IB, ktoré sme uviedli v kapitole 2 zoznam obsahuje konkrétne témy bez snahy usporiadať ich do nejakých celkov.

- použitie a manažment hesiel—vytváranie hesiel, slabé a silné heslá, frekvencia zmien hesiel, ochrana hesiel
- typy škodlivého kódu, prejavy, spôsoby šírenia a ochrana pred ním,
- Bezpečnostná politika—dôsledky nedodržiavania alebo nesúladu,
- neznáme e-maily a prílohy,
- používanie webu—dovolené, nepovolené; monitorovanie aktivít používateľov;
- spam,
- zálohovanie a uchovávanie údajov—centralizované, decentralizované, cloudové riešenia,
- sociálne inžinierstvo
- reakcia na incident—koho mám kontaktovať, čo mám robiť?
- shoulder surfing—odčítavanie citlivej informácie zadávanej z klávesnice, napr. hesiel
- zmeny v prostredí systému—nárast rizík vyplývajúcich z hrozieb voči systému a údajom (voda, prach, špina, fyzický prístup)
- inventarizácia a vyraďovanie zariadení—kto je zodpovedný za vymazávanie pamäťových médií?
- využívanie systémov organizácie na osobné účely (mail, web) a na druhej strane práca doma (na súkromných zariadeniach)
- bezpečnosť prenosných zariadení—fyzická bezpečnosť, bezpečnosť bezdrôtového spojenia
- šifrovanie a prenos citlivej informácie po Internete (prístup organizácie, procedúry, technická asistencia)
- bezpečnosť mobilných zariadení na služobných cestách (fyzická aj KIB)
- použitie vlastných systémov a softvéru pri práci—je povolené? (copyright)
- včasné nasadzovanie softvérových záplat—časť manažmentu konfigurácie
- licenčné obmedzenia na softvér—čo sa môže a čo nie
- podporovaný/povolený softvér na systémoch organizácie—časť manažmentu konfigurácie
- riadenie prístupu—princíp najmenších privilégií a separácia rôl
- individuálna zodpovednosť za činnosť (accountability)—čo to znamená pre organizáciu
- súhlasné vyjadrenia (acknowledgement statements)

- kontrola návštevníkov a fyzického prístupu do priestorov—použiteľné politiky fyzickej bezpečnosti a procedúry
- bezpečnosť pracovných staníc—šetriče obrazovky, obmedzenie možnosti návštevníka vidieť na monitor, UPS, prístup do systému
- ochrana dôvernosti údajov—v systémoch, archíve, na záložných médiách, v tlačenej podobe a i.
- etiketa hromadnej elektronickej pošty
- osobné údaje—ochrana, práva dotknutých osôb.

5.3.2 Laici

Laici sú ľudia bez systematického informatického vzdelania, ktorí používajú IKT systémy a najmä aplikácie ako nástroje na plnenie svojich pracovných úloh, ale v IKT systéme majú zvyčajne minimálne oprávnenia, postačujúce na plnenie ich základných pracovných povinností (majú právo využívať vybrané aplikácie, údaje, ale nemajú oprávnenie napr. inštalovať softvér, meniť konfiguráciu systému a pod.) V organizáciách verejnej správy laici sú zaradení do roly neprivilegovaných používateľov.

Rola: Neprivilegovaný používateľ

Charakteristika roly. V organizáciách je spravidla používateľom IKT systémov, používa ich na plnenie svojich pracovných povinností, pričom prístup do IKT systémov a k ich údajom má obmedzený na konkrétne operácie v súlade s definovanými oprávneniami. Neprivilegovaný používateľ IKT systémov spravidla nemá oprávnenie zasahovať do ich konfigurácie, inštalovať programy a pod.

Znalostný štandard

1. Prerekvizity. Ovláda základy IB. Pozná základné pojmy IB.
2. Legislatíva a štandardy IB
   a) Má základnú právnu orientáciu v informačnej bezpečnosti (trestný zákon, autorský zákon, zákon o ochrane osobných údajov, zákon o utajovaných skutočnostiach a pod.).
   b) Pozná právne požiadavky na používanie IKT systémov organizácie a etické zásady správania sa v digitálnom priestore.
   c) Dokáže identifikovať údaje v IKT systémoch s ktorými pracuje a ktoré vyžadujú osobitnú ochranu vyplývajúcu z právnych požiadaviek.
3. Riadenie KIB. Pozná v primeranej miere špecifické pravidlá vlastnej organizácie—napríklad bezpečnostnú politiku, štandardy, použité bezpečnostné opatrenia, konkrétne postupy pri nahlasovaní a riešení bezpečnostných incidentov, havarijné plány a pod.
4. Riadenie rizík—bez špecifických požiadaviek v tejto oblasti

5. Obstarávanie, vývoj a zmeny IKT systémov. Je schopný vyjadriť stanovisko k používateľskej prijateľnosti (akceptovateľnosti) obstarávaných, vyvíjaných alebo zmenených IKT systémov

6. Fyzická bezpečnosť

   a) Pozná zásady fyzickej bezpečnosti.

   b) Dokáže v praxi uplatňovať konkrétne pravidlá fyzickej bezpečnosti organizácie.

7. Riadenie prístupu

   a) Pozná rôzne prostriedky autentizácie (heslá, PIN kódy, tokeny, biometria), vie ich používať, pozná zásady ochrany autentizačných prostriedkov.

   b) Pozná základné techniky sociálneho inžinierstva, vie ich identifikovať a správne na ne reagovať (prezrádzanie hesiel, „phishing“ a pod.).

8. Bezpečnosť komunikácie

   a) Pozná základné požiadavky na ochranu počítačov a iných zariadení v sieti.

   b) Rozumie rizikám práce na Internete, ich dôsledkom a osvojil si zásady bezpečnej práce na Internete: elektronická pošta (spam, prílohy a pod.), šírenie infiltrácií (počítačové vírusy, malware, spyware a pod.), počítačové pirátstvo (sťahovanie nelegálneho obsahu).

9. Správa bezpečnostných incidentov. Dokáže vhodne reagovať a konať v súlade s postupmi definovanými pre bezpečnostné incidenty, ako aj primerane reagovať na bezpečnostné a iné upozornenia IKT systémov (aplikácií, operačného systému, antivírusového programu a pod.).

10. Prevádzka IKT systémov a kontinuita činnosti

    a) Rozumie základným typom a mechanizmom bezpečnostných opatrení v IKT systémoch.

    b) Pozná význam, spôsob zálohovania a obnovy vlastných súborov.

11. Audit

    a) Pozná význam auditu.

    b) Je schopný vyjadriť sa k používateľskej prijateľnosti ním používaných IKT systémov a jeho sa týkajúcich bezpečnostných opatrení

5.3.3 Manažéri a vedúci zamestnanci organizácie

Manažéri a vedúci zamestnanci (s výnimkou manažérov IT) sú z hľadiska informatických a informačno-bezpečnostných znalostí špeciálnou podkategóriou laikov. Na jednej strane spravidla nemajú systematické vedomosti o IKT, na druhej strane zodpovedajú za ochranu aktív organizácie, ktoré sú v ich pôsobnosti. Zároveň rozhodujú o bezpečnostnej politike organizácie (bez ohľadu na to, či je explicitne formulovaná), prostriedkoch na jej realizáciu, riadení KIB a pod. Manažéri a vedúci zamestnanci sú často zodpovední za naplnenie legislatívnych

požiadaviek na KIB v organizácii (napr. požiadavky súvisiace s ochranou osobných údajov, utajovaných skutočností, ochranou kritickej infraštruktúry a pod.). V organizáciách verejnej správy manažéri a vedúci zamestnanci sú zaradení do spoločnej roly roly vedúcich zamestnancov.

Rola: Vedúci zamestnanec

Charakteristika roly. Zamestnanec vo vedúcej pozícii, ktorý nie je manažérom IT alebo manažérom informačnej bezpečnosti. Spravidla zodpovedá za organizáciu ako celok (alebo za jej významnú časť), v konečnom dôsledku zodpovedá aj za plnenie úloh v oblasti KIB vo vnútri organizácie.

Znalostný štandard

1. Prerekvizity. Ovláda znalosti a zručnosti požadované znalostným štandardom pre laikov vo všetkých oblastiach. Tento štandard uvádza preto len požiadavky, ktoré sú navyše.

2. Legislatíva a štandardy KIB

   a) Vie o existencii a náplni štandardov upravujúcich jednotlivé oblasti KIB (rad ISO 2700x a pod.).

   b) Pozná legislatívu relevantnú pre informačné systémy a spracúvané údaje vo vlastnej organizácii (zákon o ochrane utajovaných skutočností, zákon o kybernetickej bezpečnosti, zákon o IT vo VS, zákon o elektronických komunikáciách, nariadenia GDPR, eIDAS, direktíva NIS, zákon o kritickej infraštruktúre a pod.) ako aj povinnosti, ktoré z tejto legislatívy vyplývajú pre organizáciu v ktorej pôsobí .

3. Riadenie KIB

   a) Vie identifikovať hlavné informačné aktíva organizácie.

   b) Pozná základné pojmy KIB, ich význam a vie ich aplikovať na vlastnú organizáciu.

   c) Pozná potrebu a zásady systematického riadenia kybernetickej a informačnej bezpečnosti, pozná štruktúru bezpečnostnej politiky a dokáže pre jej vypracovanie a implementáciu vytvoriť v rámci svojich kompetencií v organizácii primerané podmienky a zakomponovať KIB do informačných procesov organizácie.

   d) Dokáže stanoviť priority KIB v organizácii (z hľadiska plánovania, prijímaných opatrení, ošetrenia rizík a pod.).

   e) Dokáže stanoviť zodpovednosti pracovníkov organizácie v oblasti KIB a včleniť ich do ich pracovných náplní.

   f) Dokáže kontrolovať plnenie úloh v KIB v okruhu svojej pôsobnosti.

4. Riadenie rizík

   a) Dokáže posúdiť dôsledky výpadku, straty, zničenia, poškodenia alebo kompromitácie aktív organizácie.

b) Pozná základné pojmy riadenia rizík, ich význam a vie ich aplikovať na vlastnú organizáciu: hrozba, zraniteľnosť, bezpečnostný incident, opatrenie, analýza rizík, ošetrenie rizika a pod.

c) Pozná základné metódy ošetrenia rizík a vie určiť hranice akceptovateľného rizika.

d) Dokáže presadzovať primerané bezpečnostné požiadavky vo vzťahu k tretím stranám (pozná bezpečnostnú politiku vlastnej organizácie, hrozby vyplývajúce z prístupu tretích strán do systémov organizácie a opatrenia nevyhnutné na elimináciu alebo zníženie súvisiacich rizík).

5. Obstarávanie, vývoj a zmeny IKT systémov. Rozumie bezpečnostným požiadavkám súvisiacimi so zmenami, vývojom, obstarávaním a zavádzaním IKT systémov a dokáže ich zohľadniť pri plánovaní ďalšieho rozvoja IKT organizácie.

6. Fyzická bezpečnosť—bez špecifických dodatočných požiadaviek v tejto oblasti

7. Riadenie prístupu. Dokáže definovať ktorí pracovníci prípadne tretie strany majú mať prístup k funkciám informačných systémov a údajom v nich.

8. Bezpečnosť komunikácie—bez špecifických dodatočných požiadaviek v tejto oblasti

9. Správa bezpečnostných incidentov. Pozná význam správy bezpečnostných incidentov a dokáže vhodne reagovať v prípade výskytu závažných incidentov s dopadom na činnosť alebo povinnosti organizácie.

10. Prevádza IT systémov a kontinuita činnosti

    a) Rozumie bezpečnostným požiadavkám súvisiacimi so prevádzkou IT systémov a dokáže ich zohľadniť pri riadení organizácie.

    b) Rozumie požiadavkám na kontinuitu činnosti IT a dokáže stanoviť jej základné rámce

11. Audit. Rozumie úlohe a významu auditu, dokáže rámcovo stanoviť ciele auditu a dokáže interpretovať hlavné výsledky auditu.

Informatici, ktorí sa nešpecializujú v informačnej bezpečnosti

Informatici, ktorí IKT systémy vyvíjajú, spravujú po technickej stránke, alebo riadia IT procesy v súlade s potrebami organizácie, implementujú a udržiavajú bezpečnostné opatrenia, ale priamo nezodpovedajú za kybernetickú a informačnú bezpečnosť. Vo verejnej správe v tejto kategórii pôsobia informatici v dvoch rolách

1. manažéri IT a

2. správcovia informačných a komunikačných technológií.

Rola: Manažér IT

Charakteristika roly. Vedúci oddelenia, odboru alebo inej organizačnej jednotky zodpovednej za IT (v ďalšom oddelenie IT) v organizácii, ktorá môže ale nemusí mať špecializovaných pracovníkov zaoberajúcich sa informačnou bezpečnosťou. IT manažér riadi prevádzku IKT a v spolupráci s inými vedúcimi pracovníkmi organizácie plánuje a realizuje rozvoj IKT systémov organizácie.

Znalostný štandard

1. Prerekvizity.
   a) Ovláda znalosti a má zručnosti požadované znalostným štandardom pre laikov vo všetkých oblastiach. Tento štandard uvádza preto len požiadavky, ktoré sú navyše.
   b) IT manažér vie o úlohách a zodpovednostiach vedúceho pracovníka a špecialistov na KIB v organizácii do takej miery, ktorá umožní efektívnu komunikáciu s vedením organizácie a spoluprácu pri zabezpečovaní potrieb KIB v organizácii.
2. Legislatíva a štandardy KIB
   a) Pozná základné štandardy, odporúčania a najlepšie praktiky IB pre jednotlivé oblasti IB (rad ISO 270xx a pod.) a je schopný interpretovať ich požiadavky v prostredí IT systémov v oblasti svojej pôsobnosti.
   b) Pozná legislatívu relevantnú pre informačné systémy a spracúvané údaje vo vlastnej organizácii (zákon o ochrane utajovaných skutočností, zákon o IT vo VS, zákon o elektronických komunikáciách, nariadenia GDPR, eIDAS, smernica NIS, zákon o kybernetickej bezpečnosti, zákon o kritickej infraštruktúre a pod.) ako aj povinnosti, ktoré pre organizáciu v ktorej pôsobí, z tejto legislatívy vyplývajú.
3. Riadenie KIB
   a) Pozná základné pojmy KIB, ich význam a vie ich aplikovať na IKT systémy vo vlastnej organizácii, napríklad aktívum, integrita, dôvernosť, autentickosť, dostupnosť, súkromie, preukázateľnosť, neodmietnuteľnosť pôvodu a prijatia a pod.
   b) Vie klasifikovať informačné aktíva podľa klasifikačnej schémy.
   c) Má znalosti umožňujúce podieľať sa na tvorbe bezpečnostnej politiky organizácie (dokáže identifikovať hlavné informačné aktíva, posúdiť realizovateľnosť/dôsledky navrhovanej úrovne ich ochrany, určiť, aká informácia sa v akých systémoch spracováva, formulovať požiadavky na neinformatické zložky organizácie vyplývajúce zo stanovených bezpečnostných cieľov a pod.).
   d) Vie v oblasti svojej pôsobnosti spracovať špecifikáciu, zaistiť vypracovanie a presadiť implementáciu bezpečnostnej dokumentácie nižšej úrovne, ktorá rozpracováva bezpečnostnú politiku organizácie (bezpečnostné štandardy).
   e) Dokáže stanoviť a priradiť konkrétne zodpovednosti za výkon a prevádzku bezpečnostných opatrení pracovníkom IT oddelenia organizácie.
4. Riadenie rizík

a) Pozná základné pojmy riadenia rizík, ich význam a vie ich aplikovať na vlastnú organizáciu: hrozba, zraniteľnosť, opatrenie, analýza rizík, ošetrenie rizika a pod.

b) Dokáže posúdiť dôsledky výpadku, straty, zničenia, poškodenia alebo kompromitácie aktív organizácie v oblasti svojej pôsobnosti.

c) Vie vypracovať (sám alebo v spolupráci s manažérom KIB) zadanie pre analýzu rizík a bezpečnostný projekt IKT systémov v jeho pôsobnosti pre interných alebo externých expertov, komunikovať s nimi pri realizácii zadanej úlohy a posúdiť kvalitu výstupných dokumentov.

d) Dokáže ohodnotiť riziko a pozná metódy ošetrenia rizík.

e) Vie posúdiť dopad navrhovaných bezpečnostných opatrení (náklady, technické zabezpečenie, organizačné dôsledky, legislatíva).

f) Vie vyhodnotiť účinnosť a efektívnosť prijatých opatrení.

5. Obstarávanie, vývoj a zmeny IKT systémov.

a) Vie špecifikovať, prípadne posúdiť základné bezpečnostné požiadavky na obstarávaný alebo vyvíjaný systém (zohľadňujúc prostredie, v ktorom bude pôsobiť), vrátane postupov pri jeho vývoji a testovaní.

b) Na základe podkladov (od dodávateľa, správcu IKT systémov, špecialistov informačnej bezpečnosti a pod.) dokáže posúdiť, či dodaný systém spĺňa bezpečnostné požiadavky, ktoré boli preň definované.

6. Fyzická bezpečnosť

a) Pozná pravidlá fyzickej bezpečnosti v organizácii a v oblasti svojej pôsobnosti dokáže zabezpečiť ich naplnenie.

b) Dokáže zabezpečiť implementáciu bezpečnostných opatrení, týkajúcich sa fyzickej bezpečnosti komponentov IKT systémov (zahŕňajúcich dátové centrá, stolné aj prenosné počítače používateľov, mobilné prostriedky IKT a pod.).

7. Riadenie prístupu.

a) Rozumie základným pojmom a vie ich aplikovať v konkrétnom prostredí: separácia právomocí, princíp štyroch očí, princíp najmenších privilégií, a pod.

b) Dokáže zabezpečiť implementáciu opatrení týkajúcich sa riadenia prístupu v jednotlivých IKT systémoch (prístupy k informačným systémom, prístupy k sieťovým a iným IKT zdrojom, prístupy tretích strán).

8. Bezpečnosť komunikácie

a) Rozumie základným požiadavkám na bezpečnosť komunikácie a vie akými metódami a prostriedkami sa v IKT zabezpečujú. Rozumie tomu, čo opatrenia zabezpečujú a za akých podmienok.

b) Dokáže zabezpečiť implementáciu opatrení týkajúcich sa bezpečnosti komunikácie v jednotlivých IKT systémoch (komunikácia s externými subjektmi, prístup k IKT systémom zvnútra a zvonku organizácie, prístup tretích strán).

9. Správa bezpečnostných incidentov.

   a) Pozná význam správy bezpečnostných incidentov a dokáže klasifikovať závažnosť incidentov.

   b) Vie v oblasti svojej pôsobnosti spracovať zadanie, zaistiť vypracovanie a presadiť implementáciu postupov pri riešení bezpečnostných incidentov v IKT systémoch v súlade s pravidlami a postupmi pri správe incidentov v organizácii.

10. Prevádza IT systémov a kontinuita činnosti

    a) Pozná význam zabezpečenia kontinuity činností, pozná štruktúru havarijných plánov a plánov kontinuity činností a rozumie základným pojmom v tejto oblasti (RPO, RTO, MTO a pod.).

    b) Rozumie základným metódam a opatreniam pre zabezpečenie kontinuity činnosti a ich obmedzeniam.

    c) Vie v oblasti svojej pôsobnosti spracovať zadanie, zaistiť vypracovanie a presadiť implementáciu havarijných plánov a plánov kontinuity činnosti IKT systémov, pričom zohľadní potreby organizácie (vyplývajúce z jej úloh).

    d) Dokáže zohľadniť úlohy organizácie ako aj plány iných útvarov organizácie pri vypracovaní havarijných plánov a plánov kontinuity činnosti v IKT oblasti.

    e) Dokáže zabezpečiť praktické testovanie plánov.

11. Audit. Pozná ciele a postupy bezpečnostného auditu, dokáže spolupracovať s audítormi a interpretovať výsledky auditu.

Rola: Správca IKT systémov

Charakteristika roly. Odborník s informatickým vzdelaním, zodpovedný za správu IKT

Znalostný štandard

1. Prerekvizity. Ovláda znalosti a má zručnosti požadované znalostným štandardom pre laikov vo všetkých oblastiach. Tento štandard uvádza preto len požiadavky, ktoré sú navyše.

2. Legislatíva a štandardy KIB

   a) Pozná legislatívu relevantnú pre informačné systémy a spracúvané údaje vo vlastnej organizácii (zákon o ochrane utajovaných skutočností, zákon o IT vo VS, zákon o elektronických komunikáciách, nariadenia GDPR, eIDAS, zákon o kybernetickej bezpečnosti, zákon o kritickej infraštruktúre a pod.) ako aj povinnosti, ktoré pre organizáciu v ktorej pôsobí, z tejto legislatívy vyplývajú.

   b) Dokáže splniť povinnosti vyplývajúce z legislatívy a v prípade, ak to presahuje jeho kompetencie, vypracovať v spolupráci s manažérom IT kvalifikovaný návrh pre vedenie organizácie.

   c) Pozná bezpečnostné štandardy relevantné pre IT systémy v oblasti jeho pôsobnosti.

3. Riadenie KIB

   a) Pozná základné pojmy KIB, ich význam a vie ich aplikovať na IKT systémy vo vlastnej organizácii, napríklad aktívum, integrita, dôvernosť, autentickosť, dostupnosť, súkromie, preukázateľnosť, neodmietnuteľnosť pôvodu a prijatia a pod.

   b) Pre systém dokáže rozpracovať bezpečnostnú politiku organizácie do konkrétnych postupov (praktík); pri tvorbe bezpečnostnej politiky organizácie dokáže posúdiť návrh z hľadiska potrieb systému, resp. dopad návrhu na systém.

   c) Pozná klasifikačnú schému a vie podľa nej klasifikovať systémové údaje, za ktoré je zodpovedný (heslá, konfiguračné súbory); vie implementovať potrebné opatrenia na ochranu klasifikovanej informácie používanej v systéme (ochrana prístupu, označovanie, procedúry na spracovanie klasifikovanej informácie v systéme).

4. Riadenie rizík

   a) Pozná základné pojmy riadenia rizík, ich význam a vie ich aplikovať na systémy, ktoré spravuje: hrozba, zraniteľnosť, opatrenie, analýza rizík, ošetrenie rizika a pod.

   b) Dokáže samostatne, prípadne v spolupráci s manažérom KIB spracovať zadanie na bezpečnostný projekt, resp. analýzu rizík systému a spolupracovať pri ich realizácii.

   c) Vie posúdiť relevantnosť hrozieb voči systému, zohľadniac požiadavky na systém vyplývajúce z legislatívy, bezpečnostnej politiky organizácie, štandardov a zraniteľnosti systému.

   d) Dokáže ohodnotiť riziká identifikované počas analýzy rizík.

   e) Dokáže posúdiť úplnosť a adekvátnosť analýzy rizík/bezpečnostného projektu systému, najmä vhodnosť a použiteľnosť navrhovaných opatrení.

   f) Dokáže implementovať navrhované bezpečnostné opatrenia v systéme, ktorý spravuje.

5. Obstarávanie, vývoj a zmeny IKT systémov.

   a) Ovláda životný cyklus systému a pozná bezpečnostné požiadavky na systém v jednotlivých fázach jeho životného cyklu.

   b) Pre nové systémy, ktoré má v budúcnosti spravovať, dokáže špecifikovať kapacitné požiadavky a základné bezpečnostné požiadavky.

   c) Vie posúdiť do akej miery sú bezpečnostné požiadavky splnené v navrhovaných riešeniach.

   d) Pri vývoji/dodávke/úpravách systému pozná význam oddelenia vývojového, testovacieho a produkčného prostredia a vie primerane zabezpečiť ochranu jednotlivých prostredí vrátane údajov v nich uložených.

   e) Vie sformulovať bezpečnostné požiadavky na dodávateľov systému (dodávka, servis, iné služby).

   f) Dokáže posúdiť dopad zavedenia nového systému na existujúce systémy (aspoň na tie, za ktoré zodpovedá).

6. Fyzická bezpečnosť. Dokáže posúdiť potreby fyzického zabezpečenia systému, posúdiť stav fyzickej ochrany a adekvátnosť možných opatrení; vie sformulovať požiadavky na bezpečnostné okolie (o.i. pracovné stanice používateľov) systému.

7. Riadenie prístupu.

   a) Rozumie pojmom v oblasti riadenia prístupu a pozná význam riadenia prístupu a spôsoby jeho zabezpečenia.

   b) Efektívne spravuje používateľov systému; pre systém dokáže definovať roly, kritériá na zaradenie používateľov do rôl a vypracovať procedúry na zaradenie/vyradenie používateľa do/z roly.

   c) Dokáže implementovať opatrenia týkajúce sa riadenia prístupu v systémoch, ktoré spravuje.

8. Bezpečnosť komunikácie

   a) Ovláda bezpečnostné aspekty IKT—bezpečnosť sieťového prostredia, operačných systémov, bezpečnosť databázových systémov, bezpečnosť web systémov (všeobecne a detailne bezpečnostné aspekty systému, ktorý spravuje)

   b) Pozná a vie používať technológie sieťovej bezpečnosti.

   c) Ovláda základy kryptológie a PKI (používanie kryptografických techník a prostriedkov, vrátene správy kryptografických kľúčov).

9. Správa bezpečnostných incidentov.

   a) Pozná význam správy bezpečnostných incidentov a dokáže klasifikovať závažnosť incidentov týkajúcich sa systémov, ktoré spravuje.

   b) Dokáže spracovať a zaviesť do používania postupy pre riešenie bezpečnostných incidentov zasahujúcich systémy, ktoré spravuje.

10. Prevádzka IT systémov a kontinuita činnosti

    a) Pri prevádzke systému pozná a vie zabezpečiť dodržiavanie pravidiel pre narábanie s médiami, výmenu informácií s tretími stranami, monitorovanie aktivít v systéme a pre vytváranie, ochranu a spracovanie záznamov auditu.

    b) Pozná princípy fungovania rozličných typov škodlivého kódu a spôsob ochrany proti nim.

    c) Pozná význam zabezpečenia kontinuity činností a rozumie základným pojmom v tejto oblasti.

    d) Na základe odborného usmernenia dokáže zdokumentovať čiastkové plány kontinuity činnosti na úrovni ním vykonávaných alebo zabezpečovaných postupov, vrátane havarijných plánov a plánov obnovy pre systém, ktorý spravuje.

    e) Rozumie potrebe overovania postupov obnovy a zabezpečenia kontinuity a je schopný prakticky overiť postupy dotýkajúce sa systémov, ktoré spravuje.

    f) Má odborné poznatky potrebné na prevádzkovanie systémov, ktoré spravuje, v súlade s plánmi zabezpečenia kontinuity činnosti.

11. Audit.

    a) Pozná požiadavky na hodnotenie bezpečnosti systémov: audit a certifikácia, self-assessment v KIB.

    b) Dokáže spolupracovať s audítormi pri audite systémov, ktoré spravuje.

5.3.4 Špecialisti v informačnej bezpečnosti

Do tejto kategórie patria v prvom rade manažéri kybernetickej a informačnej bezpečnosti rozličných úrovní, audítori IKT systémov a produktov, operátori bezpečnostných technológií, bezpečnostní analytici, vyšetrovatelia špecializujúci sa na počítačovú kriminalitu. Vo verejnej správe pôsobia v štyroch rolách

1. manažéri kybernetickej a informačnej bezpečnosti
2. operátori bezpečnostných technológií (špecialisti zameraní na bezpečnosť konkrétnych IKT oblastí alebo na konkrétne bezpečnostné technológie)
3. audítori
4. bezpečnostní analytici

Rola: Manažér kybernetickej a informačnej bezpečnosti

Charakteristika roly. Vedúci pracovník, špecializovaný pre oblasť informačnej bezpečnosti. Najvyššia odborná autorita pre IB v organizácii. Je vlastníkom bezpečnostnej politiky organizácie a zodpovedá za jej správu a v spolupráci s pracovníkmi vlastného útvaru (ak taký v organizácii existuje) a/alebo s inými pracovníkmi aj za jej rozpracovanie a uplatňovanie. Samostatná pozícia manažétra KIB a/alebo útvar manažéra KIB existuje spravidla vo väčších organizáciách.

Znalostný štandard

1. Prerekvizity. Ovláda znalosti a má zručnosti požadované znalostným štandardom pre laikov vo všetkých oblastiach. Tento štandard uvádza preto len požiadavky, ktoré sú navyše.
2. Legislatíva a štandardy KIB

    a) Pozná základné štandardy, odporúčania a najlepšie praktiky KIB pre jednotlivé oblasti KIB (rad ISO 2700x, CObIT a pod.) a je schopný interpretovať ich požiadavky v prostredí IT systémov v oblasti svojej pôsobnosti.

    b) Pozná legislatívu relevantnú pre informačné systémy a spracúvané údaje vo vlastnej organizácii (zákon o ochrane utajovaných skutočností, zákon o IT vo VS, zákon o elektronických komunikáciách, nariadenia GDPR, eIDAS, smernicu NIS, zákon o kybernetickej bezpečnosti, zákon o kritickej infraštruktúre a pod.) ako aj povinnosti, ktoré pre organizáciu v ktorej pôsobí, z tejto legislatívy vyplývajú.

c) Dokáže splniť povinnosti vyplývajúce z legislatívy a v prípade, ak to presahuje jeho kompetencie, vypracovať v spolupráci s manažérom IT kvalifikovaný návrh pre vedenie organizácie.

3. Riadenie KIB

a) Pozná a orientuje sa v jednotlivých oblastiach IB.

b) Dokáže sformulovať návrh bezpečnostnej politiky organizácie.

c) Dokáže vypracovať alebo riadiť vypracovanie bezpečnostného projektu a ďalších formálnych dokumentov v súlade s legislatívnymi požiadavkami a potrebami organizácie.

d) Vie definovať vhodné bezpečnostné roly a súvisiace zodpovednosti v procesoch a systémoch organizácie .

e) Vie zhodnotiť aktuálny stav riadenia IB v organizácii, vrátane identifikácie najzávažnejších nedostatkov a vhodných nápravných opatrení.

f) Dokáže definovať bezpečnostné politiky a štandardy pre rôzne IKT oblasti v organizácii.

g) Dokáže premietnuť bezpečnostné požiadavky do iných vnútorných predpisov organizácie (ktoré upravujú riadenie projektov, riadenie zmien, riadenie kvality a pod.).

h) Dokáže sa podieľať na vzdelávaní a zvyšovaní bezpečnostného povedomia pracovníkov organizácie.

i) Dokáže komunikovať s externými bezpečnostnými expertmi v jednotlivých oblastiach KIB.

4. Riadenie rizík

a) Pozná základné pojmy riadenia rizík, ich význam a vie ich aplikovať na vlastnú organizáciu: hrozba, zraniteľnosť, opatrenie, analýza rizík, ošetrenie rizika a pod.

b) Dokáže zaviesť a riadiť systematické spravovanie IT rizík v organizácii, ohodnotiť riziká a pozná metódy ošetrenia rizík.

c) Vie vypracovať analýzu rizík IKT systémov a vie posúdiť kvalitu takýchto dokumentov ak sú vypracované externe.

d) Dokáže ohodnotiť riziko a pozná metódy ošetrenia rizík.

e) Vie posúdiť dopad navrhovaných bezpečnostných opatrení (náklady, technické zabezpečenie, organizačné dôsledky, legislatíva).

f) Vie vyhodnotiť účinnosť a efektívnosť prijatých opatrení.

g) Dokáže spolupracovať pri zavádzaní bezpečnostných prostriedkov v organizácii, vrátane ich testovania.

5. Obstarávanie, vývoj a zmeny IKT systémov.

a) Vie v spolupráci s odbornými útvarmi organizácie špecifikovať bezpečnostné požiadavky na predmet obstarávania.

b) Vie posúdiť naplnenie bezpečnostných požiadaviek na predmet obstarávania.

6. Fyzická bezpečnosť.
    a) Pozná hrozby fyzického narušenia IKT systémov a ich infraštruktúry a dokáže ohodnotiť riziká z nich vyplývajúce.
    b) Vie navrhnúť, zdôvodniť a zaistiť/zorganizovať implementáciu opatrení fyzickej ochrany IKT systémov.
    c) Dokáže vypracovať návrhy politík na zaistenie fyzickej ochrany IKT systémov v organizácii.
    d) Dokáže posúdiť účinnosť existujúcich opatrení fyzickej ochrany a dopad technických, organizačných, prípadne iných zmien v organizácii na fyzickú bezpečnosť IKT systémov.
7. Riadenie prístupu.
    a) Rozumie významu identifikácie a autentizácie; pojmom, princípom a metódam I&A; spôsobom riadenia prístupu a vie ich aplikovať v konkrétnom prostredí.
    b) Vie posúdiť akú úroveň a spôsob riadenia prístupu si vyžadujú jednotlivé IKT systémy. Dokáže navrhnúť vhodné riešenia pre riadenie prístupu ako aj posúdiť ich účinnosť a efektívnosť.
    c) Dokáže zaistiť implementáciu opatrení týkajúcich sa riadenia prístupu v jednotlivých IKT systémoch a spolupracovať pri ich implementácii.
8. Bezpečnosť komunikácie
    a) Pozná a rozumie hrozbám voči sieťam a prenášaným údajom.
    b) Pozná a rozumie bezpečnostným mechanizmom a opatreniam na ochranu sietí a údajov.
    c) Vie posúdiť návrhy bezpečnostných opatrení navrhnutých správcom siete alebo špecialistom na sieťovú bezpečnosť, ako aj spolupracovať pri ich návrhu.
    d) Dokáže vhodným spôsobom vyhodnotiť účinnosť prijatých opatrení.
9. Správa bezpečnostných incidentov.
    a) Dokáže zabezpečiť riešenie bezpečnostných incidentov v organizácii.
    b) Dokáže vyvodiť závery z bezpečnostných incidentov, ktoré sa v organizácii vyskytli.
10. Prevádzka IT systémov a kontinuita činnosti
    a) Ovláda základy procesov a postupov prevádzky IKT systémov, vrátane súvisiacich bezpečnostných požiadaviek a dopadov.
    b) Dokáže vypracovať v spolupráci s ďalšími pracovníkmi organizácie havarijné plány a plány kontinuity činnosti.
    c) Vie plánovať stratégiu testovania havarijných plánov a plánov obnovy a podieľa sa na ich testovaní.
11. Audit.

a) Pozná úlohu auditu a dokáže špecifikovať ciele a rozsah auditu (rozsah a detailnosť auditu, použitá metodika a pod.).

b) Dokáže spolupracovať s audítormi pri bezpečnostnom audite a interpretovať výsledky auditu.

Rola: Operátor bezpečnostných technológií

Charakteristika roly. Vykonáva čiastkové procesy (činnosti pri realizácii bezpečnostných opatrení) informačnej bezpečnosti ako napríklad operátor antivírusových nástrojov, nástrojov IDS/IPS, bezpečnostných tokenov, alebo vykonáva správu kryptografických kľúčov atď.

Znalostný štandard

1. Prerekvizity. Ovláda znalosti a má zručnosti požadované znalostným štandardom pre laikov vo všetkých oblastiach. Tento štandard uvádza preto len požiadavky, ktoré sú navyše.

2. Legislatíva a štandardy IB. Má základnú predstavu o legislatíve relevantnej pre informačné systémy a spracúvané údaje vo vlastnej organizácii (zákon o ochrane utajovaných skutočností, zákon o IT vo VS, zákon o elektronických komunikáciách, nariadenia GDPR, eIDAS, direktíva NIS, zákon o kybernetickej bezpečnosti, zákon o kritickej infraštruktúre a pod.) ako aj povinnosti, ktoré pre organizáciu v ktorej pôsobí, z tejto legislatívy vyplývajú.

3. Riadenie IB

   a) Dokáže efektívne vykonávať čiastkový proces kybernetickej a informačnej bezpečnosti.

   b) Dokáže sformulovať návrh bezpečnostnej smernice alebo postupu v oblasti týkajúcej sa bezpečnostného procesu v oblasti svojej pôsobnosti.

   c) Vie zhodnotiť aktuálny stav bezpečnostného procesu v organizácii, vrátane identifikácie najzávažnejších nedostatkov.

   d) Dokáže spolupracovať pri zavádzaní a zmenách bezpečnostného procesu, vrátane jeho testovania.

   e) V prípade potreby je schopný vyškoliť pracovníkov organizácie v postupoch zabezpečujúcich správne a efektívne zvládnutie bezpečnostného procesu.

4. Riadenie rizík

   a) Má všeobecné znalosti o spôsobe riadenia rizík.

   b) Pozná hrozby relevantné pre oblasť KIB v ktorej pracuje, vie zdokumentovať a vyhodnotiť riziká z nich vyplývajúce a navrhnúť opatrenia.

   c) Samostatne, prípadne v spolupráci so správcami IKT systémov vie implementovať bezpečnostné opatrenia v oblasti svojej pôsobnosti.

5. Obstarávanie, vývoj a zmeny IKT systémov.

a) Vie posúdiť dopady zmien na oblasť svojej pôsobnosti.

b) Vie sformulovať bezpečnostné požiadavky na/z oblasti svojej pôsobnosti a posúdiť, či boli v primeranej miere splnené.

6. Fyzická bezpečnosť.

a) Pozná problematiku fyzickej bezpečnosti vo všeobecnosti.

b) Dokáže vyhodnotiť fyzické hrozby a odhadnúť riziká z nich vyplývajúce v oblasti svojej pôsobnosti a navrhnúť primerané opatrenia fyzického a organizačného charakteru.

7. Riadenie prístupu.

a) Rozumie pojmom, princípom a významu identifikácie, autentizácie, metódam a spôsobom riadenia prístupu a vie ich aplikovať v konkrétnom prostredí svojej pôsobnosti.

b) Vie posúdiť akú úroveň a spôsob riadenia prístupu si vyžadujú a aké prostriedky riadenia prístupu umožňujú jednotlivé bezpečnostné technológie, ktorých prevádzku zabezpečuje. Dokáže navrhnúť vhodné riešenia pre riadenie prístupu ako aj posúdiť ich účinnosť a efektívnosť.

c) Dokáže zaistiť implementáciu opatrení týkajúcich sa riadenia prístupu v oblasti svojej pôsobnosti systémoch a spolupracovať pri ich implementácii.

8. Bezpečnosť komunikácie

a) Pozná a rozumie hrozbám voči sieťam a prenášaným údajom.

b) Pozná a rozumie bezpečnostným mechanizmom a opatreniam na ochranu sietí a údajov.

c) Pozná a vie používať prostriedky sieťovej bezpečnosti v súvislosti s bezpečnostnou technológiou, ktorej prevádzku zabezpečuje.

9. Správa bezpečnostných incidentov.

a) Ovláda postupy a činnosti pri výskyte a riešení bezpečnostného incidentu, ktorý je indikovaný ním prevádzkovanou bezpečnostnou technológiou.

b) V prípade potreby vie kvalifikovane pôsobiť v tíme na riešenie bezpečnostného incidentu.

10. Prevádza IT systémov a kontinuita činnosti. Ovláda základy procesov a postupov prevádzky IKT systémov, vrátane súvisiacich bezpečnostných požiadaviek a dopadov

11. Audit. Dokáže spolupracovať s audítormi pri bezpečnostnom audite bezpečnostného procesu a interpretovať výsledky auditu.

Rola: Audítor bezpečnosti IKT systémov

Charakteristika roly. Pracovník posudzujúci zhodu riadenia KIB, vykonávaných procesov KIB a implementovaných opatrení s definovanými legislatívnymi a inými relevantnými požiadavkami, prípadne s najlepšou praxou

Znalostný štandard

1. Prerekvizity. Ovláda znalosti a má zručnosti požadované znalostným štandardom pre laikov vo všetkých oblastiach. Tento štandard uvádza preto len požiadavky, ktoré sú navyše.

2. Legislatíva a štandardy KIB.

   a) pozná a orientuje sa v základných štandardoch IB (rad ISO 2700x, CObIT a pod.)

   b) pozná a orientuje sa v platnej legislatíve upravujúcej požiadavky na IB v organizácii (zákon o ochrane utajovaných skutočností, zákon o IT vo VS, zákon o elektronických komunikáciách, nariadenia GDPR, eIDAS, zákon o kybernetickej bezpečnosti, zákon o kritickej infraštruktúre a pod.)

3. Riadenie KIB. Vie analyzovať vnútorné procesy organizácie a zhodnotiť spôsob a kvalitu riadenia a procesov informačnej bezpečnosti v organizácii, vrátane súvisiacej vnútornej legislatívy (politiky, postupy, štandardy a pod.)

4. Riadenie rizík

   a) vie zdôvodniť a zdokumentovať identifikované riziká

   b) dokáže odporučiť potenciálne vhodné opatrenia na zníženie alebo elimináciu identifikovaných rizík, prípadne spolupracovať so zodpovednými pracovníkmi organizácie na návrhu nápravných opatrení

   c) vie zhodnotiť vhodnosť a spôsob implementácie bezpečnostných prostriedkov a technológií v IKT

5. Obstarávanie, vývoj a zmeny IKT systémov. Vie zhodnotiť spôsob riadenia životného cyklu informačných systémov v organizácii

6. Fyzická bezpečnosť. Má prehľad o fyzickej bezpečnosti (hrozby, riziká, opatrenia), vie posúdiť závažnosť rizík relevantných pre organizáciu a adekvátnosť prijatých opatrení

7. Riadenie prístupu. Pozná význam a metódy I&A, vie posúdiť účinnosť metód I&A používaných v organizácii a ich súlad s politikou riadenia prístupu (klasifikáciou informačných aktív)

8. Bezpečnosť komunikácie. Ovláda základy kryptológie, sieťovej a komunikačnej bezpečnosti v dostatočnej miere na to, aby vedel posúdiť relevantné hrozby voči sieti organizácie a či sú prijaté opatrenia primerané

9. Správa bezpečnostných incidentov.

   a) pozná postupy pri riešení bezpečnostných incidentov vo všeobecnosti,

   b) dokáže vyhodnotiť záznamy o incidentoch v organizácii,

   c) dokáže posúdiť, či sú postupy, ktoré sa používajú pri riešení bezpečnostných incidentov v organizácii primerané, či sú v súlade s legislatívou a bezpečnostnou politikou organizácie a či sú účinné.

10. Prevádzka IT systémov a kontinuita činnosti.

    a) pozná „najlepšie praktiky“ pre prevádzku informačných systémov a bezpečnostných prostriedkov,

    b) vie zhodnotiť adekvátnosť havarijných plánov a plánov kontinuity činností,

    c) vie zhodnotiť kvalitu a adekvátnosť používaných procesov a postupov prevádzky IKT (konfiguračné riadenie, správa incidentov, kapacitné plánovanie, riadenie zmien a pod.).

11. Audit.

    a) ovláda a vie prakticky použiť vhodnú metodiku pre audit informačného systému,

    b) vie navrhnúť stratégiu auditu a vykonať audit informačného systému podľa najlepších praktík, štandardov, legislatívnych a iných požiadaviek na bezpečnosť.

Rola: Bezpečnostný analytik

Charakteristika roly. Špecialista zodpovedný za riešenie zložitých bezpečnostných incidentov, bezpečnostných incidentov veľkého rozsahu alebo incidentov s vážnym dopadom na organizáciu. Má široké vedomosti zo všetkých oblastí informačnej bezpečnosti a hlboké špecializované znalosti z jednej alebo viacerých oblastí KIB.

Znalostný štandard

1. Prerekvizity. Ovláda znalosti a má zručnosti požadované znalostným štandardom pre laikov vo všetkých oblastiach. Tento štandard uvádza preto len požiadavky, ktoré sú navyše.

2. Legislatíva a štandardy KIB.

    a) Pozná legislatívu relevantnú pre oblasť KIB organizácie (zákon o ochrane utajovaných skutočností, zákon o IT vo VS, zákon o elektronických komunikáciách, nariadenia GDPR, eIDAS, zákon o kybernetickej bezpečnosti, zákon o kritickej infraštruktúre a pod.)

    b) pozná medzinárodné štandardy KIB.

3. Riadenie IB

    a) Pozná systém riadenia KIB podľa štandardov ISO/IEC 27000-27002,

    b) pozná systém riadenia KIB v organizácii, v ktorej pôsobí

4. Riadenie rizík

    a) pozná systém riadenia rizík podľa štandardu ISO/IEC 27005 a

    b) pozná systém riadenia rizík v organizácii, kde pôsobí,

    c) dokáže vykonať analýzu rizík,

    d) dokáže posúdiť účinnosť prijatých/navrhovaných opatrení.

5. Obstarávanie, vývoj a zmeny IKT systémov.
    a) pozná životný cyklus IKT systému a dokáže posúdiť, či sa priebehu životného cyklu konkrétneho IKT systému dostatočne uplatňovali bezpečnostné požiadavky, resp. kde organizácia mala bezpečnostné riziká,
    b) dokáže navrhnúť opatrenia na odstránenie zistených bezpečnostných rizík.
6. Fyzická bezpečnosť.
    a) pozná hrozby, zraniteľnosti a opatrenia na zaistenie fyzickej bezpečnosti IKT systémov vo všeobecnosti,
    b) dokáže posúdiť, ktoré z hrozieb sú relevantné pre IKT systémy organizácie a účinnosť prijatých opatrení,
    c) dokáže identifikovať nedostatky vo fyzickej ochrane IKT po bezpečnostnom incidente a navrhnúť opatrenia na ich odstránenie.
7. Riadenie prístupu.
    a) pozná význam I&A, metódy I&A
    b) vie posúdiť vhodnosť použitých metód I&A v organizácii a kvalitu ich implementácie
8. Bezpečnosť komunikácie
    a) má primerané vedomosti o fungovaní počítačových sietí, používaných sieťových protokoloch, hrozbách a bezpečnostných mechanizmoch,
    b) má primerané poznatky o kryptológii a jej aplikáciách (šifrovanie, elektronický podpis a i.),
    c) dokáže posúdiť kvalitu použitých riešení na zabezpečenie siete organizácie, vie nájsť zraniteľnosti a navrhnúť vhodný spôsob ich odstránenia alebo ochrany.
9. Správa bezpečnostných incidentov.
    a) vie identifikovať a analyzovať bezpečnostný incident (charakteristika, pôvodca/príčina, postup/spôsob vzniku, zhodnotenie rozsahu a dopadov a pod.)
    b) pozná metodiku vyšetrovania/riadenia bezpečnostného incidentu a vie ju aplikovať na riešenie bezpečnostných incidentov
    c) dokáže riadiť situáciu v prípade bezpečnostného incidentu
        i. navrhnúť vhodný spôsob reakcie na bezpečnostný incident, minimalizujúc dopady na činnosť organizácie,
        ii. odporučiť spôsob zotavenia sa z incidentu,
        iii. po zvládnutí incidentu navrhnúť preventívne nápravné opatrenia, prípadne dodatočné opatrenia včasnej detekcie incidentu,
        iv. poskytuje informácie o incidente a odporučenia zodpovedným riadiacim pracovníkom organizácie,
        v. v prípade potreby zabezpečiť získanie dôkazov, prípadne potrebnú komunikáciu s externými subjektmi,

vi. formálne zdokumentovať incident.

d) pozná štandardné bezpečnostné technológie a ovláda technológie použité v systémoch, ktorých sa týka bezpečnostný incident

e) pozná právne požiadavky na získavanie a uchovávanie dôkazov pri bezpečnostných incidentoch v IKT a vie ich aplikovať v praxi

f) pozná postupy a ovláda nástroje pre bezpečnú a preukaznú evidenciu získaných informácií

g) pozná techniky a ovláda nástroje forenzného získavania informácií z nosičov dát, operačných systémov a aplikácií (vrátane živých systémov), počítačových sietí a ich komponentov a pod.

h) pozná techniky a ovláda nástroje pre rekonštrukciu priebehu incidentu, vrátane časovej línie (priebehu), spôsobu uskutočnenia a identifikácie pôvodcu incidentu

i) pozná techniky a ovláda nástroje pre analýzu prebiehajúceho bezpečnostného incidentu

10. Prevádzka IT systémov a kontinuita činnosti.

a) pozná bezpečnostné problémy, ktoré je potrebné riešiť počas prevádzky systému,

b) dokáže posúdiť prevádzkové predpisy, používané postupy a v prípade bezpečnostného incidentu vie posúdiť, či došlo k porušeniu predpísaných postupov, alebo či tieto postupy nemajú nedostatky,

c) dokáže vyhodnotiť hrozby, ktoré môžu spôsobiť rozsiahle/závažné narušenie IKT systémov a posúdiť účinnosť opatrení na zabezpečenie kontinuity činnosti.

11. Audit. Pozná metódy auditu a dokáže využívať výsledky auditu pri analýze stavu IKT systémov a príčin bezpečnostných incidentov.

5.3.5 Učitelia a lektori kybernetickej a informačnej bezpečnosti

Učiteľ kybernetickej a informačnej bezpečnosti je odborník v informačnej bezpečnosti, ktorý v tejto oblasti pravidelne vykonáva systematickú vzdelávaciu činnosť. Kvalifikácia učiteľa informačnej bezpečnosti je daná znalosťami, ktoré má poslucháčom odovzdať a schopnosťou podať ich tak, aby im poslucháči porozumeli a osvojili si ich. Učiteľ KIB musí byť schopný naštudovať pre neho neznámu problematiku z nejakej oblasti KIB a spracovať ju do formy primeranej pre jeho poslucháčov. Predpokladáme, že učiteľ KIB aktívne pracuje v KIB a je schopný riešiť odborné problémy. Učitelia KIB by mali mať informatické alebo právne vzdelanie a skúsenosti z praxe.

Učiteľov kybernetickej a informačnej bezpečnosti je málo a ich príprava si vyžiada úpravu študijných programov vysokoškolského štúdia, alebo zavedenie vzdelávacích programov celoživotného vzdelávania. Návrh takýchto programov presahuje rámec tejto knihy.

Ako sme už viackrát spomenuli, na zaistenie potrebnej úrovne KIB bude treba zaviesť v organizáciách vzdelávanie v KIB. Predpokladá sa, že vzdelávať budú manažéri KIB a ďalší odborníci v KIB. Odborníkov v KIB, ktorí (popri inej činnosti) príležitostne vzdelávajú zamestnancov verejnej správy v KIB zaraďujeme do roly lektorov KIB.

Rola: Lektor KIB

Charakteristika roly. Lektor s informatickým vzdelaním, ktorý učí základy KIB dospelých laikov (zamestnancov nejakej organizácie verejnej správy, vrátane manažérov a vedúcich pracovníkov).

Znalostný štandard

1. Špeciálne znalosti
   a) Pozná základné pojmy a rozumie procesom a ich významu vo všetkých oblastiach KIB. Okrem špecifických znalostí KIB navyše:
   b) Dokáže pripraviť a viesť praktické cvičenia zamerané na osvojenie potrebných zručností v oblastiach KIB.
   c) Dokáže demonštrovať preberané oblasti KIB na konkrétnych príkladoch (požiadavky štandardov, legislatívy, spôsoby riadenia KIB, bezpečnostné mechanizmy, postupy a pod.), ilustrovať dobré aj záporné stránky jednotlivých riešení a opatrení, atď.
   d) Dokáže pripraviť a realizovať skúšku na overenie získaných znalostí a zručností.
2. Legislatíva a štandardy KIB.
   a) Pozná legislatívu relevantnú pre oblasť KIB (zákon o ochrane utajovaných skutočností, zákon o IT vo VS, zákon o elektronických komunikáciách, nariadenia GDPR, eIDAS, direktívu NIS, zákon o kybernetickej bezpečnosti, zákon o kritickej infraštruktúre a pod.)
   b) Pozná právne požiadavky na používanie IT systémov organizácie a etické zásady správania sa v digitálnom priestore.
   c) Vie o existencii a náplni štandardov upravujúcich jednotlivé oblasti IB (rad ISO 2700x a pod.).
3. Riadenie KIB
   a) Pozná základné pojmy KIB, ich význam a vie ich aplikovať na konkrétnu organizáciu, napríklad aktívum, integrita, dôvernosť, autentickosť, dostupnosť, súkromie, preukázateľnosť, neodmietnuteľnosť pôvodu a prijatia a pod.
   b) Pozná v primeranej miere špecifické pravidlá vlastnej organizácie—napríklad bezpečnostnú politiku, štandardy, použité bezpečnostné opatrenia, konkrétne postupy pri nahlasovaní a riešení bezpečnostných incidentov, havarijné plány a pod.
   c) Vie identifikovať hlavné informačné aktíva organizácie.
   d) Pozná potrebu a zásady systematického riadenia IB, pozná štruktúru bezpečnostnej politiky a rozumie zásadám, ako zakomponovať IB do informačných procesov organizácie.
   e) Rozumie spôsobom, akým stanoviť priority IB v organizácii (z hľadiska plánovania, prijímaných opatrení, ošetrenia rizík a pod.).
   f) Pozná zásady organizačnej bezpečnosti a stanovenia zodpovednosti pracovníkov organizácie v oblasti IB

4. Riadenie rizík

   a) Pozná základné pojmy riadenia rizík, ich význam a vie ich aplikovať na vlastnú organizáciu: hrozba, zraniteľnosť, bezpečnostný incident, opatrenie, analýza rizík, ošetrenie rizika a pod.

   b) Rozumie ohodnoteniu rizík, spôsobom posúdenia dôsledkov výpadku, straty, zničenia, poškodenia alebo kompromitácie aktív organizácie.

   c) Pozná základné metódy ošetrenia rizík a spôsoby určenia hranice akceptovateľného rizika.

5. Obstarávanie, vývoj a zmeny IKT systémov. Rozumie bezpečnostným požiadavkám súvisiacimi so zmenami, vývojom, obstarávaním a zavádzaním IT systémov.

6. Fyzická bezpečnosť.

   a) Pozná význam fyzickej bezpečnosti a zodpovedajúce zásady a pravidlá.

   b) Dokáže v praxi uplatňovať konkrétne pravidlá fyzickej bezpečnosti organizácie.

7. Riadenie prístupu.

   a) Pozná princípy fungovania rôznych prostriedkov autentizácie (heslá, PIN kódy, tokeny, biometria), vie ich používať, pozná zásady ochrany autentizačných prostriedkov.

   b) Pozná základné techniky sociálneho inžinierstva, vie ich identifikovať a správne na ne reagovať (prezrádzanie hesiel, „phishing“ a pod.).

8. Bezpečnosť komunikácie

   a) Pozná základné požiadavky na ochranu počítačov a iných zariadení v sieti.

   b) Pozná princípy fungovania bezpečnostných riešení v tejto oblasti.

   c) Rozumie rizikám práce na Internete, ich dôsledkom a zásadám bezpečnej práce na Internete: elektronická pošta (spam, prílohy a pod.), šírenie infiltrácií (počítačové vírusy, malware, spyware a pod.), počítačové pirátstvo.

9. Správa bezpečnostných incidentov. Pozná význam správy bezpečnostných incidentov a zásady pri reakcii na bezpečnostné incidenty.

10. Prevádzka IT systémov a kontinuita činnosti.

    a) rozumie princípom fungovania jednotlivých typov a mechanizmov bezpečnostných opatrení v IT systémoch.

    b) Pozná význam, spôsob zálohovania a obnovy údajov v IT systémoch ako aj údajov jednotlivých používateľov.

    c) Rozumie bezpečnostným požiadavkám súvisiacimi s prevádzkou IT systémov a spôsobu, akým ich zohľadniť v konkrétnej organizácii.

    d) . Rozumie požiadavkám na kontinuitu činnosti IT a dokáže stanoviť jej základné rámce v konkrétnej organizácii.

11. Audit. Pozná význam auditu, úlohu audítora, laika a vedúceho pracovníka pri audite.

Literatúra

[1] A. Gordon, ed. *Official (ISC)² Guide to the CISSP CBK*. Angl. 4. vyd. (ISC)² Press. Auerbach Publications, 11. mar. 2015. 1304 strán. ISBN: 9781482262759 (citované na strane 89).

[2] *Information Technology (IT) Security Essential Body of Knowledge (EBK): A Competency and Functional Framework for IT Security Workforce Development*. Washington, D.C.: United States Department of Homeland Security, okt. 2007 (citované na strane 89).

[3] *ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls*. Angl. 2. vyd. ISO a IEC, okt. 2013. 80 strán (citované na stranách: 85, 89).

[4] Bowen P., Hash J. a Wilson M. *Information Security Handbook: A Guide for Managers*. NIST Special publications 800-100. Washington: U.S. Government Printing Office, 2006 (citované na strane 88).

[5] *Information Security Training Requirements: A Role- and Performance-Based Model*. NIST Special publications 800-16r1. Draft. Washington: U.S. Government Printing Office, 2014 (citované na stranách: 88–90).

[6] W. M. a H. J. *Building an Information Technology Security Awareness and Training Program*. NIST Special publications 800-50. Draft. Washington: U.S. Government Printing Office, 2003 (citované na stranách: 88–90).

Kapitola 6

Fyzická bezpečnosť a bezpečnosť prostredia

Daniel Olejár

6.1 Úvod

Keď si prelistujeme katalóg hrozieb, zistíme, že množstvo z nich je priamo zameraných na fyzické aktíva organizácie a že aj narušenie nehmotných aktív organizácie býva často spôsobené nepriamo, poškodením jej fyzických aktív. Zaistenie bezpečnosti informácií a činností, ktoré na základe nich organizácia vykonáva, nie je preto možné bez primeranej úrovne ochrany technických zariadení IKT, podpornej infraštruktúry, priestorov, budov; ustanovenia a dodržiavania pravidiel pre narábanie s IKT a dátovými nosičmi. Túto časť agendy KIB pokrýva fyzická bezpečnosť a bezpečnosť prostredia. Pri výklade problematiky sa budeme pridržiavať normy [3], ktorá zaistenie fyzickej bezpečnosti organizácie delí na dve časti:

- zaistenie oblastí,
- zaistenie zariadení.

6.2 Bezpečné oblasti

Cieľom zaistenia oblasti (alebo vytvorenia bezpečných oblastí[1]) je zabrániť

1. fyzickému poškodeniu IKT a informácií organizácie,
2. neoprávnenému fyzickému prístupu k nim,
3. ich poškodeniu alebo manipulovaniu s nimi.

Informácie sa spracovávajú prostredníctvom IKT, ktoré sú umiestnené v nejakých priestoroch (miestnostiach). Miestnosti sa nachádzajú v budovách a budovy stoja (niekedy) na

[1] v origináli Secure areas

vlastnom pozemku organizácie. Hranica každej z týchto oblastí predstavuje líniu obrany, ktorú treba využiť (a primerane zaistiť).

Vonkajšiu líniu obrany proti neoprávnenému fyzickému prístupu k aktívam organizácie tvorí hranica pozemku (ak má organizácia vlastný pozemok). Túto je možné chrániť múrom, plotom a/alebo elektronickými zabezpečovacími prostriedkami (bezpečnostné kamery, hlásiče pohybu). Vstup na pozemok (a odchod z neho) je možný len cez miesta na to vyhradené. Tie by mali byť vybavené tak, umožňovali kontrolu osôb (dopravných prostriedkov, nákladu) a zabraňovali osobám, ktoré nemajú potrebné oprávnenia na vstup na pozemok, resp. odchod z pozemku organizácie. Je zrejmé, že požiadavka na zabránenie vstupu/odchodu je relatívna, ak sa útočník chce dostať na pozemok (a do priestorov) organizácie, s dostatočným vybavením dokáže prekonať prostriedky fyzickej ochrany. Pre opatrenia fyzickej ochrany platí rovnaká zásada, ako pre ostatné opatrenia kybernetickej a informačnej bezpečnosti: náklady na opatrenia majú byť primerané hodnote aktív, ktoré majú tieto opatrenia chrániť. Cieľom plota nie je zabrániť akokoľvek vybavenému útočníkovi preniknúť na pozemok organizácie, ale odradiť príležitostných narušiteľov a prinútiť cieľavedomého, dobre vybaveného útočníka k činnostiam (napr prekonanie plota), ktoré ho zdržia a umožnia ho odhaliť (detektory pohybu, kamery, poškodenie plota).

Vlastný pozemok si máloktorá organizácia môže dovoliť, nanajvýš niekoľko organizácií, ktoré sídlia v rovnakej budove, zdieľa spoločné parkovisko a vrátnicu. Vonkajšia hranica organizácie sa tak posúva a tvoria ju múry (strechy, podlahy) budovy, v ktorej sídli[2]. Táto hranica sa nazýva *fyzický bezpečnostný perimeter (physical security perimeter)* a je ju potrebné explicitne definovať a primerane chrániť[3].

6.2.1 Fyzický bezpečnostný perimeter

Norma [3] kladie na fyzický bezpečnostný perimeter nasledujúce požiadavky:

a) Bezpečnostné perimetre je potrebné explicitne definovať a zohľadniť pri tom bezpečnostné požiadavky kladené na aktíva, ktoré sú umiestnené vnútri perimetra a ohodnotenie rizík vyplývajúcich z hrozieb voči nim. Perimeter nestačí len vyznačiť, ale je potrebné ho aj zabezpečiť, preto (ako uvedieme nižšie) pri jeho vymedzení treba zohľadniť aj potenciálne slabé miesta a prípadne sa im vyhnúť.

b) Perimetre budov, alebo sídel organizácií v ktorých sú umiestnené IKT tvoria múry, strechy, podlahy, okná a dvere. Tieto musia byť v prvom rade fyzicky dostatočne odolné (t.j. nemali byť postavené z materiálov, ktoré je možné ľahko preraziť a preniknúť do priestorov organizácie). Všetky dvere, okná, vývody klimatizácie, kanalizácie, technologické kanály a iné otvory v múroch, cez ktoré je možné preniknúť do priestorov organizácie by mali byť primerane zabezpečené (dostatočne pevné dvere, bezpečnostné zámky, zamykateľné okná aspoň na prízemí, mreže, senzory a pod.)

c) Zamestnanci, klienti a tretie strany by mali do priestorov organizácie prechádzať výlučne cez recepciu (vrátnicu), kde recepčný (príslušník strážnej služby) overí (a zaznamená) ich

[2] primerane sa vzťahuje na organizácie, ktoré sídlia vo viacerých budovách

[3] ako fyzický bezpečnostný perimeter sa najčastejšie vymedzuje vonkajšia hranica organizácie, ale má zmysel členiť priestory organizácie na časti (zóny) podľa požadovanej úrovne ochrany. Pre tieto časti je možné explicitne definovať vnútorné hranice (perimetre).

totožnosť a účel vstupu do priestorov organizácie. Keďže recepcia by mohla byť úzkym miestom pre veľké organizácie, na riadenie vstupu je možné použiť elektronické systémy, založené na identifikačných tokenoch a elektricky ovládaných zábranách (turnikety).

d) Tam, kde to je vhodné, by mali byť vybudované fyzické bariéry (dvere) na ochranu pred prístupom neoprávnených osôb a negatívnym vplyvom prostredia,

e) Organizácia by mala mať inštalovaný systém

- požiarnej signalizácie. Tento systém by mal monitorovať protipožiarne dvere perimetra a hlásiť poplach v prípade požiaru; protipožiarne dvere a steny miestností by mali mať požadovanú úroveň odolnosti voči požiaru.
- detekcie pohybu, ktorý monitoruje všetky vstupy do priestorov organizácie (dvere) a zvonka prístupné okná, priestory v ktorých nie sú zamestnanci, počítačové miestnosti, prípadne iné miesta, ktoré sú z hľadiska bezpečnosti dôležité.

f) IKT, ktoré spravuje organizácia by mali byť fyzicky oddelené od tých, ktoré spravujú externé organizácie. Ak by totiž systémy organizácie boli (napr.) v jednej miestnosti so systémami, ktoré spravuje externá organizácia, hrozilo by riziko, že pracovníci externej organizácie popri údržbe vlastných systémov získajú prístup aj do systémov organizácie.

6.2.2 Opatrenia na fyzické riadenie prístupu

Aby sa do zabezpečených oblastí nedostali nepovolané osoby, organizácia prijme (aj) opatrenia na fyzické riadenie prístupu. Každý človek, ktorý vstupuje do chránených priestorov organizácie, by sa mal identifikovať a jeho identita overiť u osoby (vrátnika, zamestnanca strážnej služby, pracovníka recepcie) alebo v elektronickom systéme (identifikačná karta, prístupový kód, biometrické charakteristiky). O pohybe osôb v chránených priestoroch by organizácia mala vieť evidenciu (v papierovej alebo elektronickej forme), obsahujúcej minimálne údaje o tom, kedy ktorá osoba vstúpila do chránených priestorov a kedy ich opustila (dátum a čas). Implicitne sa predpokladá, že osoby, ktoré vstupujú do chránených priestorov prešli školením (inštruktážou) o podmienkach (bezpečnostných požiadavkách) pobytu v chránených priestoroch a že v týchto chránených priestoroch a zariadeniach, ktoré sa v nich nachádzajú, sú implementované ďalšie bezpečnostné opatrenia (kamerový systém, logické riadenie prístupu do systémov, vytváranie záznamov auditu o činnosti v systéme a pod.) Do chránených priestorov organizácie by cudzie osoby mali vstupovať len v sprievode vlastného zamestnanca organizácie, ktorý zodpovedá za to, že návštevník dodržiava bezpečnostné požiadavky. Zamestnanci, pracovníci tretích strán aj návštevníci by mali nosiť visačky a výskyt neznámeho človeka bez visačky v (chránených) priestoroch organizácie je považovaný za bezpečnostný incident, ktorý je zamestnanec, ktorý takúto osobu spozoroval, povinný hlásiť príslušnému pracovníkovi organizácie (minimálne strážnej službe).

Vstup do priestorov s vyššou úrovňou ochrany (napr. takých, kde sa spracovávajú citlivé informácie, kde sú umiestnené prvky kritickej infraštruktúry a pod.) by mali mať len oprávnené osoby (len vybraní zamestnanci organizácie a v mimoriadnych prípadoch (napr. servisný zásah) a za dodržiavania bezpečnostných opatrení (schválenie vstupu, identifikácia, autentifikácia, sprevádzanie vlastným zamestnancom organizácie) externí špecialisti) a to až po úspešnej identifikácia a autentifikácii vyššej úrovne (napr. dvojfaktorová autentifikácia, karta a heslo, prípadne autentifikácia na základe biometrických charakteristík osoby).

Záznam o pohybe osôb v chránených priestoroch je dôležitý dokument, ktorý môže poskytnúť cenné informácie pri vyšetrovaní bezpečnostných incidentov, ale spolu s inými informáciami môže byť užitočný aj napr. pri detekcii príprav na útok na organizáciu. Vstup oprávneného zamestnanca do chránených priestorov v čase, keď do nich nezvykne vstupovať, môže znamenať, že niekto zneužil jeho identitu na nekalé účely. Aby bol takýto záznam použiteľný, musí byť riadne vedený a primerane chránený aby nedošlo k jeho odcudzeniu, alebo manipulácii údajov v ňom.

6.2.3 Zabezpečenie kancelárií, miestností a priestorov

Mnohým problémom sa dá predchádzť, ak organizácia má ešte pred začiatkom svojej činnosti v nových priestoroch predstavu o tom, na čo sa budú jej priestory a miestnosti používať a aké bezpečnostné požiadavky a majú spĺňať. Vhodným výberom miestností (napr. nie prízemné, bez veľkých sklenených okien) môže ušetriť náklady na zavedenie dodatočných bezpečnostných opatrení. V prvom rade by kľúčové zariadenia organizácie mali byť umiestnené tak, aby k nim verejnosť nemala prístup, dokonca ani by nemala vedieť, že v danej budove sú umiestnené výpočtové kapacity a kde konkrétne. Zariadenia by nemali byť viditeľné alebo elektronicky monitorovateľné na diaľku, a ak to je potrebné, malo by byť odtienené aj ich elektromagnetické vyžarovanie. Informácie o umiestnení zariadení, kde sa spracováva citlivá informácia by mali byť k dispozícii len oprávneným osobám. To znamená, že informácie, ktoré by mohli nepovolanej osobe ukázať cestu k dôležitým (kritickým) výpočtovým kapacitám organizácie by nemali byť uvádzané vo verejne dostupných zdrojoch, ako sú orientačné tabule alebo telefónne zoznamy organizácie.

6.2.4 Ochrana pred externými a prírodnými vplyvmi

Podľa toho, v akom vonkajšom prostredí organizácia pôsobí, by sa mala pripraviť na to, aby čelila aj nepriaznivým vplyvom spôsobeným prírodnými javmi, poruchami alebo ľuďmi. Ak to je možné, organizácia by nemala umiestniť svoje výpočtové kapacity v lokalite, kde hrozia záplavy, prudké búrky, silné vetry; v našich podmienkach našťastie hurikány, zemetrasenia ani výbuchy sopiek nehrozia. Reálnym nebezpečenstvom, ktorému sa nedá vyhnúť je prepätie, spôsobené úderom blesku, alebo technickou poruchou a požiar. Aspoň kritické systémy organizácie by mali mať prepäťovú ochranu. Organizácia musí dodržiavať požiadavky na protipožiarnu ochranu, okrem splnenia tých základných by mala mať protipožiarny signalizačný systém, a ako sme už uviedli, protipožiarne dvere a voči požiaru dostatočne odolné steny miestností, aby sa požiar z vonkajších priestorov nedostal ku kritickým zariadeniam a informačným zdrojom organizácie. Na hasenie požiaru zasahujúceho IKT zariadenia nie je možné použiť štandardné hasiace zariadenia, pretože IKT zariadenia môžu byť pod prúdom (voda) a nevhodné hasiace médium (prášok, pena) by poškodilo elektroniku. Na hasenie horiacich IKT zariadení sa používajú plynové hasiace systémy, ktorých výber, inštaláciu a údržbu však treba ponechať na profesionálov. Nasadenie takejto techniky si vyžaduje aj uzavretie požiarom ohrozených priestorov. (čo s ľuďmi, ktorí sú v čase vypuknutiu požiaru prítomní v miestnosti?)

Prozaickejšie problémy v činnosti organizácie môže spôsobovať nadmerné znečistenie, hluk, prašnosť prostredia, nedostatočná infraštruktúra (najmä elektrina, voda, telekomunikačné linky, klimatizácia), slabá dopravná obsluha, nedostatok parkovacích miest; na druhej strane aj blízkosť frekventovaných ulíc, dopravných uzlov, letísk, nákupných a zábavných centier, športových štadiónov a podobných zariadení môže byť pre činnosť organizácie rušivá. Aj umiestnenie IKT

zariadení v samotnej budove má vplyv na ich bezpečnosť, rozhodne by sa nemali umiestňovať v priestoroch, ktoré sú ohrozené vodou (poškodená strecha, zaplavená pivnica, prasknuté vodovodné alebo kanalizačné potrubie), v blízkosti skladov s horľavými alebo nebezpečnými chemickými látkami, ale ani v ľahko dostupných a ťažko ochrániteľných priestoroch.

6.2.5 Práca v bezpečných priestoroch

Aby neboli prostriedky na zabezpečenie priestorov vynaložené zbytočne, organizácia potrebuje zaviesť pravidlá a uplatňovať na ich základe vytvorené postupy pri práci v bezpečných priestoroch. V prvom rade by o bezpečných priestoroch a aktivitách, ktoré v nich prebiehajú mali vedieť len tí ľudia, ktorí to potrebujú na výkon svojich pracovných povinností (need-to-know principle). Týmto opatrením sa minimalizuje počet ľudí, ktorí môžu potenciálnemu útočníkovi poskytnúť informácie o možnom cieli a znižuje pravdepodobnosť úniku informácií potrebných na úspešný útok. Navyše, menší počet vybraných ľudí je možné jednoduchšie školiť, pripraviť na potenciálne nebezpečenstvo[4]. Práca v bezpečných priestoroch by mala podliehať kontrole jednak z bezpečnostných dôvodov a jednak kvôli prevencii činností poškodzujúcich záujmy organizácie. Kontrola sa týka tak vlastných zamestnancov, ako aj zamestnancov tretích strán, ktorí pracujú v bezpečných priestoroch a pokrýva všetky činnosti, ktoré títo ľudia v bezpečných priestoroch vykonávajú. Ak sú bezpečné priestory prázdne, mali by byť fyzicky uzavreté a periodicky kontrolované, aby sa do nich nepozorovane nedostali nepovolané osoby, resp. aby nedošlo k poškodeniu aktív, ktoré sú v nich umiestnené. Informácie o bezpečnostných opatreniach, zariadeniach a ich rozmiestnení v bezpečných priestoroch sa dajú využiť na prípravu útoku. Preto bez predchádzajúceho výslovného povolenia nie dovolené nosiť do bezpečných priestorov fotoaparáty, vrátane mobilných telefónov.

6.2.6 Nakladacie rampy a podobné priestory

Okrem oficiálnych vstupov pre zamestnancov a návštevnikov organizácie v budove existujú technické a pomocné vstupy, ktoré potenciálny protivník tiež môže využiť na to, aby sa dostal k IKT systémom organizácie. Ak to je možné, IKT systémy organizácie by mali byť v budove umiestnené tak, že sa k nim nedá dostať z týchto pomocných a technických vstupov. Navyše [3]

a) do nakladacích a vykladacích priestorov zvonka budovy by mali mať prístup len identifikovaní ľudia, ktorí na vstup majú oprávnenie,

b) nakladacie a vykladacie priestory by mali byť navrhnuté tak, aby sa materiál mohol naložiť resp. vyložiť bez toho, aby personál, ktorý ho doručil (prebral na odvezenie) mal prístup do ostatných častí budovy,

c) vonkajšie dvere do nakladacieho/vykladacieho priestoru by mali byť zabezpečené (zavreté, alebo kontrolované zamestnancom organizácie), keď sú otvorené vnútorné dvere z nakladacieho/vykladacieho priestoru do budovy,

d) ak to je pre organizáciu relevantné, materiál, ktorý organizácii doviezli, by mal byť preverený na obsah nebezpečných látok ešte predtým, ako ho prevezú z nakladacieho/vykladacieho priestoru do budovy/priestorov organizácie,

[4] manipulácie sociálneho inžiniera

e) dovezený materiál by mal byť zaevidovaný pri vstupe do sídla organizácie,

f) materiál, ktorý z organizácie odchádza by mal byť fyzicky oddelený od toho, ktorý do organizácie dovážajú,

g) dovezený materiál by mali zamestnanci organizácie skontrolovať, či do neho niekto počas dopravy nejako nezasahoval (nepoškodil ho, nevymenil alebo nejako neupravil). Kontrolu podľa toho, o aký materiál ide, bude robiť pracovník organizácie pri dodaní (celistvosť obalu, identifikácia materiálu podľa dodacieho listu), ale zložitejšie zariadenia bude musieť dodávateľ inštalovať a organizácia skontrolovať, či dodané zariadenia spĺňajú dohodnutú špecifikáciu a formálne prebrať.

6.3 Bezpečnosť zariadení

Cieľom ochrany zariadení je zabrániť ich strate, poškodeniu, krádeži, kompromitácii a narušeniu operácií, ktoré od nich závisia. Pod zariadeniami rozumieme predovšetkým fyzické komponenty IKT, komunikačnú infraštruktúru, ktorú využívajú a podporné technické zariadenia, ktoré sú nevyhnutné pre fungovanie IKT.

6.3.1 Umiestnenie a ochrana zariadení

Mnohým (a nielen bezpečnostným) problémom môže organizácia predísť celkom jednoducho tým, že vhodne umiestni zariadenia a bude sa o ne primerane starať:

a) zariadenia je potrebné umiestniť tak, aby sa minimalizoval zbytočný prístup do pracovných priestorov. To znamená, že (napr.) výpočtové zariadenia by mali byť umiestnené v oddelenej časti budovy, ktorá sa dá uzavrieť a dá sa tak vytvoriť bezpečná zóna. Ak by sa však v tejto oddelenej časti nachádzali kancelárie, pracovne iných zamestnancov, spoločný výťah, sklady alebo toalety, nedalo by sa zabrániť prístupu iných ľudí do tejto časti a riziko neoprávneného prístupu k zariadeniam organizácie by sa zbytočne zvýšilo.

b) zariadenia, na ktorých sa spracovávajú citlivé údaje, by mali byť umiestnené tak, aby sa znížilo riziko toho, že ich bude vidieť nepovolaná osoba. Ide najmä o monitory, na ktorých sa zobrazuje informácia počas toho, ako s ňou pracuje oprávnená osoba. Nepovolanou osobou môže byť aj kolega, ktorý vsúpil do miestnosti a ktorý na oboznámenie sa s citlivou informáciou nemá dôvod ani potrebné oprávnenie; návštevník, údržbár, akákoľvek cudzia osoba, ktorá môže vstúpiť do miestnosti z nejakých legitímnych dôvodov, ale nemá oprávnenie na prístup k citlivej informácii. Technicky je možné čítať citlivé údaje z monitoru aj na diaľku, preto by monitor nemal byť otočený smerom k oknu.[5]

c) rovnako ako zariadenia, na ktorých sa spracovávajú údaje by mali byť pred neoprávneným prístupom chránené aj dátové úložiská a pamäťové médiá, na ktorých sa uchovávajú zálohy údajov a systémov.

d) ochranu aktív (systémy, zariadenia, údaje a pod.), na ktoré sú kladené špeciálne bezpečnostné požiadavky, by organizácia mala riešiť zvlášť a zvážiť, aké opatrenia sa budú

[5] to však ešte nevylučuje možnosť čítania obrazovky monitora pomocou tajne inštalovanej kamery.

vzťahovať len na vybrané aktíva a ktoré budú pokrývať všetky[6] aktíva organizácie. Ak by sa úroveň ochrany napr. nejakého systému mala prispôsobiť potrebám najvyššie klasifikovanej informácie, ktorá sa v ňom spracováva[7], potom stojí za úvahu, či nespracovávať citlivú informáciu na menšom samostatnom systéme.

e) prijaté opatrenia by samozrejme mali vychádzať z analýzy rizík, ktorá by mala pokrývať hrozby ako požiar, únik vody, záplava, výbuch, prach, vibrácie, chemické zamorenie[8], dym, elektrická interferencia, komunikačná interferencia, elektromagnetické vyžarovanie, vandalizmus a krádež.

f) IKT zariadenia obsluhujú ľudia, ktorí majú svoje biologické potreby. Organizácia by mala vydať usmernenia upravujúce jedenie, pitie, fajčenie v blízkosti IKT zariadení.

g) organizácia by mala sledovať (monitorovať) teplotu a vlhkosť v miestnostiach s IKT zariadeniami a zabezpečiť, aby sa tieto veličiny udržali v stanovených medziach. V opačnom prípade môže dôjsť k výpadkom, resp. poškodeniu systémov.

h) budovy, v ktorých sídli organizácia by samozrejme mali byť vybavené bleskozvodmi; navyše, prepäťová ochrana by mala byť na prívodoch elektrického prúdu a prichádzajúcich telekomunikačných káblach.

i) u IKT zariadení, na ktorých sa spracováva klasifikovaná informácia (napr. utajované skutočnosti) treba uvažovať, či by nebolo potrebné zaistiť ochranu aj pre únikom informácií v dôsledku elektromagnetického vyžarovania.

6.3.2 Podporné zariadenia

IKT sú závislé od prostredia, v ktorom pôsobia. Narušenie podpornej infraštruktúry, ktorá udržuje podmienky potrebné pre spoľahlivé fungovanie IKT, môže spôsobiť výpadok, poškodenie, narušenie funkčnosti IKT zariadení, narušenie dostupnosti, dôvernosti a integrity údajov, ktoré sa v nich spracovávajú a činností, ktoré organizácia pomocou IKT vykonáva. O ochrane podpornej infraštruktúry sme už na rozličných miestach hovorili. Teraz ponecháme bokom ochranu budov a sústredíme sa na technickú časť podpornej infraštruktúry, ako sú telekomunikačné linky, vedenia elektrického prúdu, vody, plynu, kanalizácie; ventilácia a klimatizácia.

Organizácia

a) udržiava technické podporné zariadenia v súlade s odporúčaniami výrobcu (a platnou legislatívou a normami; napr. protipožiarna ochrana),

b) pravidelne posudzuje, či podporné zariadenia stačia pokryť meniace sa požiadavky organizácie a či kapacitne stačia uspokojiť potreby IKT a iných zariadení (kapacita klimatizovanej serverovne, pridanie nového servra a pod.),

c) by technické podporné zariadenia mala monitorovať a pravidelne testovať, či správne fungujú,

[6] samozrejme len tie, pre ktoré sú dané opatrenia relevantné

[7] čo je princíp, ktorý sa uplatňuje pri klasifikácii informácií a systémov v štandardoch [1] a [2]

[8] napr. pri poškodení veľkej UPS došlo ku kontaminácii miestnosti, kde boli umiestnené aktívne prvky siete kyselinou z UPS

d) tam kde to je potrebné, mať poplašný systém, umožňujúci včas detegovať poruchu a vyhlásiť poplach,

e) ak to organizácia potrebuje, mať viacero zdrojov (napr. elektrického prúdu, pripojenia na Internet), ktoré vedú do organizácie po rozličných fyzických trasách. Zmysel tohto opatrenia je zrejmý, výpadok jedného zdroja organizácia vyrieši prepnutím sa na nezávislý náhradný zdroj.

Pre prípad mimoriadnych udalostí spojených s výpadkom podporných zariadení by organizácia mala mať núdzové zdroje osvetlenia (kvôli evakuácii ľudí) a náhradný komunikačný systém (kvôli vyhláseniu poplachu a riadenia záchranných prác). Aby sa dala vypnúť elektrina, zastaviť prívod plynu a vody, hlavný vypínač prúdu a centrálne ventily vody a plynu by mali byť primerane chránené ale zároveň dostupné.[9]

6.3.3 Bezpečnosť elektrického vedenia a telekomunikačných káblov

Narušenie elektrického vedenia môže spôsobiť výpadok napájania systémov, klimatizácie alebo inej podpornej infraštruktúry a v konečnom dôsledku spôsobiť ohrozenie IKT systémov organizácie. Prístup ku telekomunikačným káblom a kabeláži počítačovej siete organizácie by umožnil protivníkovi prerušiť pripojenie organizácie k Internetu, umožnil mu odchytávať komunikáciu prebiehajúcu na sieti a prípadne do nej zasahovať. Na elimináciu alebo aspoň zníženie rizík vyplývajúcich z týchto hrozieb musí organizácia

a) chrániť elektrické vedenie napájajúce IKT organizácie, telekomunikačné linky a káble internej počítačovej siete organizácie pred prístupom nepovolaných osôb,

b) oddeliť elektrické vedenie a sieťové káble, aby sa zabránilo interferencii[10]

c) v prípade, ak má zvlášť citlivé alebo kritické systémy prijať opatrenia na

- potlačenie elektromagnetického vyžarovania IKT zariadení,
- kontrolu či k sieťovým káblom neboli pripojené odpočúvacie alebo podobné zariadenia,
- riadenie prístupu k rozvodným skriniam elektrického napätia a k aktívnym sieťovým prvkom.

6.3.4 Údržba zariadení

Organizácia musí zabezpečiť (vlastnými zamestnancami alebo pomocou externých pracovníkov) správnu údržbu zariadení, aby zaistila ich dostupnosť a integritu. Pri údržbe zariadení organizácia musí

[9] Tu je potrebné nájsť nejaký rozumný kompromis—zastavenie prívodu plynu v prípade požiaru je nevyhnutné, aby nedošlo k výbuchu. Ak by však boli centrálne ovládacie prvky plynu, vody a elektriny ľahko dostupné, stali by sa zraniteľnosťou organizácie, pretože protivník by nepotreboval útočiť na chránené IKT systémy, ale stačilo by mu napríklad vyradiť prívod elektriny. Jedno z riešení je uchovanie kľúča od miestnosti/priestoru s rozvodmi v chránenej skrinke (napríklad sklom, ktoré sa dá ľahko rozbiť), ku ktorej sa v prípade potreby môže oprávnená osoba (vedúci, strážna služba) dostať, vyberie z nej kľúč a zasiahne.

[10] v prípade, ak sa na vnútorné rozvody nepoužívajú optické, ale kovové vodiče

a) dodržiavať servisné intervaly a zariadenia udržiavať v súlade s výrobcovými špecifikáciami,

b) zaistiť, aby opravy a údržbu zariadení vykonával len kvalifikovaný a na to oprávnený personál,

c) viesť záznamy o možných a skutočných poruchách a všetkých servisných zásahoch a opravách,

d) pri plánovaných údržbách zariadení prijať potrebné opatrenia ako odstránenie citlivej informácie zo zariadení, overenie totožnosti a oprávnení externého personálu vykonávajúceho údržbu,

e) dodržiavať všetky požiadavky na údržbu zariadení vyplývajúce z poistných zmlúv,

f) pred opätovným uvedením zariadení do prevádzky po údržbe overiť, či zariadenia neboli upravené a či fungujú správne.

Aj v prípade, ak je potrebný servisný zásah externého odborníka v priestoroch organizácie, musí organizácia zabezpečiť, aby mal prístup len k zariadeniu, ktoré si servisný zásah vyžaduje, ale nie k iným systémom organizácie napríklad tak, že externého odborníka sprevádza vlastný zamestnanec organizácie.

6.3.5 Vynášanie aktív

Niekedy je potrebné vyniesť aktíva (zariadenia, softvér, údaje) organizácie mimo jej priestorov (prezentácia, rokovanie, služobná cesta, zapožičanie alebo oprava zariadenia). Organizácia by však mala mať aj v takýchto prípadoch prehľad, kde sa jej aktíva nachádzajú a kto je za ne zodpovedný. Aby sa nestalo, že niekto zo zamestnancov, alebo cudzí človek si odnesie z organizácie (údajne na opravu) počítač, organizácia musí mať pravidlá upravujúce vynášanie aktív z priestorov organizácie. Organizácia by mala

a) jasne stanoviť osoby, ktoré môžu vynesenie aktív z organizácie povoliť,

b) jasne stanoviť, ako dlho môžu byť aktíva mimo organizácie,

c) viesť evidenciu vynesených a vrátených aktív,

d) v podmienkach na vynesenie aktíva stanoviť požiadavku vedenia záznamov obsahujúcich identitu, rolu, zamestnanie každého človeka, ktorý narába s vynesenými aktívami, alebo ich používa. Tento záznam by mal byť odovzdaný organizácii spolu s vrátenými aktívami.

Zaujímavá je posledná požiadavka, ide v podstate o accountability, dosledovateľnosť. Organizácia potrebuje vedieť, kto narábal s aktívom, kým bolo mimo organizácie. Požiadavky na vynášanie aktív z organizácie sa dajú dobre uplatiť na počítače a fyzické zariadenia, ktoré majú svojho vlastníka (ktorý je za ne zodpovedný a rýchle by zistil, keby mu ich niekto bez jeho vedomia vyniesol z organizácie), identifikačné čísla a sú také veľké, že ich nie je možné nepozorovane vyniesť z organizácie. Dodržiavanie vyššie uvedených požiadaviek je možné presadiť pomocou organizačných a administratívnych opatrení a kontrolovať. Ťažšie sa uplatňujú

v prípade nehmotných aktív, ako je programové vybavenie a údaje, pri ktorých bude prinajmenšom problematické skontrolovať, či človek v na SD karte svjho smartfónu nevynáša tajné dokumenty organizácie, databázu klientov, alebo inštalačné súbory zaujímavého softvéru. Tieto aktíva bude potrebné chrániť tak, že sa k nim nepovolaná osoba nedostane a o prístupe oprávnených osôb k nim a narábaní s nimi bude vedený záznam, ktorý používateľ nebude môcť ovplyvniť.

6.3.6 Bezpečnosť zariadení a aktív mimo priestorov organizácie

Organizácia môže výrazne zasahovať do prostredia vo vlastných priestoroch, prijímať a implementovať opatrenia, stanovovať pravidlá a kontrolovať ľudí (vlastných zamestnancov, externistov aj návštevníkov), či ich dodržiavajú. Ale ľudia pracujú aj doma, pristupujú z externého prostredia do systémov organizácie a buď vynášajú mimo priestorov organizácie aj jej fyzické zariadenia, alebo na prácu používajú vlastné zariadenia.[11] Niekedy tiež organizácia zapožičia svoje zariadenia iným organizáciám. Vynášanie zariadení organizácie mimo jej priestorov, práca doma (na prostriedkoch organizácie, alebo vlastných), prístup k zdrojom organizácie z domu by zamestnancovi malo schváliť vedenie organizácie. Externé prostredie, v ktorom človek pracuje, obsahuje množstvo rôznych hrozieb a nie je možné dať všeobecne platný návod na to, ako sa im vyhnúť. Norma [3] je v tomto smere veľmi všeobecná a sústreďuje sa na ochranu fyzických aktív[12]. Prvé dve odporúčania sa týkajú prenosných zariadení, ktoré má zamestnanec so sebou napríklad na služobnej ceste, tretie bezpečnostných rizík práce doma.

a) zamestnanec by nemal nechávať zapožičané zariadenia bez dohľadu na verejných miestach (napríklad notebook v taške na letisku),

b) mal by poznať a dodržiavať inštrukcie výrobcu ohľadne ochrany zariadenia (napr. ochrana pred silným elektromagnetickým poľom),

c) pre prácu v domácom prostredí by mala byť najprv spravená analýza rizík[13] a na jej základe prijaté opatrenia, ktoré bude zamestnanec pri práci doma musieť implementovať, resp. dodržiavať.

d) posledné odporúčanie sa týka evidencie majetku. Organizácia musí viesť evidenciu o pohybe jednotlivých IKT zariadení. Každé zariadenie, ktoré organizácia niekomu požičia, musí byť zaznamenané (kedy, komu, na aký čas, za akým účelom, kedy a v akom stave bolo vrátené), podobne, ako sme už spomínali, sa vedie záznam o zariadeniach, ktoré sa vynášajú z organizácie na opravu.

6.3.7 Bezpečné vyradenie alebo opätovné používanie zariadení

Ak organizácia vyraďuje počítače, alebo iné zariadenia, ktoré obsahujú pamäťové médiá, musí pred ich vyradením overiť, či na pamäťových médiách nie je uložená nejaká citlivá informácia alebo licencované programové vybavenie[14]. Údaje a programy zo zariadenia nestačí vymazať,

[11] takúto situáciu v nebývalom rozsahu zažívame/sme zažili v časoch pandémie Covid 19

[12] prácu z domu rieši v inej časti

[13] dá sa očakávať, že sa podmienky u jednotlivých zamestnancov nebudú líšiť do takej miery, aby bolo u každého potrebné spraviť samostatnú analýzu rizík.

[14] ak aj zariadenie neobsahuje citlivé údaje, ale organizácia napr. daruje vyradený počítač, switch alebo iné zariadenie škole, môže porušiť licenčné podmienky a spôsobiť aj sebe aj obdarovanému zbytočné problémy

pretože existujú ľahko dostupné nástroje, ktoré umožňujú obnoviť vymazané informácie. Postupy na spoľahlivé odstránenie citlivých údajov z pamäťových médií sú podrobne opísané v [4].

Lacnejšie pamäťové médiá obsahujúce citlivú informáciu sa odporúča fyzicky zničiť; ak sa majú médiá opätovne použiť, údaje z nich je potrebné spoľahlivým spôsobom odstrániť [4].

Organizácia je vystavená hrozbe úniku citlivých údajov aj v prípade poškodenia počítača, či iného zariadenia, ktorého opravu je potrebné zveriť externému špecialistovi. V takom prípade stojí za zváženie, či pre organizáciu nie je výhodnejšie zariadenie, resp. jeho pamäťové médiá fyzicky zničiť, ako riskovať únik citlivých údajov. Riziko prezradenia citlivých údajov pri oprave zariadenia je podstatne menšie, ako sú údaje na disku alebo inom pamäťovom médiu šifrované, za predpokladu, že šifrovanie je dostatočne silné a pokrýva celý disk (vrátane swapovacieho priestoru a súborov, ktoré sú v ňom uložené).

6.3.8 Nestrážené zariadenie používateľa

Často sa stáva, že používateľ v priebehu práce na nejakej úlohe opustí svoju pracovnú stanicu a venuje sa na chvíľu nejakej inej činnosti. Ak by nechal spustený počítač (otvorenú session), protivník by v lepšom prípade mohol získať informácie, na ktorých používateľ pracoval, v horšom zneužiť jeho prístupové práva a preniknúť z jeho počítača do systému organizácie, prípadne si otvoriť zadné vrátka do jeho počítača. Aby sa zamedzilo takýmto incidentom, používateľov je potrebné naučiť, aby

a) po ukončení práce uzavreli všetky úlohy, na ktorých pracovali,

b) odhlásili sa z aplikácií, ktoré už prestali používať,

c) nastavili si počítače a mobilné zariadenia tak, že keď ich nepoužívajú, uzamknú sa a od používateľa budú vyžadovať, aby sa znova prihlásil.

Organizácia môže konfigurovať počítače zamestnancov tak, že po nejakej dobe bez zásahu používateľa sa počítač uzamkne a na aktiváciu bude vyžadovať napr. zadanie hesla.

6.3.9 Politika čistého stola a čistej obrazovky

Podobne ako v prípade počítača, alebo mobilného zariadenia, ktoré nechal jeho používateľ na chvíľu bez dohľadu, aj dočasne opustené pracovné miesto môže obsahovať citlivé údaje, ktoré sa v neprítomnosti zamestnanca môžu dostať do nepovolaných rúk[15]. Citlivé informácie v papierovej podobe, alebo na pamäťových médiách by zamestnanec nemal nechávať na stole, ale aj v prípade chvíľkovej neprítomnosti by ich mal uložiť a zamknúť do (podľa úrovne citlivosti) uzamykateľnej zásuvky, skrine, alebo trezoru.

Z citlivých dokumentov by sa nemali vytvárať neautorizované kópie pretože tak sa stráca prehľad o tom, koľko exemplárov dokumentu existuje a dokument by sa mohol dostať do nepovolaných rúk. Dokumenty obsahujúce citlivú informáciu by sa mali tlačiť len na vyhradených

[15] napríklad, ak počas jeho neprítomnosti príde za ním kolega, alebo nejaký návštevník

tlačiarňach, ktoré sú pod kontrolou osoby oprávnenej oboznamovať sa s dokumentom a odstraňovať z tlačiarní hneď po vytlačení, aby sa nedostali do nepovolaných rúk. V prípade, ak došlo pri tlačení k poruche a tlačiareň dokument nevytlačila, je potrebné mať na pamäti, že v tlačiarni ostal súbor obsahujúci dokument a odstrániť tento súbor z tlačiarne.

Literatúra

[1] *FIPS 199 Standards for Security Categorization of Federal Information and Information Systems,* U.S. Department of commerce & NIST, 2003 (citované na strane 119).

[2] *FIPS 200 Minimum Security Requirements for Federal Information and Information Systems.* U.S. Department of commerce & NIST, 2006 (citované na strane 119).

[3] *ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls.* Angl. 2. vyd. ISO a IEC, okt. 2013. 80 strán (citované na stranách: 113, 114, 117, 122).

[4] K. R., S. M., S. S a L. X. *Guidelines for Media Sanitization.* NIST Special publications 800-88. Draft. Washington: U.S. Government Printing Office, 2006 (citované na strane 123).

Kapitola 7

Riadenie prístupu

Ladislav Hudec

7.1 Úvod

Počítačová bezpečnosť v klasickom ponímaní je charakteristika systému, ktorá vo vzťahu k zdrojom systému vyžaduje zaistenie ich dôvernosti, integrity a dostupnosti. Počítačové systémy manipulujú s údajmi a sprostredkujú prístup k zdieľaným zdrojom. Musia zabezpečiť kontrolu prístupu k údajom a zdrojom, predovšetkým z dôvodov dôvernosti.

Na riadenie prístupu sa môžeme dívať ako na centrálny prvok počítačovej bezpečnosti. Základným cieľom počítačovej bezpečnosti je zabrániť neoprávneným používateľom získať prístup k zdrojom, zabrániť oprávneným používateľom pristúpiť k zdrojom neoprávneným spôsobom a umožniť oprávneným používateľom pristúpiť k zdrojom oprávneným spôsobom.

Mechanizmus riadenia prístupu robí sprostredkovateľa medzi používateľom (alebo procesom vykonávaným v mene používateľa) a systémovými zdrojmi, ako sú aplikácie, operačné systémy, bezpečnostné brány, smerovače, súbory a databázy. Systém musí najprv autentizovať entitu žiadajúcu prístup. Autentizačná funkcia typicky určuje, či je používateľovi dovolené vôbec pristupovať k systému. Potom funkcia riadenia prístupu určuje, či je povolený tomuto používateľovi špecifický požadovaný prístup.

Tématicky možno túto kapitolu rozdeliť na tri časti. V prvej časti sú formulované vysokoúrovňové bezpečnostné požiadavky na počítačové systémy[1]. Bezpečnostné požiadavky sú rozdelené na základné a odvodené. K jednotlivým bezpečnostným požiadavkám je uvedený aj stručný výklad. Druhá časť obsahuje základný koncept riadenia prístupu v počítačovom systéme. Sú podrobnejšie opísané autentizácia a autorizácia používateľa, prístupové operácie k zdrojom počítčového systému a jednotlivé komponenty štruktúry riadenia prístupu. V tretej časti sú uvedené formálne modely počítačovej bezpečnosti z pohľadu riadenia prístupu. Ide konkrétne o model Bell-LaPadula, model riadenia prístupu založený na rolách RBAC, model Čínskeho múru a model riadenia prístupu založený na atribútoch ABAC.

[1]Pojem počítačový systém a informačný systém budeme považovať za ekvivalenty.

7.2 Bezpečnostné požiadavky na riadenie prístupu

Bežné organizácie nespracúvajú informácie, ktoré by podliehali zákonu číslo 215/2004 Z. z. o ochrane utajovaných skutočností (klasifikované informácie). Napriek tomu musia organizácie nimi spracúvané informácie chrániť zo zákona (napríklad osobné údaje) alebo majú záujem ich chrániť (napríklad obchodné informácie). Chrániť informácie organizácie okrem iného znamená implementovať riadenie prístupu k informáciám organizácie podľa daných pravidiel, ktoré sú určené bezpečnostnou politikou organizácie. Uvedený druh informácií môžeme nazvať riadené neklasifikované informácie. V dokumente [8] sú formulované bezpečnostné požiadavky na riadenie prístupu k takýmto informáciam. Bezpečnostné požiadavky možno rozdeliť na základné bezpečnostné požiadavky a na odvodené bezpečnostné požiadavky. Tieto bezpečnostné požiadavky a ich výklad sú uvedené nižšie.

7.2.1 Základné bezpečnostné požiadavky

1. Obmedziť prístup do systému na oprávnených používateľov, procesy konajúce v mene oprávnených používateľov a zariadení (vrátane ďalších systémov).

   Táto požiadavka sa zameriava na správu účtov pre systémy a aplikácie a vyjadruje základnú funkciu riadenia prístupu v informačnom systéme organizácie. Politiky riadenia prístupu riadia prístup medzi aktívnymi entitami alebo subjektmi (t.j. používateľmi alebo procesmi konajúcimi v mene používateľov) a pasívnymi entitami alebo objektmi (napr. zariadeniami, súbormi, záznamami a doménami) v systémoch. Na zabezpečenie zvýšenej informačnej bezpečnosti je možné na úrovni aplikácií a služieb použiť mechanizmy na presadzovanie prístupu. Medzi ďalšie systémy patria systémy interné a externé vo vťahu ku organizácii.

2. Obmedziť prístup do systému na typy transakcií a funkcií, ktoré je povolené oprávneným používateľom vykonávať.

   Táto požiadavka bližšie špecifikuje typy prístupov pre oprávnených používateľov. Organizácie v politike riadenia prístupu môžu stanoviť prístupové práva alebo iné atribúty podľa účtu, typu účtu alebo ich kombinácie. Medzi štandardné typy účtov informačného systému patria bežný používateľ, správca aplikácie, správca operačného systému, bezpečnostný správca prípadne ďalšie podľa charakteru informačného systému. Medzi ďalšie atribúty potrebné na autorizáciu prístupu patria obmedzenia denného času, dňa v týždni a miesta pripojenia k informačnému systému. Pri definovaní ďalších atribútov účtu organizácie zohľadňujú systémové požiadavky (napr. plánovaná údržba na aktualizáciu systému) a požiadavky na úlohy organizácie alebo obchodné požiadavky (napr. rozdiely v časových pásmach, požiadavky zákazníkov, vzdialený prístup na podporu požiadaviek pri cestách).

7.2.2 Odvodené bezpečnostné požiadavky

1. Riadiť tok informácií v súlade so schválenými autorizáciami.

   Táto požiadavka rieši bezpečný tok informácií v systémoch organizácie. Riadenie toku informácií reguluje, kam sa informácie môžu prenášať v rámci systému a medzi systémami v závislosti od toho, kto má prístup k informáciám. Medzi obmedzenia riadenia

toku patrí: zabránenie prenosu v otvorenom tvare na internet takých informácií, ktoré sú kontrolované na export; blokovanie premávky z vonku, ktorá vyhlasuje, že je z vnútra organizácie; obmedzenie žiadostí prístupu na internet, ktoré nie sú z interného webového proxy servera; a obmedzenie prenosu informácií medzi organizáciami na základe dátových štruktúr a obsahu. Organizácie bežne používajú politiky riadenia toku informácií a mechanizmy presadzovania riadenia toku informácií medzi určenými zdrojmi a cieľmi (napr. sieťami, jednotlivcami a zariadeniami) v rámci systémov a medzi vzájomne prepojenými systémami. Riadenie toku je založené na vlastnostiach informácie alebo informačnej cesty. Vynútenie nastáva v zariadeniach na ochranu hraníc (napr. brány, smerovače, šifrované tunely, bezpečnostné brány), ktoré používajú sady pravidiel alebo zavádzajú konfiguračné nastavenia, ktoré obmedzujú systémové služby, poskytujú schopnosť filtrovania paketov na základe informácií z hlavičiek alebo filtrujú správy na základe obsahu správy (napr. implementáciou hľadania kľúčových slov alebo použitím charakteristík dokumentu). Organizácie tiež berú do úvahy dôveryhodnosť mechanizmov filtrovania a kontroly (t.j. hardvér, firmvér a softvérové komponenty), ktoré sú rozhodujúce na presadzovanie toku informácií. Prenos informácií medzi systémami predstavujúcimi rôzne bezpečnostné domény s rôznymi bezpečnostnými politikami predstavuje riziko, že takéto prenosy porušujú doménové bezpečnostné politíky. V takýchto situáciách vlastníci alebo správcovia informácií poskytujú poradenstvo pre určené miesta presadzovania politiky medzi vzájomne prepojenými systémami. Keď sa to vyžaduje na presadzovanie konkrétnych bezpečnostných politík, organizácie zvážia prikázanie konkrétnych architektonických riešení. Presadzovanie politiky toku môže obsahovať: zákaz prenosu informácií medzi vzájomne prepojenými systémami; používanie hardvérových mechanizmov na vynucovanie jednosmerných tokov informácií; a implementácia dôveryhodných mechanizmov zmeny klasifikácie na zmenu priradenia bezpečnostných atribútov a bezpečnostných návestí.

2. Oddeliť povinnosti jednotlivcov na zníženie riziko škodlivej aktivity bez kolúzie.

   Táto požiadavka rieši potenciál zneužitia oprávnených privilégií (privilégiá sú vlastne prístupové práva pre privilegovaných používateľov na prístup k funkciám spravovania systému) jedného používateľa prostredníctvom oddelenia povinností (rozdelenie privilégií) na viacerých používateľov a pomáha znižovať riziko škodlivej aktivity bez kolúzie. Oddelenie povinností zahrňuje rozdelenie funkcií úloh a funkcií podpory systému medzi rôznych jednotlivcov alebo rolí; vykonávanie funkcií podpory systému a aplikácií s rôznymi jednotlivcami (napr. správa konfigurácie, zabezpečenie kvality a testovanie, správa systému, správa aplikácie, programovanie a bezpečnosť siete); a zabezpečenie toho, aby bezpečnostný personál spravujúci funkcie riadenia prístupu nespravoval tiež aj auditné funkcie.

3. Uplatňovať zásadu najmenších privilégií vrátane špecifických bezpečnostných funkcií a privilegovaných účtov.

   Táto požiadavka rieši obmedzenie rozsahu prístupových práv (privilégií) používateľa na minimálny rozsah z pohľadu potreby plnenia úloh používateľa. Organizácie využívajú zásadu najmenších privilégií na špecifické povinnosti a autorizovaný prístup pre používateľov a procesy. Zásada najmenších privilégií sa uplatňuje s cieľom autorizovať privilégiá nie vyššie ako je potrebné na splnenie požadovaných úloh organizácie alebo obchodných funkcií. Organizácie môžu zvážiť vytvorenie ďalších procesov, rolí a systémových účtov, aby dosiahli čo najmenšie privilégiá. Organizácie tiež uplatňujú najmenšie privilégiá pre

vývoj, implementáciu a prevádzku svojich systémov. Medzi bezpečnostné funkcie patrí zriadenie systémových účtov, nastavenie udalostí, ktoré sa majú logovať, nastavenie parametrov detekcie prienikov a konfigurácia autorizácií prístupu (t. j. povolenia, privilégiá).

Pre rôzne typy komerčne dostupných operačných systémov sa privilegované účty (účty s privilégiami) vrátane superužívateľských účtov zvyčajne opisujú ako správca systému. Obmedzenie privilegovaných účtov na konkrétny personál alebo roly znemožňuje bežným používateľom prístup k privilegovaným informáciám alebo funkciám.

4. Pri prístupe k funkciám netýkajúcich sa bezpečnosti používať neprivilegované účty alebo roly.

   Táto požiadavka obmedzuje vystavenie systému rizika pri jeho prevádzke v rámci privilegovaných účtov alebo rolí. Uvažovanie rolí sa týka situácií, keď organizácie implementujú politiky riadenia prístupu na základe rolí a kde zmena role zabezpečuje rovnaký stupeň istoty pri zmene autorizácií prístupu používateľa a všetkých procesov konajúcich v mene používateľa takisto ako by bola zabezpečená zmenou medzi privilegovaným a neprivilegovaným účtom.

5. Zabrániť neprivilegovaným používateľom vykonávať privilegované funkcie a zaznamenávať vykonávanie takýchto funkcií do auditných logov.

   Táto požiadavka sa zaoberá potrebou ochrany prístupu k privilegovaným funkciám. Medzi privilegované funkcie patrí zriaďovanie systémových účtov, vykonávanie kontrol integrity systému, vykonávanie operácií záplat alebo správa činností administrácie kryptografických kľúčov. Neprivilegovaní používatelia nemajú takéto oprávnenia. Príklady obchádzania mechanizmov detekcie a prevencie prienikov alebo mechanizmov ochrany pred škodlivým kódom sú príklady privilegovaných funkcií, ktoré vyžadujú ochranu pred neprivilegovanými používateľmi.

   Zneužitie privilegovaných funkcií úmyselne alebo neúmyselne autorizovanými používateľmi alebo neautorizovanými externými subjektmi, ktoré kompromitovali systémové účty, je vážnym a pretrvávajúcim problémom a môže mať výrazný nepriaznivý vplyv na organizácie. Logovanie používania privilegovaných funkcií je jedným zo spôsobov detekcie takéhoto zneužitia a je pomocou pri zmiernení rizika hrozieb od interných používateľov a pokročilej pretrvávajúcej hrozby.

6. Obmedziť neúspešné pokusy o prihlásenie.

   Táto požiadavka platí bez ohľadu na to, či ide o lokálne alebo vzdialené pripojenia používateľa k systému. Aby nedošlo pri neúspešnom pokuse o prihlásenie k odmietnutiu služby sú automatické blokovania účtu iniciované systémami vo väčšine prípadov dočasné a blokovania sa automaticky uvoľnia po vopred určenej dobe stanovenej organizáciou. Organizácia môže používať rôzne doby pre uvoľnenie blokovania pre rôzne komponenty systému na základe spôsobilostí príslušných komponentov. Reakcie na neúspešné pokusy o prihlásenie sa môžu implementovať na úrovni operačného systému a tiež na úrovni aplikácie.

7. Poskytovať oznámenia o ochrane súkromia a bezpečnosti v súlade s platnými pravidlami.

   Táto požiadavka sa týky oznámenia o oprávnenom používaní systému. Oznámenia sa môžu implementovať pomocou správ alebo výstražných bannerov zobrazených predtým,

ako sa jednotlivci prihlásia do systémov organizácie. Oznámenia o používaní systému sa používajú iba na prístup prostredníctvom používateľských prihlasovacích rozhraní a nevyžadujú sa, ak takéto rozhrania neexistujú. Na základe posúdenia rizika organizácie zvážia, či po počiatočnom prihlásení do siete je potrebné oznámenie opakovať pri prístupe do ďalšieho systému k aplikáciám alebo k iným systémovým zdrojom.

8. Na zabránenie prístupu k údajom a ich prezeraniu po určitej dobe nečinnosti používať uzamknutie relácií so skrytím obsahu obrazovky.

   Táto požiadavka sa týka ochrany údajov na obrazovke neobsluhovaného terminálu. Uzamknutie relácie je dočasná akcia vykonaná v prípade, keď používatelia prestanú pracovať a odídu z bezprostrednej blízkosti systému, ale nechcú sa odhlásiť kvôli dočasnej povahe neprítomnosti. Uzamknutie relácií sa implementujú tam, kde je možné zistiť aktivity relácie, zvyčajne na úrovni operačného systému (ale môžu byť aj na úrovni aplikácií). Uzamknutie relácií nie sú prijateľnou náhradou za odhlásenie sa zo systému. Odomknutie relácie vykoná používateľ napríklad zadaním hesla alebo iným spôsobom autentizácie.

9. Automaticky ukončiť reláciu používateľa po definovanej podmienke.

   Táto požiadavka sa týka ukončenia logických relácií iniciovaných používateľom na rozdiel od ukončenia sieťových pripojení, ktoré sú spojené s komunikačnými reláciami (t. j. odpojenie od siete). Logická relácia (pre lokálny, sieťový a vzdialený prístup) sa iniciuje vždy, keď používateľ (alebo proces konajúci v mene používateľa) pristúpi k systému organizácie. Takéto používateľské relácie môžu byť ukončené (a tým ukončený prístup používateľa do systému) bez ukončenia sieťových relácií. Ukončenie relácie ukončí všetky procesy spojené s logickou reláciou používateľa s výnimkou procesov, ktoré sú špecificky vytvorené používateľom (t. j. vlastníkom relácie), aby pokračovali aj po ukončení relácie. Podmienky alebo spúšťacie udalosti, ktoré si vyžadujú automatické ukončenie relácie, môžu predstavovať organizáciou definované doby nečinnosti používateľa, cielené reakcie na určité typy incidentov a časové obmedzenia používania systému.

10. Monitorovať a riadiť relácie vzdialeného prístupu.

    Táto požiadavka sa týka ochrany relácie pri vzdialenom prístupe. Vzdialený prístup je taký prístup k systémom organizácie, v ktorom sa používatelia pripájajú k systémom prostredníctvom externých sietí (napr. Internetu). Organizácie na zvýšenie dôvernosti pri vzdialených pripojeniach často používajú šifrované virtuálne privátne siete (VPN). Použitie šifrovaných sietí VPN nevytvára lokálny prístup; použitie sietí VPN, ak sú adekvátne zabezpečené primeraným opatrením (napr. použitím šifrovacích techník na ochranu dôvernosti údajov), však môže organizácii poskytnúť dostatočnú záruku, že môže efektívne zaobchádzať s takýmito pripojeniami ako s lokálnymi sieťami.

    Automatické monitorovanie a riadenie relácií vzdialeného prístupu umožňuje organizáciám detekovať kybernetické útoky a napomáhať pri zabezpečovaní trvalého súladu s politikami vzdialeného prístupu prostredníctvom auditu aktivít pripojenia vzdialených používateľov.

11. Využiť kryptografické mechanizmy na ochranu dôvernosti relácií vzdialeného prístupu.

    Táto podmienka požaduje ochranu dôvernosti prenášaných údajov pri vzdialenom prístupe prostredníctvom kryptografických mechanizmov, ktoré sú definované v štandardoch.

12. Smerovať vzdialený prístup cez body so spravovaným riadením prístupu.

    Táto požiadavka sa týka bodov prístupu pre vzdialené pripojenie zariadení k informačnému systému organizácie. Na zvýšenie explicitnej kontroly organizácie nad vzdialenými pripojeniami sa požaduje smerovanie vzdialeného prístupu prostredníctvom bodov so spravovaným riadením prístupu. Toto opatrenie znižuje náchylnosť vzdialených pripojení na neoprávnený prístup k systémom organizácie.

13. Autorizovať vzdialené vykonávanie privilegovaných príkazov a vzdialený prístup k informáciám súvisiacich s bezpečnosťou.

    Táto požiadavka sa zaoberá bezpečnosťou pri vzdialenom zadávaní príkazov a vzdialenom prístupom k informáciám. Privilegovaný príkaz je príkaz iniciovaný používateľom (interaktívne alebo prostredníctvom procesu fungujúceho v mene používateľa) vykonaný v systéme zahrňujúci riadenie, monitorovanie alebo administráciu systému vrátane bezpečnostných funkcií a súvisiacich bezpečnostných informácií. Informácia súvisiaca s bezpečnosťou je akékoľvek informácia v systéme, ktorá môže potenciálne ovplyvniť fungovanie bezpečnostných funkcií alebo poskytovanie bezpečnostných služieb spôsobom, ktorý by mohol viesť k zlyhaniu pri presadzovaní bezpečnostnej politiky systému alebo k spôsobeniu nedostupnosti kódu a údajov. Privilegované príkazy dávajú jednotlivcom možnosť vykonávať citlivé, bezpečnostne kritické alebo s bezpečnstne relevantné funkcie systému. Riadenie tohto prístupu zo vzdialených miest pomáha zaistiť, aby neoprávnené osoby neboli schopné vykonávať takéto príkazy, v opačnom prípade by to mohlo spôsobiť vážne alebo katastrofické škody systémom organizácie. Treba mať na zreteli, že schopnosť ovplyvniť integritu systému sa považuje za bezpečnostne relevantnú, pretože by mohla umožniť spôsob obchádzania bezpečnostných funkcií, hoci to priamo neovplyvňuje samotnú funkciu.

14. Autorizovať bezdrôtový prístup pred povolením takéhoto pripojenia.

    Táto požiadavka stanovuje autorizáciu prístupu bezdrôtového zariadenia pred povolením pripojenia do informačného systému organizácie. Podmienky na autorizáciu pripojenia bezdrôtového zariadenia môžu obsahovať obmedzenia používania a požiadavky na konfiguráciu / pripojenie bezdrôtového prístupu k systému. Takéto obmedzenia a požiadavky znižujú náchylnosť na neoprávnený prístup do systému prostredníctvom bezdrôtových zariadení. Bezdrôtové siete používajú autentizačné protokoly, ktoré poskytujú ochranu prístupových údajov a vzájomnú autentizáciu.

15. Chrániť bezdrôtový prístup pomocou autentizácie a šifrovania.

    Táto požiadavka sa týka ochrany bezdrôtového prístupu do informačného systému organizácie. Na ochranu prístupu do systému organizácie používajú autentizáciu jednotlivcov a zariadení. Táto požiadavka vyžaduje osobitná pozornosť v súvislosti so širokou škálou zariadení internetu vecí (IoT) a ich možným bezdrôtovým prístupom do systému organizácie.

16. Riadiť pripojenie mobilných zariadení.

    Táto požiadavka rieši bezpečnosť pripojenia mobilných zariadení. Mobilné zariadenie je výpočtové zariadenie, ktoré má malý rozmer, takže je používateľom ľahko prenosné; je navrhnuté tak, aby fungovalo bez drôtového spojenia (štandardne je vybavené na bezdrôtové spojenie); obsahuje nevymeniteľné alebo vymeniteľné úložisko údajov; a obsahuje

samostatný zdroj energie. Mobilné zariadenia môžu tiež obsahovať funkcie hlasovej komunikácie, zabudované senzory, ktoré umožňujú zariadeniu zaznamenávať informácie, alebo vstavané funkcie na synchronizáciu lokálnych údajov so vzdialenými úložiskami. Medzi príklady mobilných zariadení patria smart telefóny, elektronické čítačky a tablety.

Z dôvodu veľkého množstva mobilných zariadení s rôznymi technickými charakteristikami a možnosťami sa môžu obmedzenia organizácie pre rôzne typy zariadení líšiť. Medzi obmedzenia použitia a implementačné pokyny pre mobilné zariadenia patria: identifikácia a autentizácia zariadenia; správa konfigurácie; implementácia povinného bezpečnostného softvéru (napr. detekcia škodlivého kódu, bezpečnostná brána); skenovanie zariadení na škodlivý kód; aktualizácia softvéru na ochranu pred vírusmi; vyhľadávanie kritických aktualizácií softvéru a záplat; vykonávanie kontrol integrity primárneho operačného systému (a prípadne iného rezidentného softvéru); a vypnutie nepotrebného hardvéru (napr. bezdrôtový, infračervený prijímač).

17. Šifrovať informácie na mobilných zariadeniach a mobilných počítačových platformách.

    Táto požiadavka sa týka ochrany údajov uložených na nosičoch, ktoré sa môžu vynášať z priestorov organizácie. Organizácie môžu na zabezpečenie dôvernosti údajov na mobilných zariadeniach a počítačových platformách používať šifrovanie celého údajového úložiska alebo šifrovanie po častiach v kontajneroch.

18. Overiť a riadiť / obmedziť pripojenia a použitie externých systémov.

    Táto požiadavka sa týka bezpečnosti pripojenia a použitia externých systémov. Externé systémy sú systémy alebo súčasti systémov, na ktoré organizácie zvyčajne nemajú priamy dohľad a právomoc nad uplatňovaním bezpečnostných požiadaviek a opatrení alebo na stanovenie účinnosti zavedených opatrení týchto systémov. Externé systémy predstavujú systémy, komponenty alebo zariadenia v osobnom vlastníctve a počítačové a komunikačné zariadenia v súkromnom vlastníctve spravidla umiestnené mimo priestorov organizácie. Táto požiadavka sa tiež týka použitia externých systémov na spracovanie, ukladanie alebo prenos informácií vrátane prístupu ku cloudovým službám zo systémov organizácie.

    Organizácie stanovujú podmienky používania externých systémov v súlade s bezpečnostnými politikami a procedúrami organizácie. Podmienky sa týkajú minimálne typov aplikácií organizácie, ku ktorým môžu pristupovať externé systémy. Ak nie je možné stanoviť podmienky s vlastníkmi externých systémov, organizácie môžu uložiť obmedzenia svojmu personálu na používanie a prístup externých systémov.

    Táto požiadavka rešpektuje, že existujú prípady, keď jednotlivci používajúci externé systémy (napr. dodávatelia, spolupracujúci partneri) musia mať prístup k systémom organizácie. V týchto situáciách organizácie potrebujú istotu, že externé systémy obsahujú potrebné opatrenia, aby nedošlo k ohrozeniu alebo poškodeniu systémov organizácie. Overenie, či sa požadované opatrenia účinne implementovali sa dá dosiahnuť pomocou nezávislých hodnotení, osvedčení alebo inými prostriedkami v závislosti od úrovne istoty alebo dôveryhodnosti požadovanej organizáciami.

19. Obmedziť používanie prenosných pamäťových zariadení na externých systémoch.

    Táto požiadavka sa týka obmedzenia používania prenosných pamäťových zariadení na externých systémoch. Obmedzenia môžu obsahovať úplný zákaz používania takýchto zariadení alebo obmedzenia týkajúce sa spôsobu použitia týchto zariadení a za akých pod-

mienok sa tieto zariadenia môžu používať. Označenie „externý“ sa zvyčajne vzťahuje na priamy dohľad a právomoci organizácie nad informačným systémom. Nemusí to však byť vždy tak. Organizácia môže prevádzkovať informačné systémy spracúvajúce informácie s rôznym stupňom ochrany, napríklad chránené vyžadujúce ochranu riadením prístupu a nechránené informácie nevyžadujúce ochranu. Medzi systémami spracúvajúce chránené informácie sú pravdepodobne obmedzenia prístupu pre chránené informácie, ktoré sa uplatňujú medzi týmito systémami. Z hľadiska daného systému (spracúvajúceho chránené informácie) sa preto iné systémy (nespracúvajúce chránené informácie) v organizácii môžu považovať za „externé“.

20. Riadenie informácií poslaných do alebo spracovávaných na verejne prístupných systémoch.

    Táto požiadavka sa týka možného zverejňovania informácií organizáciou. V súlade s platnými zákonmi, bezpečnostnými politikami organizácie a ich smernicami verejnosť nemá oprávnený prístup k neverejným informáciám (napr. k informáciám chráneným podľa zákona o ochrane osobných údajov, k informáciám chráneným autorskými právami a k vlastníckym informáciám). Táto požiadavka sa týka systémov, ktoré sú riadené organizáciou a sú prístupné verejnosti, zvyčajne bez identifikácie alebo autentizácie. V organizácii sú určené osoby oprávnené posielať chránené informácie (v prípade, že sú uvoľnené pre verejnosť) do verejne prístupných systémov. Obsah informácií sa kontroluje pred poslaním do verejne prístupných systémov s cieľom zabezpečiť, že neobsahujú neverejné informácie.

7.3 Základný koncept riadenia prístupu

7.3.1 Autentizácia a autorizácia

Aby sme mohli diskutovať o riadení prístupu, je potrebné podrobnejšie sa pozrieť na používanú terminológiu v tejto oblasti. Keďže sa hovorí o „riadení prístupu“, musia existovať aspoň tri entity, ktoré sa zúčastňujú tohto procesu. Musí existovať aktívna entita, ktorá pristupuje (subjekt), pasívna entita, ktorá je pristupovaná (objekt) a entita, ktorá riadi prístup (referenčný monitor). Výklad vyššie uvedených pojmov upresníme podľa slovníka kľúčových termínov informačnej bezpečnosti [7]:

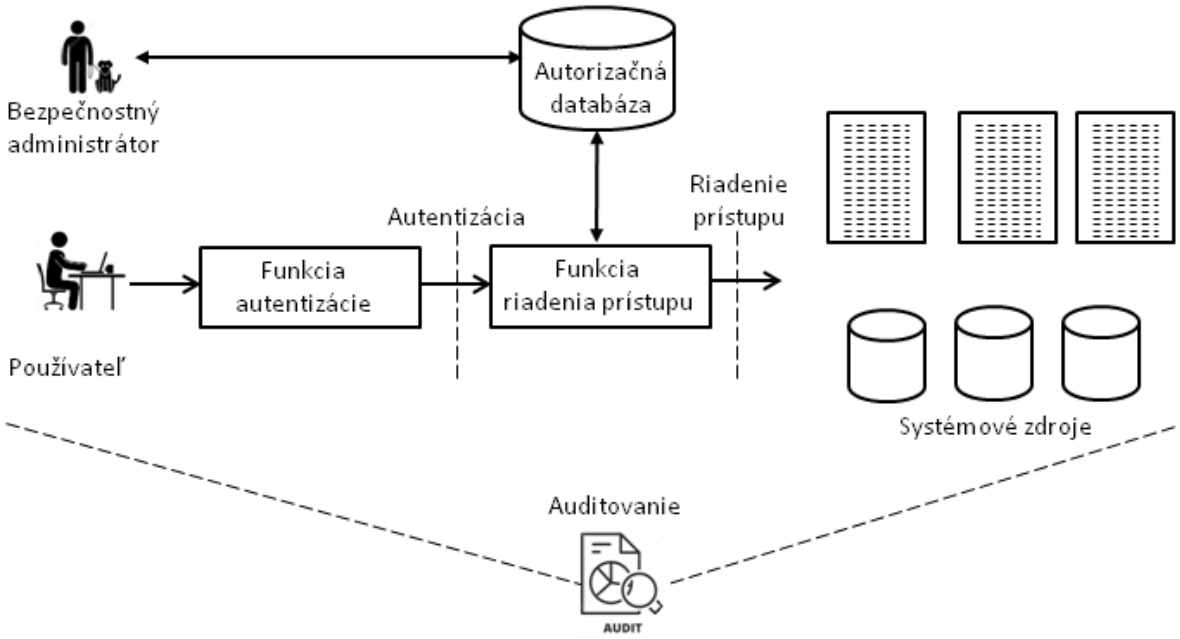
- **Subjekt** je aktívna entita, zvyčajne vo forme osoby, procesu alebo zariadenia, ktorá spôsobuje tok informácií medzi objektmi alebo mení stav systému.

- **Objekt** je pasívna entita súvisiaca s informačným systémom (napr. zariadenia, súbory, záznamy, tabuľky, procesy, programy, domény) obsahujúca alebo prijímajúca informácie. Prístup subjektu k objektu znamená prístup subjektu k informáciám, ktoré objekt obsahuje.

- **Riadenie prístupu** je proces udeľovania alebo zamietania konkrétnych žiadostí o: 1) získanie a používanie informácií a súvisiacich služieb spracovania informácií; a 2) vstup

do konkrétnych fyzických zariadení (napr. federálne budovy, vojenské zariadenia, vstupy na hraničné priechody)[2].

- **Referenčný monitor** je termín bezpečnostného inžinierstva pre funkčnosť IT, ktorý (1) riadi všetky prístupy, (2) nemožno ho pri prístupe obísť, (3) je odolný voči neoprávneným zásahom a (4) poskytuje dôveru, že ostatné tri položky sú splnené.



Obr. 7.1: Riadenie prístupu a ďalšie bezpečnostné mechanizmy.

Riadenie prístupu sa spolieha na ďalšie bezpečnostné mechanizmy v informačnom systéme a spolupracuje s nimi. Na Obrázku 7.1 sú znázornené relevantné bezpečnostné mechanizmy a to autentizácia a autorizácia [12]. Výklad týchto pojmov opäť prevezmeme z [7].

- **Autentizácia** je overenie totožnosti používateľa, procesu alebo zariadenia, často ako predpoklad povolenia prístupu k zdrojom v informačnom systéme.
- **Autorizácia** je prístupové právo udelené používateľovi, programu alebo procesu alebo úkon udelenia týchto práv.

Riadenie prístupu sa týka obmedzenia aktivít oprávnených používateľov. Obmedzenia vynucuje referenčný monitor, ktorý sprostredkuje každý pokus o prístup používateľa (alebo programu vykonávaného v mene tohto používateľa) k objektom v informačnom systéme. Referenčný monitor sa dopytuje autorizačnej databázy s cieľom zistiť, či používateľ je oprávnený vykonať operáciu, o ktorú sa pokúša. Autorizácie v tejto databáze spravuje a udržiava bezpečnostný

[2]Treba si všimnúť, že definícia pojmu riadenie prístupu je všeobecnejšia a zahrňuje aj riadenie fyzického prístupu.

administrátor. Bezpečnostný administrátor nastavuje tieto autorizácie na základe bezpečnostnej politiky organizácie. Používatelia môžu tiež upraviť niektoré časti autorizačnej databázy, napríklad nastaviť povolenia pre ich osobné súbory (presnejšie súbory, ktorých sú vlastníci). Audit monitoruje a vedie záznamy o relevantných aktivitách v systéme.

Obrázok 7.1 zobrazuje bezpečnostné mechanizmy a ich interakcie na logickej úrovni. Nemalo by sa to interpretovať doslovne. Ako uvidíme neskoršie, napríklad autorizačná databáza sa často ukladá s objektmi, ktoré sú chránené referenčným monitorom, a nie vo fyzicky oddelenej oblasti. Obrázok je tiež trochu idealizovaný v tom, že oddelenie medzi autentizačnými mechanizmami, riadením prístupu, auditovaním a administráciou nemusí byť vždy také jasné, ako to ukazuje obrázok. Toto oddelenie sa považuje za vysoko žiaduce, ale nie v každom systéme sa vždy dôsledne implementuje.

Je dôležité jasne rozlišovať medzi autentizáciou a riadením prístupu. Za správne zistenie identity používateľa je zodpovedný mechanizmus autentizácie (niekedy sa používa aj termín autentizačná služba). Riadenie prístupu predpokladá, že autentizácia používateľa bola úspešne overená pred vynútením riadenia prístupu prostredníctvom referenčného monitora. Účinnosť riadenia prístupu spočíva na správnej identifikácii používateľa a na správnosti nastavených autorizácií, ktorými sa riadi referenčný monitor (ako súčasť funkcie riadenia prístupu).

Je dôležité uvedomiť si, že riadenie prístupu nie je z bezpečnostného hľadiska úplným riešením pre zabezpečenie informačného systému. Musí byť spojené s auditovaním. Opatrenia auditu sa využívajú na následnú analýzu všetkých žiadostí a aktvít používateľa v systéme. Auditovanie si vyžaduje zaznamenanie (logovanie) všetkých žiadostí a aktivít používateľa v systéme pre ich neskoršiu analýzu. Opatrenia auditu majú multiplikatívny efekt. Jednak sú užitočné na odstrašenie (používatelia sú odrádzaní od pokusov o narušenie systému, ak vedia, že všetky ich žiadosti sú sledované), ako aj prostriedky na analýzu správania sa používateľov pri používaní systému ako aj na zistenie možných pokusov o narušenie alebo skutočného narušenia. Okrem toho môže byť auditovanie užitočné pri určovaní možných nedostatkov v bezpečnostnom systéme pri nevhodnom nastavení bezpečnostnej politiky informačného systému. Auditovanie je nakoniec nevyhnutné aj na zabezpečenie toho, aby autorizovaní používatelia nezneužívali svoje oprávnenia. Inými slovami, viesť používateľov k zodpovednosti za svoje aktivity. Treba poznamenať, že základnou podmienkou efektívneho auditovania je fungovanie spoľahlivej autentizácie.

V systémoch riadenia prístupu sa všeobecne rozlišuje medzi politikami a mechanizmami. Politiky sú vysokoúrovňové usmernenia, ktoré určujú ako sú riadené prístupy a ako sú stanovené rozhodnutia o prístupe. Mechanizmy sú nízkoúrovňové softvérové a hardvérové nástroje, ktoré možno nakonfigurovať tak, aby implementovali danú politiku. Snahou návrhárov je vyvinúť mechanizmy riadenia prístupu tak, aby boli nezávislé od politiky, na implementáciu ktorej by sa mali použiť. Toto je žiaduci cieľ, aby bolo možné opakované použitie mechanizmov, ktoré slúžia na rôzne bezpečnostné účely. Rovnaké mechanizmy sa často môžu použiť na podporu cieľov dôvernosti, integrity alebo dostupnosti.

V článku [9] je podaný rozsiahly prehľad o mechanizmoch riadenia prístupu.

7.3.2 Prístupové operácie

Rozlišovanie entít v počítačovom systéme na subjekty a objekty je základom riadenia prístupu. Subjekty iniciujú akcie alebo operácie nad objektami. Tieto akcie sú povolené alebo zamietnuté v súlade so zavedenými autorizáciami v systéme. Autorizácia je vyjadrená v zmysle pridelenia prístupových práv alebo prístupových režimov subjektu k objektu. Význam práv závisí od konkrétneho objektu. Prístupové právo opisuje spôsob prístupu subjektu k objektu. Prístupové práva by mohli predstavovať nasledujúce:

- **Čítať:** Používateľ si môže zobraziť informácie uložené v systémovom zdroji (napr. súbor, vybrané záznamy v súbore, vybrané polia v zázname alebo nejakú kombináciu). Prístup čítať zahrňuje možnosť kopírovať alebo tlačiť.
- **Zapísať:** Používateľ môže pridávať, modifikovať alebo vymazať údaje v systémových zdrojoch (napr. súbory, záznamy, programy). Prístup zapísať obsahuje prístup čítať.
- **Pripojiť:** Používateľ pripája údaje k súboru bez toho, aby súbor čítal.
- **Vykonať:** Používateľ vykoná špecifikované programy.
- **Vlastniť:** Používateľ nastavuje prístupové práva k systémovým zdrojom, ktoré vlastní.

Pre súbory sú typické prístupové práva čítať, zapísať, vykonať a vlastniť. Význam týchto troch je z ich názvu zrejmý. Bližší výklad prístupových práv sa demonštruje na príklade bankového účtu. Objekt ako je napríklad bankový účet môže mať prístupové práva Dopyt (zistenie stavu finančných prostriedkov na bankovom účte), Kredit (vloženie finančných prostriedkov na bankový účet) a Debet (výber finančných prostriedkov z bankového účtu), čo zodpovedá základným operáciám nad bankovým účtom. Tieto operácie sa vykonajú príslušnými aplikačnými programami bankového informčného systému. Majiteľ bankového účtu má k svojmu účtu prístupové právo Dopyt, Kredit a Debet ale paradoxne nemá prístupové právo Vlastniť. Vlastníkom účtu majiteľa účtu je banka, ktorá rozhodne o tom, ktorí bankoví úradníci majú prístup k účtu klienta. Prístup bankových úradníkov k účtu klient je na základe ich pracovných funkcií v banke.

Pri demonštrácii prístupových práv sa dá na príklade bankového účtu ukázať aj prístupové právo Pripojiť. Všetky prístupy k bankovému účtu klienta auditný systém bankovej aplikácie zapisuje do auditného záznamu (logu). Informácie o prístupe k účtu klienta sa zapíše na koniec auditného záznamu bez toho, aby banková aplikácia auditný záznam čítala.

7.3.3 Štruktúry riadenia prístupu

Matica riadenia prístupu

Odborníci v oblasti bezpečnosti pri riešení riadenia prístupu vyvinuli v priebehu rokov množstvo abstrakcií. Asi najzákladnejšou abstrakciou z nich je koncept, že všetky zdroje riadené počítačovým systémom môžu byť reprezentované údajmi uloženými v objektoch. Ochrana objektov je preto rozhodujúcou požiadavkou na ochranu systému.

Prístupová matica je koncepčný model, ktorý určuje prístupové práva každého subjektu na každý objekt v systéme. V tejto matici má každý subjekt pridelený riadok a každý objekt

má pridelený stĺpec. Každý prvok matice špecifikuje prístup autorizovaný pre subjekt v riadku k objektu v stĺpci. Treba poznamenať, že model prístupovej matice jasne oddeľuje problém autentizácie od autorizácie.

Úlohou riadenia prístupu je zabezpečiť, aby sa skutočne vykonali iba tie operácie, ktoré sú autorizované prístupovou maticou. To sa realizuje prostredníctvom referenčného monitora, ktorý je zodpovedný za sprostredkovanie všetkých pokusov o operácie subjektov nad objektmi.

		Objekty			
		Súbor 1	Súbor 2	Súbor 3	Súbor 4
Subjekty	Používateľ A	Vlastniť Čítať Zapísať			Vlastniť Čítať Zapísať
	Používateľ B	Čítať	Vlastniť Čítať Zapísať		Čítať
	Používateľ C	Čítať Zapísať	Čítať	Vlastniť Čítať Zapísať	Zapísať

Obr. 7.2: Príklad prístupovej matice

Na obrázku 7.2 je príklad prístupovej matice pre systém, ktorý má troch používateľov (subjekty) a štyri súbory (objekty). Používateľ A vlastní Súbor 1 a tento súbor môže čítať a môže doňho zapisovať. Prístupové právo Vlastniť umožňuje Používateľovi A udeliť alebo odobrať Používateľovi B alebo Používateľovi C prístupové právo Čítať alebo Zapisovať z/do Súboru 1. Používateľ A vlastní Súbor 4 a tento súbor môže čítať a môže doňho zapisovať. Používateľ B vlastní Súbor 2 a tento súbor môže čítať a môže doňho zapisovať, Súbor 1 a Súbor 4 môže iba čítať. Používateľ B môže udeliť alebo odobrať Používateľovi A alebo Používateľovi C prístupové právo Čítať alebo Zapisovať z/do Súboru 2. Podľa prístupovej matice vidieť, že Používateľ A nemá udelené prístupové práva k Súboru 2 a k Súboru 3. Podobne to je aj v prípade Používateľa B, ktorý nemá udelené prístupové práva k Súboru 3. Používateľ C má prístup k všetkým súborom.

Aktivitu v systéme iniciujú entity známe ako subjekty. Subjekty sú zvyčajne používatelia alebo programy vykonávané v mene používateľov. Používateľ sa môže prihlásiť do systému pod viacerými prihlasovacími účtami. Teda z pohľadu systému môže predstavovať používateľ viacero subjektov v závislosti od toho, aké oprávnenia chce používateľ v danej relácii uplatniť. Napríklad používateľ pracujúci na dvoch rôznych projektoch sa môže prihlásiť na účely práce na jednom alebo druhom projekte. Potom máme tomuto používateľovi dva odpovedajúce subjekty, v závislosti od projektu, na ktorom používateľ momentálne pracuje.

Citlivou často prehliadanou skutočnosťou je fakt, že samotné subjekty môžu byť objektmi. Subjekt môže na splnenie svojej úlohy vytvoriť ďalšie subjekty. Rodičovský subjekt je zvyčajne schopný podľa potreby pozastaviť alebo ukončiť činnosť ním vytvorených subjektov. Skutočnosť, že subjekty môžu byť objekty, zodpovedá pozorovaniu, že iniciátor jednej operácie môže byť cieľom druhej.

Prístupová matica vzhľadom na počet subjektov a objektov v počítačovom systéme bude

veľmi rozsiahla a väčšina jej prvkov bude pravdepodobne prázdna (riedka matica). Vychádzajúc z tohto faktu je prístupová matica veľmi zriedka implementovaná ako matica. Teraz si preberieme niektoré bežné prístupy k implementácii prístupovej matice v praktických systémoch. Je možné prístupovú maticu dekomponovať po stĺpcoch a implementovať ju ako zoznam prístupových práv subjektov k danému objektu (zoznamy prístupových práv) alebo prístupovú maticu dekomponovať po riadkoch a implementovať ju ako zoznam prístupových práv k objektom pre daný subjekt (spôsobilosti) alebo maticu dekomponovať podľa jednotlivých prístupových práv ako tabuľku, v ktorej riadok predstavuje reláciu subjekt, prístupové právo, objekt (autorizačné relácie).

Zoznamy riadenia prístupu

Populárny prístup k implementácii prístupovej matice je prostredníctvom zoznamu riadenia prístupu ACL (Access Control List). Ku každému objektu je pripojený ACL, ktorý obsahuje zoznam subjektov autorizovaných pristúpiť k objektu. Tento prístup zodpovedá uloženiu prístupovej matice podľa stĺpcov. ACL zodpovedajúce súborom v prístupovej matici z obrázku 7.2 sú zapísané nižšie.

ACL pre Súbor 1:	Používateľ A:	Vlastniť, Čítať, Zapísať
	Používateľ B:	Čítať
	Používateľ C:	Čítať, Zapísať
ACL pre Súbor 2:	Používateľ B:	Vlastniť, Čítať, Zapísať
	Používateľ C:	Čítať
ACL pre Súbor 3:	Používateľ C:	Vlastniť, Čítať, Zapísať
ACL pre Súbor 4:	Používateľ A:	Vlastniť, Čítať, Zapísať
	Používateľ B:	Čítať
	Používateľ C:	Zapísať

Z pohľadu ACL objektu je ľahké určiť, ktoré režimy prístupov subjektov sú v súčasnosti pre tento objekt autorizované. Inými slovami, mechanizmus ACL umožňuje pohodlné riadenie prístupu k objektu. Je tiež ľahké odvolať všetky prístupy k objektu nahradením existujúceho ACL za prázdny ACL. Na druhej strane je v systéme s mechanizmom ACL ťažké určiť všetky autorizované prístupy subjektu. Na zistenie všetkých prístupových práv subjektu je potrebné preskúmať ACL každého objektu v systéme. Podobne, ak je potrebné zrušiť všetky prístupy subjektu, potom treba opäť preskúmať všetky zoznamy ACL a v relevantných ACL zrušiť prístupy deného subjektu. (V praxi je zrušenie všetkých prístupov subjektu často vykonávané zablokovaním používateľského účtu zodpovedajúceho danému subjektu. Je to akceptovateľné, ak používateľ opúšťa organizáciu. Ak je však používateľ v organizácii iba preložený, je pohodlnejšie ponechať mu účet a zmeniť jeho oprávnenia odrážajúce zmenené zaradenie používateľa.)

Mnoho systémov umožňuje, aby sa v ACL vyskytovali názvy skupín používateľov. Napríklad položka v zozname ACL ako SKUPINA: Čítať môže autorizovať všetkých členov skupiny SKUPINA na čítanie súboru. Niekoľko populárnych operačných systémov ako sú UNlX implementujú skrátenú formu ACL, v ktorej sa v ACL môže vyskytnúť malý počet, často iba jedno alebo dve mená skupín. Mená jednotlivých subjektov nie sú povolené. Pri takomto prístupe má ACL malú konštantnú veľkosť, takže ACL možno uložiť pomocou niekoľkých bitov

spojených so súborom. Na druhej strane existuje množstvo balíkov na riadenie prístupu, ktoré umožňujú pomocou zložitých pravidiel v ACL obmedziť, kedy a ako sa dá prístup vyvolať. Tieto pravidlá je možné uplatniť na jednotlivých používateľov alebo na všetkých používateľov, ktorí zodpovedajú definovanému vzoru vytvoreného z mena používateľa alebo iných atribútov používateľa.

Spôsobilosti

Spôsobilosti subjektu sú duálnym prístupom k mechanizmu ACL. Každý subjekt má zoznam (nazývaný zoznam spôsobilostí), v ktorom sú zapísané objekty, ku ktorým je subjekt autorizovaný pristúpiť. Tento mechanizmus zodpovedá uloženiu prístupovej matice podľa riadkov. Spôsobilosti zodpovedajúce používateľom v prístupovej matici z Obrázku 7.2 sú zapísané nižšie.

Spôsobilosti Používateľa A:	Súbor 1: Vlastniť, Čítať, Zapísať Súbor 4: Vlastniť, Čítať, Zapísať
Spôsobilosti Používateľa B:	Súbor 1: Vlastniť, Čítať, Zapísať Súbor 4: Vlastniť, Čítať, Zapísať
Spôsobilosti Používateľa C:	Súbor 1: Čítať, Zapísať Súbor 2: Čítať Súbor 3: Vlastniť, Čítať, Zapísať Súbor 4: Zapísať

Pri prístupe podľa zoznamu spôsobilostí je ľahké skontrolovať všetky prístupy, ktoré má subjekt oprávnený vykonať, jednoducho preskúmaním zoznamu spôsobilostí subjektu. Určenie všetkých subjektov, ktoré majú prístup k určitému objektu, si však vyžaduje preskúmanie zoznamu spôsobilostí každého subjektu. Bolo vyvinutých množstvo počítačových systémov s operačnými systémami založenými na spôsobilostiach, ale nepreukázalo sa, že by boli komerčne úspešné. Moderné operačné systémy zvyčajne využívajú prístup založený na ACL.

Je možné kombinovať mechanizmus ACL a spôsobilostí. Vlastnenie spôsobilosti subjektom je dostatočné na to, aby subjekt získal prístup autorizovaný touto spôsobilosťou. V distribuovanom systéme má tento prístup tú výhodu, že sa nevyžaduje opakovaná autentizácia subjektu. To umožňuje subjektu sa raz autentizovať, získať svoje spôsobilosti a potom prezentovať tieto spôsobilosti, aby získal služby z rôznych serverov v systéme. Každý server môže ďalej používať ACL na zabezpečenie jemnejšieho riadenia prístupu.

Autorizačné relácie

Videli sme, že prístupy založené na ACL a spôsobilostiach majú dvojaké výhody a nevýhody, pokiaľ ide o preskúmanie prístupu. Existujú reprezentácie prístupovej matice, ktoré neuprednastňujú jeden aspekt riadenia prístupu pred druhým. Napríklad prístupová matica môže byť reprezentovaná autorizačnou reláciou (alebo tabuľkou), ako je uvedené v tabuľke 7.1.

Každý riadok alebo trojica tejto tabuľky určuje jedno prístupové právo subjektu k objektu. Prístup Používateľa A k Súboru 1 preto vyžadujú tri riadky. Ak je táto tabuľka zoradená podľa subjektu, dostaneme formu zoznamov spôsobilostí. Ak je tabuľka zoradená podľa objektu,

Tabuľka 7.1: Tabuľka autorizačných relácií.

Subjekt	Prístupový režim	Objekt
Používateľ A	Vlastniť	Súbor 1
Používateľ A	Čítať	Súbor 1
Používateľ A	Zapísať	Súbor 1
Používateľ A	Vlastniť	Súbor 4
Používateľ A	Čítať	Súbor 4
Používateľ A	Zapísať	Súbor 4
Používateľ B	Čítať	Súbor 1
Používateľ B	Vlastniť	Súbor 2
Používateľ B	Čítať	Súbor 2
Používateľ B	Zapísať	Súbor 2
Používateľ B	Čítať	Súbor 4
Používateľ C	Čítať	Súbor 1
Používateľ C	Zapísať	Súbor 1
Používateľ C	Čítať	Súbor 2
Používateľ C	Vlastniť	Súbor 3
Používateľ C	Čítať	Súbor 3
Používateľ C	Zapísať	Súbor 3
Používateľ C	Zapísať	Súbor 4

dostaneme formu zoznamov ACL. Systémy manažmentu relačných databáz zvyčajne používajú takúto reprezentáciu.

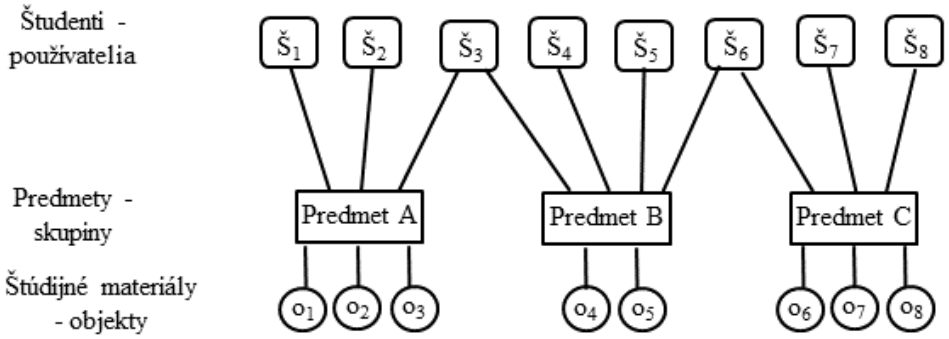
Prechodné vrstvy

Informačný systém môže mať veľa používateľov, Napríklad univerzitný informačný systém univerzity, ktorá má 15 000 študentov a 5 tisíc zamestnancov, má aspoň 20 000 tisíc používateľov. V informačnom systéme univerzity sa tiež nachádza niekoľko tisíc objektov. Ak by mal správca používateľov individuálne priraďovať prístupové práva používateľa k jednotlivým objektom informačného systému, bola by to aktivita veľmi náročná a iste nie bezchybná. Z dôvodu zjednodušenia práce správcu používateľov sa v mechanizme riadenia prístupu medzi používateľmi (subjektami) a objektami zavádzajú prechodná vrstva.

Uvedený koncept prechodnej vrstvy dokumentujme na jednoduchom príklade. Prednášajúci chce svojim študentom umožniť prístup k učebným materiálom. Namiesto toho, aby správca používateľov zaradil každého študenta na zoznam ACL pre každý materiál kurzu, správca používateľov umiestni všetkých študentov do skupiny a zaradí túto skupinu do príslušných ACL.

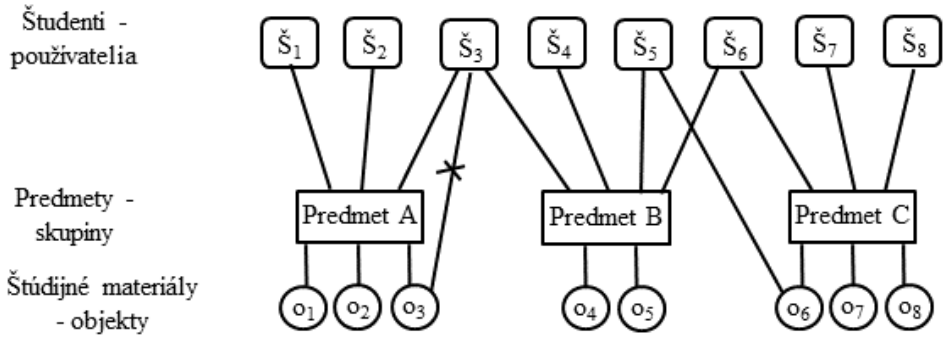
Skupiny sú teda prostriedkom na zjednodušenie definície politík riadenia prístupu a ich implementácií. Používatelia s podobnými prístupovými právami sa zaraďujú do skupín a skupinám sa udeľuje povolenie na prístup k objektom. Niektoré bezpečnostné politiky vyžadujú, aby mohol byť používateľ členom iba jednej skupiny, iné umožňujú členstvo vo viac ako jednej skupine.

Na Obrázku 7.3 je dokumentovaná situácia, v ktorej všetky prístupové práva používateľov sú sprostredkované prostredníctvom členstva v skupine. Študenti (používatelia) by mohli mať prístup vo všeobecnosti prístup študijným materiálom (objekty). Prístup študentov k študijným materiálom je sprostredkovaný prostredníctvom ich zaradenia do predmetov Predmet A, Predmet B a Predmet C (skupiny). Prístupové práva k študijným materiálom daného predmetu majú iba študenti zaradení do daného predmetu. Z Obrázku 7.3 vidno, že študent $Š_3$ je zaradený do dvoch predmetov Predmet A a Predmet B. Podobne študent $Š_6$ je zaradený do dvoch predmetov Predmet B a Predmet C.



Obr. 7.3: Skupiny ako prechodné vrstvy v riadení prístupu

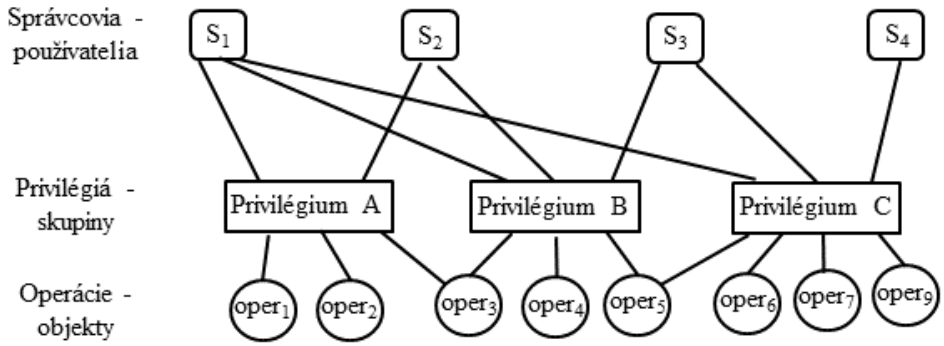
Bezpečnostné politiky majú často výnimky zo všeobecných pravidiel, v ktorých niektorý používateľ má povolenie na prístup k objektu priamo alebo v ktorých je používateľovi zamietnuté povolenie na prístup k objektu zvyčajne vyplývajúce z členstva v niektorej skupine. Negatívne povolenie je položka v štruktúre riadenia prístupu indikujúca prístup, ktorý používateľ nemá povolené vykonávať. Na Obrázku 7.4 je používateľovi $Š_3$ zamietnutý prístup k objektu o_3 (študent študuje Predmet A a Predmet B, študijné materiály na tému o_3 nepotrebuje vzhľadom na to, že súčasne študuje Predmet B) a používateľovi $Š_5$ je priamo udelený prístup k objektu o_6 (študent študuje Predmet Predmet B, študijné materiály na tému o_6 potrebuje na riešenie projektu).



Obr. 7.4: Konflikt v riadení prístupu

Negatívne povolenie udelené používateľovi $Š_3$ je v rozpore s pozitívnym povolením udeleným skupine Predmet A. Takáto situácia je príkladom konfliktu politiky. Pri určovaní politiky musí byť stanovené ako referenčný monitor vyrieši prípadné konflikty. Ak politiky sú definované

prostredníctvom zoznamu ACL, na riešenie konfliktov sa používa jednoduchý a široko používaný algoritmus, ktorý postupne prechádza zoznam ACL a aplikuje prvé pravidlo týkajúce sa daného používateľa. Ďalšie konfliktné položky uvedené v zozname sa ignorujú.



Obr. 7.5: Privilégiá ako prechodné vrstvy v riadení prístupu

Politika riadenia prístupu sa môže vzťahovať na operácie (nie iba elementárne prístupové práva), ktoré môže používateľ v systéme vykonávať. Termín privilégium sa používa na právo používateľa vykonávať určité operácie. Označenie privilégium je frekventovane používané, pretože privilégiá sú spojené s funkciami operačného systému prípadne ďalšími systémami ako sú napríklad databázy. Existujú privilégiá na správu systému, správu používateľov, správu databázy, zálohovanie, prístup k pošte alebo prístup k sieti. Na privilégiá možno nazerať ako na prechodovú vrstvu medzi subjektmi a operáciami. Schematicky je to znázornené na Obrázku 7.5. Systém spravuje viacero správcov (používatelia označení S_1 až S_4), v systéme je zriadených viacero privilégií (skupiny Privilégium A, Privilégium B, Privilégium C) a každému privilégiu sú pridelené operácie z množiny operácií (objekty $oper_1$ až $oper_9$).

7.4 Modely počítačovej bezpečnosti

Dva historické fakty poukazujú na zásadný problém, ktorý je potrebné riešiť v oblasti počítačovej bezpečnosti. Po prvé, všetky zložité softvérové systémy časom odhalili nedostatky alebo chyby, ktoré bolo potrebné následne opraviť. Po druhé, je mimoriadne obťažné, ak nie nemožné, vybudovať hardvérový/softvérový počítačový systém, ktorý nie je napadnuteľný rôznymi bezpečnostnými útokmi.

Problémy súvisiace so zaistením počítačovej bezpečnosti sa týkali návrhu a implementácie. Pri navrhovaní akéhokoľvek hardvérového alebo softvérového modulu je ťažké zabezpečiť, aby návrh skutočne zaisťoval zamýšľanú úroveň bezpečnosti. Tento problém má za následok veľa neočakávaných bezpečnostných zraniteľností. Aj keď je návrh v určitom zmysle správny, je ťažké, ak nie nemožné, implementovať návrh bez chýb, čo predstavuje ďalšie množstvo zraniteľností.

Uvedené problémy viedli k úsiliu vyvinúť metódu, ktorá dokazuje, že konkrétny návrh spĺňuje uvedený súbor bezpečnostných požiadaviek a že implementácia tohto návrhu presne zodpovedá špecifikácii návrhu. Na tento účel boli vyvinuté formálne modely počítačovej bezpečnosti, ktoré je možné použiť na overenie bezpečnostných návrhov a implementácií. V článku [9] je podaný rozsiahly prehľad o modeloch a politikách riadenia prístupu.

V tejto časti sa zameriame na snáď najvplyvnejší model počítačovej bezpečnosti, ktorým je model dôvernosti Bell-LaPadula. Následne opíšeme ďalšie modely zabezpečujúce riadenie prístupu (riadením prístupu sa zabezpečuje dôvernosť zdrojov počítačového systému) a to konkrétne model riadenia prístupu založený na rolách RBAC, model Čínskeho múru a model riadenia prístupu založený na atribútoch ABAC.

7.4.1 Model dôvernosti Bell-LaPadula

Model Bell-LaPadula je jedným z najvplyvnejších bezpečnostných modelov vo vojenskom prostredí. Model Bell-LaPadula bol navrhnutý na striktnú ochranu dôverných informácií. Aj keď model poskytuje ochrana dôvernosti informácií pre vojenské aplikácie, tento model je do určitej miery príliš prísny na použitie v komerčných prostrediach, v ktorých je dôležitejšia integrita informácií. Aplikácie postavené na modeli Bell-LaPadula sa preto väčšinou používajú vo vojenských alebo v podobných prostrediach.

Politika Bell-LaPadula [1] je politika kombinujúca viacúrovňovú bezpečnostnú politiku s politikou voliteľného riadenia prístupu. Politiky Bell-LaPadula presadzujú tak viacúrovňové bezpečnostné politiky (na zabezpečenie požiadaviek dôvernosti), ako aj politiky voliteľného riadenia prístupu (na zabezpečenie flexibility politík riadenia prístupu). Pri presadzovaní politiky Bell-LaPadula môže mať subjekt prístup k objektu iba vtedy, ak má subjekt prístup k objektu prostredníctvom viacúrovňovej bezpečnostnej politiky aj podľa politiky voliteľného riadenia prístupu.

V modeli Bell-LaPadula je každému subjektu a každému objektu priradená bezpečnostná trieda. V najjednoduchšej formulácii tvoria triedy bezpečnosti prísnu hierarchiu a označujú sa ako bezpečnostné úrovne. Príkladom je americká (rovnaká je aj v slovenskom zákone č. 215/2004) schéma vojenskej klasifikácie: prísne tajné > tajné > dôverné > vyhradené > neklasifikované. Znakom > je vyjadrený vzťah medzi bezpečnostnými úrovňami. Na ľavej strane znaku > je vyššia bezpečnostná úroveň, na pravej strane nižšia bezpečnostná úroveň. To znamená, že bezpečnostná úroveň prísne tajné je najvyššia bezpečnostná úroveň a bezpečnostná úroveň neklasifikované je najnižšia bezpečnostná úroveň.

Táto koncepcia je rovnako použiteľná v iných oblastiach, kde je možné informácie všeobecne usporiadať do úrovní, a používateľom môžu byť udelené povolenia na prístup k určitým informáciám. Napríklad najvyššia bezpečnostná úroveň môže byť pre dokumenty a informácie strategického podnikového plánovania, ktoré sú prístupné iba vrcholovým manažérom v organizácii; ďalšie by mohli byť citlivé finančné a osobné údaje, prístupné strednému manažmentu, vedúcim zamestnancom atď. To naznačuje takúto klasifikačnú schému: strategické > citlivé > dôverné > verejné.

V paxi často používame jednoduchú schému: dôverné > interné > verejné. Dôverné informácie sú dostupné iba určeným zamestnancon organizácie, interné informácie sú dostupné všetkým zamestnancom organizácie (sú to informácie, ktoré nechce organizácia zverejňovať) a verejné informácie sú dostupné verejnosti.

Komponenty modelu

Model Bell-LaPadula pozostáva z nasledujúcich komponentov:

- Množina S je množina subjektov systému. Subjekt sa bude označovať s. V pozícii subjektu budeme často hovoriť o používateľovi.
- Množina O je množina objektov systému. Objekt sa bude označovať o.
- Množina L je množina bezpečnostných úrovní definovaných v systéme. V množine L je definovaná operácia čiastočného usporiadania, ktorá sa označuje znakom menší alebo rovný $\leq$. Ak medzi dvomi bezpečnostnými úrovňami l_1 a l_2 platí vzťah $l_1 \leq l_2$ potom hovoríme, že bezpečnostná úroveň l_2 dominuje bezpečnostnej úrovni l_1.
- Množina F je množina trojíc $(f_S(s), f_O(o), f_C(s))$, kde $f_S(s)$ je maximálna bezpečnostná úroveň, ktorú subjekt s môže mať, $f_O(o)$ je bezpečnostná úroveň objektu o a $f_C(s)$ je aktuálna bezpečnostnú úroveň každého subjektu. Maximálna bezpečnostná úroveň subjektu sa niekedy nazýva previerka subjektu a bezpečnostná úroveň objektu sa niekedy nazýva bezpečnostná klasifikácia. Aktuálna bezpečnostná úroveň subjektu s nemôže byť vyššia ako je maximálna úroveň, teda $f_C(s) \leq f_S(s)$ vyjadrené slovne $f_S(s)$ dominuje $f_C(s)$.
- Množina $P = (V, \text{Č}, P, Z)$ je množina prístupových práv subjektov k objektom predstavujúcich Vykonať (execution), Čítať (read), Pripojiť (append) a Zapísať (write). Pri zapisovaní sa implicitne predpokladá, že subjekt má prístupové právo čítania. Prístupové právo sa bude vo všeobecnosti označovať písmenom p.
- Množina B je podmnožinou kartézskeho súčinu množín $S \times O \times P$ a je to množina aktuálnych prístupov, ktoré majú používatelia v systéme k dispozícii.
- Množina M je podmnožina kartézskeho súčinu $S \times O \times P$ a je to množina všetkých (voliteľných) prístupových práv, ktoré majú používatelia v systéme k dispozícii.

Bell-LaPadula modeluje stav systému ako štvoricu (b, m, f, h), kde b je podmnožina množiny B a obsahuje aktuálny povolený prístup pre používateľov, m je podmnožina množiny M a je to aktuálna množina všetkých prístupových práv pre používateľov,

$$f = (f_S(s), f_O(o), f_C(s)) \in F$$

je trojica funkcie bezpečnostných úrovní F a h je hierarchia objektov. K vôli jednoduchosti nebudeme v našich ďalších úvahách hierarchiu objektov h uvažovať.

Podľa modelu Bell-LaPadula je systém bezpečný, ak spĺňuje tri vlastnosti: jednoduchú bezpečnostnú vlastnosť (ss-vlastnsť), hviezdičkovú vlastnosť (*-vlastnosť) a voliteľnú bezpečnostnú vlastnosť (ds-vlastnosť). Ďalej sú podrobne opísané tieto uvedené vlastnosti.

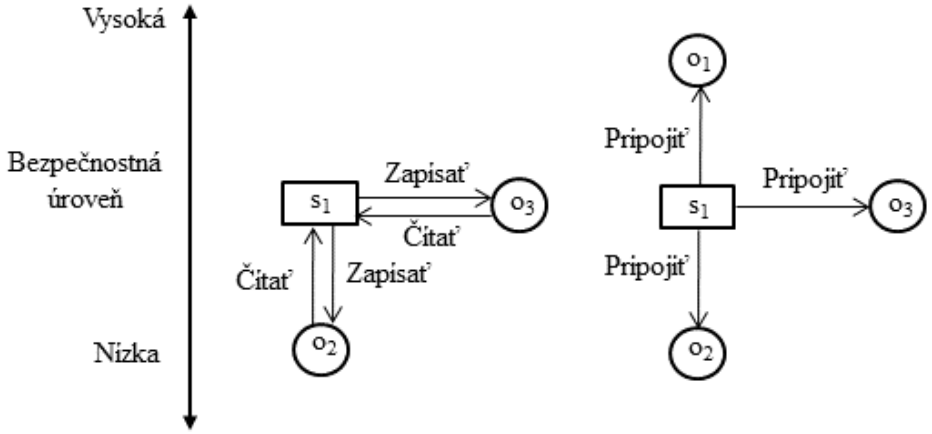
Jednoduchá bezpečnostná vlastnosť

Jednoduchá bezpečnostná vlastnosť vyjadruje tradičnú politiku nečítania nahor, v ktorej subjekt môže čítať alebo zapisovať do/z objektu s nižšou alebo rovnakou bezpečnostnou úrovňou než je úroveň subjektu.

Jednoduchú bezpečnostnú vlastnosť (single security property, označuje sa ako ss-vlastnosť) je možné formálne vyjadriť takto: Každý prvok $(s, o, p) \in S \times O \times P$ spĺňuje jednoduchú bezpečnostnú vlastnosť vtedy a len vtedy, ak platí jedno z týchto dvoch:

- $p = P$
- $p =$ Č alebo $p = Z$ a $f_O(o) \leq f_C(s)$.

Na obrázku 7.6 je to graficky vyjadrené v ľavej časti. Subjekt s_1 má prístupové práva Čítať a Zapisovať k objektom o_2 a o_3, pretože bezpečnostná úroveň objektov o_2 a o_3 nie je vyššia ako aktuálna bezpečnostná úroveň subjektu s_1. V pravej časti obrázku 7.6 je graficky formálne vyjadrené prístupové právo Pripojiť. Vzhľadom k tomu, že prístupové právo Pripojiť nevykonáva operáciu čítania, prístup subjektu s_1 k objektom o_1, o_2 a o_3 nie je obmedzený bezpečnostnou úrovňou subjektu.

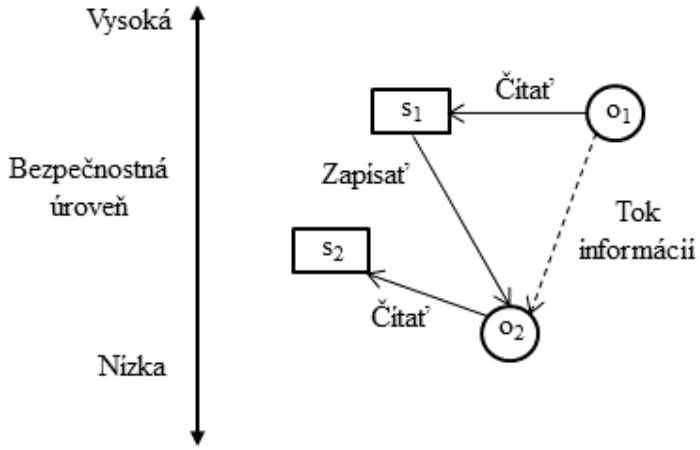


Obr. 7.6: Jednoduchá bezpečnostná vlastnosť.

Hviezdičková vlastnosť

Jednoduchá bezpečnostná vlastnosť vyjadruje tradičnú politiku nečítania nahor, v ktorej subjekt môže čítať alebo zapisovať dokument (objekt) s nižšou alebo rovnakou bezpečnostnou úrovňou než je úroveň subjektu. Čo v prípade, že subjekt má k dispozícii pamäť alebo kanál, ktorým môže prenášať informácie medzi objektami? Na Obrázku 7.7 je uvedený príklad toku informácií z objektu o_1 do objektu o_2. Subjekt s_1 má v zmysle jednoduchej bezpečnostnej vlastnosti prístup Čítať objekt o_1 a získanú informáciu z objektu o_1 preniesť prístupom Zapísať do objektu o_2. Touto operáciou dochádza k deklasifikovaniu informácie, pretože je prenesená informácia z objektu s vyššou bezpečnostnou úrovňou do objektu s nižšou bezpečnostnou úrovňou. To umožní inému subjektu s_2, ktorý má nižšiu bezpečnostnú úroveň ako subjekt s_1 (ale aspoň takú bezpečnostnú úroveň ako má objekt o_2), nasledujúci prístup čítania týchto informácií z objektu o_2.

Preto je potrebná politika na riadenie zápisu. Zápis subjektov do objektov nižšej úrovni môže spôsobovať nové problémy (ak predtým čítali z objektu vyššej úrovni). Takáto politika, označované ako *-vlastnosť, by mala zabezpečiť nezapisovanie nadol čo znamená, že subjekt s vyššou bezpečnostnou úrovňou by nemal byť schopný poslať správu subjektu s nižšou bezpečnostnou úrovňou. Toto obmedzenie je možné obísť dvomi spôsobmi a to dočasne znížiť



Obr. 7.7: Príklad toku informácií spôsobujúci ich deklasifikáciu

vysokú úroveň (toto je dôvod na zavedenie aktuálnej bezpečnostnej úrovni f_C) alebo identifikovať množinu subjektov, ktorým je dovolené porušiť *-vlastnosť (tieto subjekty sa nazývajú dôveryhodné subjekty).

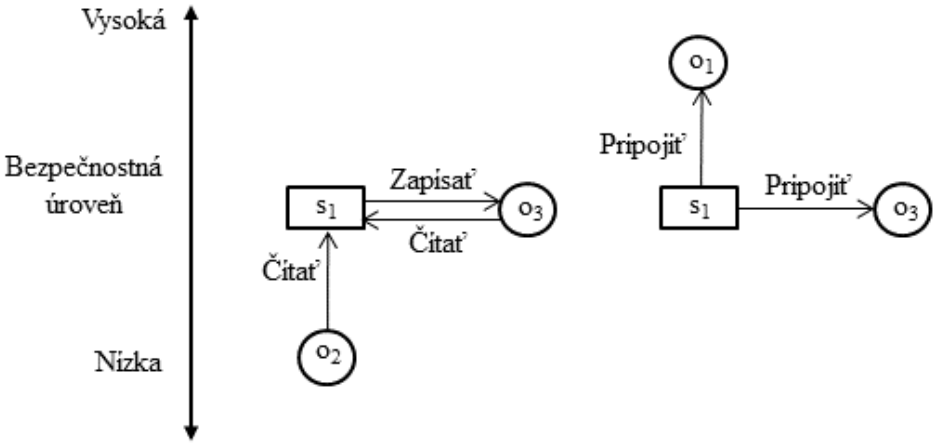
* -Vlastnosť (star property, označuje sa ako *-vlastnosť) je možné formálne vyjadriť takto. Každý prvok $(s, o, p) \in S \times O \times P$ vyhovuje *-vlastnosti vtedy a len vtedy, ak platí jedno z nasledujúcich pravidiel:

- $p = P$ a $f_C(s) \leq f_O(o)$,
- $p = Z$ a $f_C(s) = f_O(o)$,
- $p = \text{Č}$ a $f_O(o) \leq f_C(s)$.

Politiku na riadenie zápisu prostredníctvom *-vlastnosti je dokumentované na Obrázku 7.8. V ľavej časti obrázku subjekt s_1 číta a zapisuje prístupovými právami Čítať a Zapísať z/do objektu o_3 s rovnakou bezpečnostnou úrovňou. Navyše subjekt s_1 číta s prístupovým právom Čítať z objektu o_2, ktorý má nižšiu bezpečnostnú úroveň ako subjekt s_1. V pravej časti Obrázku 7.8 je graficky vyjadrené prístupové právo Pripojiť. Vzhľadom k tomu, že prístupové právo Pripojiť vykonáva zápis bez čítania, prístup subjektu s_1 k objektom o_1 a o_3 je v zmysle politiky povolený, pretože objekty o_1 a o_3 nemajú nižšiu bezpečnostnú úroveň ako je bezpečnostná úroveň subjektu s_1.

Voliteľná bezpečnostná vlastnosť

Voliteľná bezpečnostná vlastnosť (discretionary security property, označuje sa ako ds-vlastnosť): Stav systému (b, m, f, h) vyhovuje voliteľnej bezpečnostnej vlastnosti vtedy a iba vtedy, ak pre každý prvok $(s, o, p) \in b$, platí $(s, o, p) \in m$.



Obr. 7.8: Hviezdičková vlastnosť

Bezpečnosť modelu Bell-LaPadula

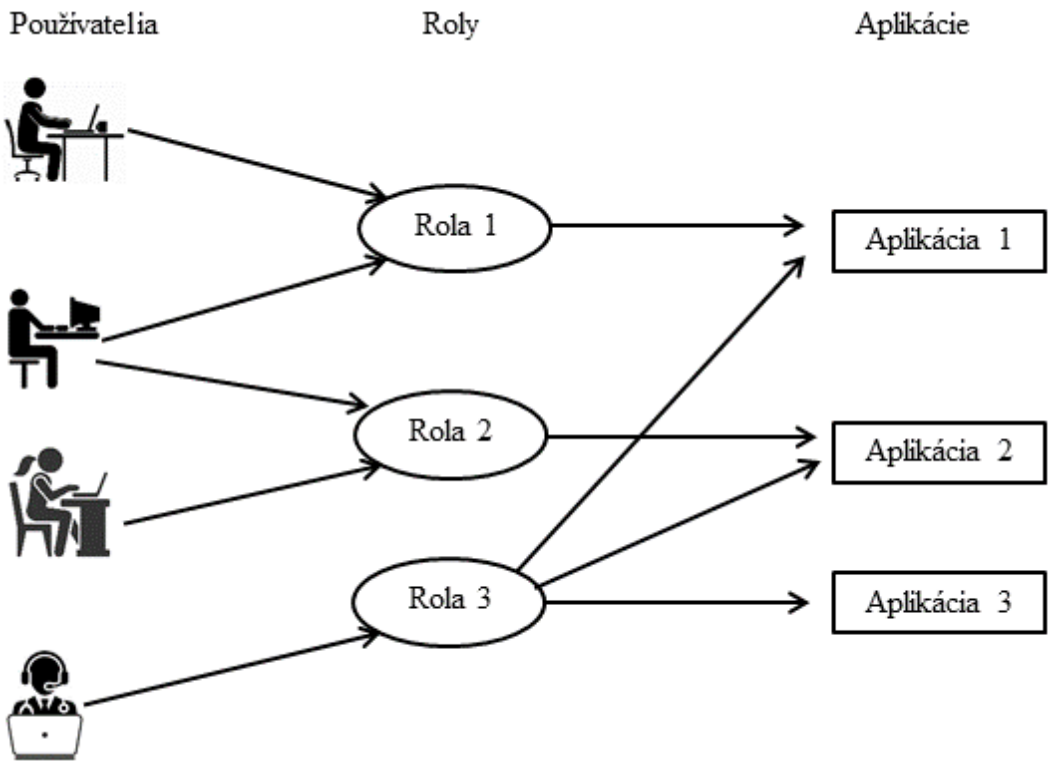
Dve bezpečnostné vlastnosti ss-vlastnosť a *-vlastnosť špecifikujú bezpečnostný model povinného riadenia prístupu MAC (Mandatory Access Control). V systéme MAC nie je povolený žiadny prístup, ktorý nesplňuje tieto dve vlastnosti. Model Bell-LaPadula okrem toho obsahuje ustanovenie o voliteľnom riadení prístupu DAC (Discretionary Access Control). Vyjadruje to ds-vlastnosť: Používateľ (subjekt) môže udeliť inému používateľovi prístup k dokumentu (objektu) na základe rozhodnutia vlastníka, obmedzeného pravidlami MAC. Subjekt môže teda vykonávať iba prístupy, na ktoré má potrebné oprávnenie a ktoré splňujú pravidlá MAC.

Okrem toho, že model Bell-LaPadula je pre komerčné organizácie z pohľadu riadenia prístupu (dôvernosti) veľmi prísny a teoreticky by mohol položiť základy bezpečného počítačového spracovania v prostredí jednej administratívnej oblasti, existujú určité dôležité obmedzenia jeho použiteľnosti a ťažkostí pri jeho implementácii. Prvým problémom je, že v jednom systéme viacúrovňovej bezpečnosti existuje nekompatibilita dôvernosti a integrity. Vo všeobecnosti môže viacúrovňová bezpečnosť fungovať buď pre oblasť integrity pre oblasť dôvernosti, ale nie pre obidve oblasti súčasne. Toto vzájomné vylúčenie možno analyzovať pri porovnaní modelu dôvernosti Bell-LaPadula a modelom integrity Biba [2]. Druhým dôležitým obmedzením použiteľnosti je takzvaný problém spolupracujúceho útočníka v prítomnosti skrytých kanálov [4]. V prípade zdieľaných zdrojov sa môže stať, že *-vlastnosť sa stane nevymožiteľnou. Toto je problém najmä v prítomnosti aktívneho obsahu, ktorý prevláda v súčasnom spracovaní textu a iných formátoch dokumentov. Škodlivý dokument by mohol obsahovať subjekt, ktorý by pri vykonávaní odvysielal utajované dokumenty pomocou skrytých kanálov vytvorených zdieľanými zdrojmi. Model Bell-LaPadula sa v podstate efektívne rozpadá, keď vykonateľné údaje s nízkou bezpečnostnou úrovňou môžu byť spracovávané subjektom s vysokou bezpečnostnou úrovňou.

7.4.2 Model riadenia prístupu založený na rolách

Koncept riadenia prístupu na základe rolí RBAC (Role Based Access Control) sa začal vo viacpoužívateľských a viacúlohových online systémoch na začiatku 70. rokov. Základný koncept RBAC spočíva v tom, že oprávnenia sú spojené s rolami a používateľom sú priradené príslušné role. Role sa vytvárajú pre rôzne pracovné funkcie v organizácii a používateľom sa prideľujú roly na základe ich povinností a kvalifikácie. Používateľov možno ľahko preradiť z jednej role do druhej. Rolám je možné udeliť nové oprávnenia, keď sa začlenia nové aplikácie a systémy, a oprávnenia je možné v prípade potreby z rolí odvolať. Základy konceptu riadenia prístupu na báze rolí sú podrobne opísané v prácach [10] a [11].

Na Obrázku 7.9 je demonštrovaný koncept RBAC. Systém poskytuje služby prostredníctvom troch aplikácií, oprávnenia k aplikáciám majú tri roly a štyria používatelia sú priradení k rolám.



Obr. 7.9: Koncept riadenia prístupu na základe rolí RBAC

Aj keď je koncepcia RBAC neutrálna z hľadiska politiky, priamo podporuje tri známe bezpečnostné princípy:

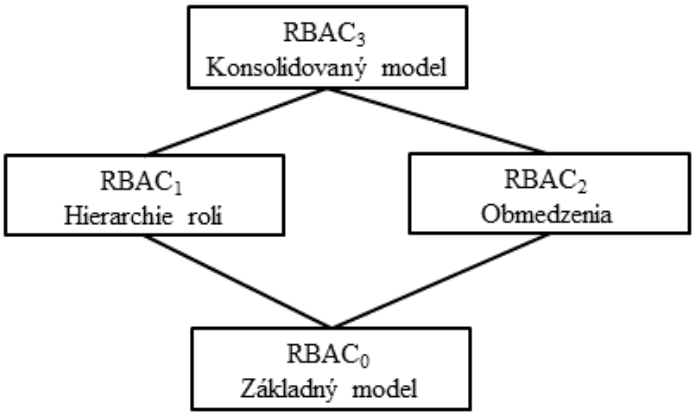
Najmenšie privilégium: Rolám sú pridelené iba tie oprávnenia, ktoré sú nevyhnutné pre úlohy vykonávané používateľom v role.

Oddelenie povinností: Na vykonanie citlivej úlohy môžu byť potrebné aktivity vzájomne sa vylučujúcich rolí, ako je napríklad požiadavka, aby sa na zaplatení faktúry podieľal

manažér nákupu (potvrdí, že nákup bol objednaný a dodaný) a manažér účtarne (zaplatí za skutočne objednaný a dodaný nákup).

Abstrakcia údajov: Namiesto prístupových práv čítať, zapísať a vykonať, ktoré zvyčajne poskytuje operačný systém, je možné vytvoriť abstraktné oprávnenia ako sú napríklad kreditné a debetné oprávnenia na objekte bankový účet.

Politiku riadenia prístupu RBAC možno modelovať viacerými súvisiacimi modelmi. S cieľom analyzovať rôzne dimenzie RBAC sú definované skupiny štyroch koncepčných modelov. Obrázok 7.10 zobrazuje vzťahy modelov. Základný model $RBAC_0$ je v spodnej časti a predstavuje minimálnou požiadavku pre systém RBAC. Pokročilé modely $RBAC_1$ a $RBAC_2$ zahrňujú model $RBAC_0$. Model $RBAC_1$ pridáva modelu $RBAC_0$ hierarchiu rolí, čo predstavuje situáciu, keď roly môžu dediť povolenia od iných rolí. Model $RBAC_2$ pridáva modelu $RBAC_0$ obmedzenia, ktoré kladú obmedzenia na akceptovateľné konfigurácie rôznych komponentov RBAC. Modely $RBAC_1$ a $RBAC_2$ sú v rámci RBAC jedinečné a nedajú sa navzájom zrovnávať. Konsolidovaný model $RBAC_3$ zahrňuje $RBAC_1$ a $RBAC_2$ a tranzitívne aj model $RBAC_0$. Štyri modely môžu slúžiť aj ako návod pri vývoji produktu a jeho hodnotení zákazníkmi.



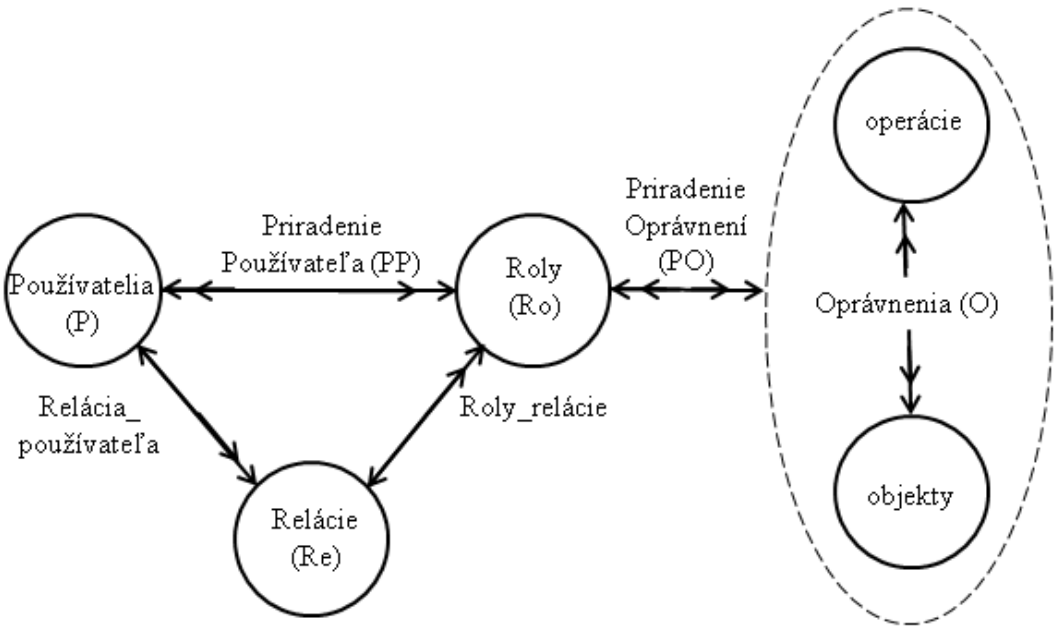
Obr. 7.10: Hierarchia referenčných modelov RBAC

Základný model $RBAC_0$

Na Obrázku 7.11 je základný model $RBAC_0$, pozostáva zo štyroch komponentov: používatelia (P), roly (Ro), oprávnenia (O) a relácie (Re).

Používatelia a roly. V uvedenom modeli je pre jednoduchosť používateľom osoba. Rola je pomenovaná pracovná funkcia v rámci organizácii, ktorá opisuje právomoc a zodpovednosť prenesenú na člena tejto roly.

Oprávnenie. Oprávnenie je schválenie konkrétneho režimu prístupu k jednému alebo viacerým objektom v systéme. Pojmy autorizácia, prístupové právo a privilégium sa v literatúre používajú aj na označenie oprávnenia. Oprávnenia sú vždy pozitívne a udeľujú ich držiteľovi spôsobilosť vykonať akciu v systéme. Objekty sú dátové objekty alebo objekty zdrojov reprezentované údajmi v počítačovom systéme.



Obr. 7.11: Základný model RBAC_0

Povaha oprávnenia do značnej miery závisí od typu a implementácie systému. Teda model všeobecného riadenia prístupu musí narábať s oprávneniami ako s neinterpretovateľnými symbolmi. Každý typ systému chráni objekty systému podľa danej abstrakcie implementovanej systémom, napríklad operačný systém chráni súbory, adresáre, zariadenia a porty prostredníctvom operácií ako je čítanie, zápis a vykonávanie.

Oprávnenia sa môžu vzťahovať na jednotlivé objekty alebo na mnoho objektov a môžu byť rovnako špecifické ako prístup na čítanie z konkrétneho súboru alebo rovnako všeobecné ako prístup na čítanie zo všetkých súborov patriacich konkrétnemu oddeleniu. Spôsob, akým sú jednotlivé oprávnenia spojené do všeobecného oprávnenia (aby ho bolo možné prideliť ako jediné oprávnenie), je vysoko implementačná závislý.

Obrázok 7.11 zobrazuje relácie priradenia používateľa (PP) a priradenia oprávnení (PO). Obidve relácie sú typu mnoho-na-mnoho a obidve relácie sú kľúčom k modelu RBAC. Používateľ môže patriť do mnohých rolí a rola môže mať veľa používateľov. Podobne rola môže mať veľa oprávnení a rovnaké oprávnenie je možné prideliť mnohým rolám. V konečnom dôsledku používateľ vykonáva oprávnenia. Pozícia role je úloha sprostredkovateľa umožňujúceho používateľovi vykonávať oprávnenie. Tento koncept poskytuje väčšiu kontrolu nad konfiguráciou riadenia prístupu a preskúmanie prístupu než ako by poskytoval priamy vzťah medzi používateľmi a oprávneniami.

Relácie. Používatelia vytvárajú relácie, počas ktorých môžu aktivovať podmnožinu rolí, do ktorých patria. Každá relácia mapuje jedného používateľa na pravdepodobne viacero rolí. Dve šipky v jednom smere na hrane od od uzla *Re* do uzla *Ro* na Obrázku 7.11 naznačuje, že je súčasne aktivovaných viacero rolí. Oprávnenia dostupné používateľovi sú zjednotením oprávnení všetkých rolí aktivovaných v danej relácii. Každá relácia z uzla *Re* je priradená k jednému používateľovi, ako je naznačené jednou šípkou na hrane z uzla *Re* do uzla *P* na

Obrázku 7.11. Toto priradenie zostáva konštantné po celú dobu relácie. Koncept relácie sa rovná tradičnému poňatiu subjektu v riadení prístupu.

Používateľ môže mať súčasne otvorených viacero relácií, každú v inom okne na obrazovke pracovnej stanice. Každá relácia môže kombinovať rôzne aktívne roly. Táto funkcia RBAC_0 podporuje princíp najmenších privilégií. Používateľ patriaci do niekoľkých rolí môže vyvolať ktorúkoľvek z nich, čo umožní vykonávanie úloh v rámci tejto relácii. Používateľ, ktorý je členom „silnej“ role (rola má významné oprávnania, napríklad zrušenie alebo vytvorenie objektu v systéme, zápis do bezpečnostných záznamov), tak môže bežne túto rolu ponechať deaktivovanú a v prípade potreby ju explicitne aktivujte. (Všetky obmedzenia sú opísané v modeli RBAC_2.) V modeli RBAC_0 používateľ podľa vlastného uváženia určuje aktivovanie rolí v danej relácii. Tento model tiež umožňuje počas relácie dynamicky aktivovať a deaktivovať roly.

Definícia modelu RBAC_0. Model má tieto komponenty:

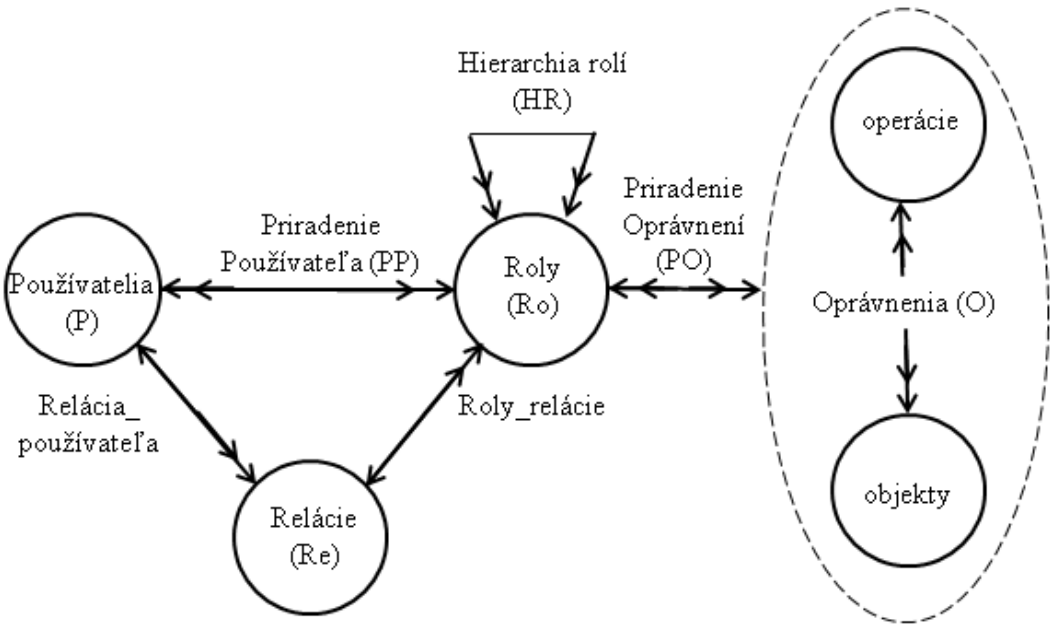
- Množiny P, Ro, O a Re sú používatelia, roly, oprávnenia a relácie.
- PO je podmnožina kartézskeho súčinu $O \times Ro$, relácia priradenia oprávnení k rolám, typ mnoho-na-mnoho.
- PP je podmnožina kartézskeho súčinu $P \times Ro$, relácia priradenia používateľov k rolám, typ mnoho-na-mnoho.
- Používateľ: $Re \to P$, funkcia mapujúca každú reláciu re_i (prvok množiny Re) na jedného používateľa, označené používateľ(re_i), (konštantné počas trvania relácie).
- Roly: $Re \to 2^{Ro}$, funkcia mapujúca každú reláciu re_i na množinu rolí, roly(re_i) je podmnožina množiny $\{ro \in Ro \mid (\text{používateľ}(re_i), ro) \in PP\}$ (ktorá sa môže s časom meniť) a relácia re_i má oprávnenia, ktoré sú zjednotením oprávnení (opr) rolí $ro \in \text{roly}(re_i)$, pričom $\{opr \in O \mid (opr, ro) \in PO\}$.

Hierarchie rolí – model RBAC_1

Model RBAC_1 zavádza hierarchie rolí (HR) ako je to znázornené na Obrázku 7.12. Princíp hierarchie rolí je prirodzený princíp v organizáciach a sú samozrejme bežne implementované v systémoch, ktoré poskytujú roly.

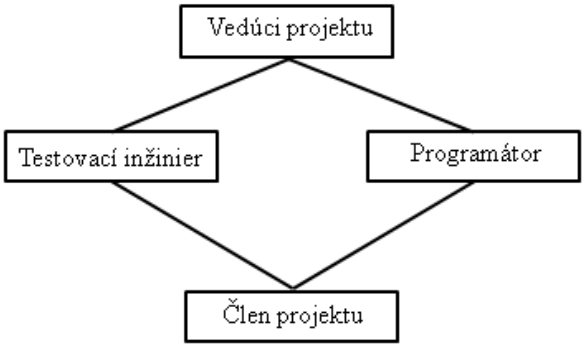
Hierarchie sú prirodzeným prostriedkom na štruktúrovanie rolí tak, aby odrážali línie manažmentu, pracovných povinností a zodpovedností v organizácie ako je zobrazené na Obrázku 7.13. Podľa konvencie sú „silnejšie“ role (seniorské) zobrazené v hornej časti týchto diagramov a „slabšie“ role (juniorské) role v dolnej časti.

Na Obrázku 7.13 je príklad vývojového tímu projektu, ktorý demonštruje koncept hierarchie rolí. Vývojový tím projektu má štyri roly a to, vedúci projektu, programátor, testovací inžinier a člen projektu. Každý člen projektu má oprávnenia prístupu k bežným údajom o projekte. Programátor má oprávnenie prístupu k bežným údajom o projekte a k zdrojovým kódom vyvíjanej aplikácie a k vývojovému prostrediu, v ktorom aplikáciu vyvíja. Testovací inžinier má oprávnenie prístupu k bežným údajom o projekte a k vyvinutej aplikácii a testovaciemu prostrediu, v ktorom aplikáciu testuje. Vedúci projektu má oprávnenia prístupu k bežným



Obr. 7.12: Model s hierarchiou rolí RBAC_1

údajom o projekte, k zdrojovým kódom vyvíjanej aplikácie a k vývojovému prostredu, v ktorom sa aplikácia vyvíja, k vyvinutej aplikácii a testovaciemu prostrediu, v ktorom sa aplikácia testuje. Ináč povedané, programátor a testovací inžinier dedia oprávnenia člena projektu a majú svoje špecifické oprávnenia. Vedúci projektu dedí oprávnenia programátora a testovacieho inžiniera.



Obr. 7.13: Hierarchia rolí vo vývojovom tíme projektu

Definícia modelu $\mathbf{RBAC}_1$. Model má tieto komponenty:

- Množiny P, Ro, O, Re, relácie PO, PP a používateľ sú rovnaké ako v RBAC_0.
- Množina HR je podmnožinou kartézskeho súčinu $Ro \times Ro$, predstavuje čiastočné usporiadanie na množine Ro a nazýva sa hierarchia rolí. Zapíše sa vzťahom dominancie rolí $\geq$.

- Roly: $Re \rightarrow 2^{Ro}$, oproti RBAC_0 je funkcia upravená, požaduje sa, aby roly(re_i) boli podmnožinou množiny

$$\{ro \in Ro \mid \exists \text{ rola } ro_1 \geq ro \text{ taká, že } (\text{používateľ}(re_i), ro_1) \in PP\}$$

(ktorá sa môže s časom meniť) a relácia re_i má oprávnenia, ktoré sú zjednotením oprávnení (opr) rolí $ro \in \text{role}(re_i)$, pričom $\{opr \in O \mid (\exists\, ro_2 \leq ro)\ (opr, ro_2) \in PO)\}$.

Obmedzenia – model RBAC_2

Model RBAC_2 zavádza do modelu RBAC_0 obmedzenia. Aj keď sú modely označené vzostupným číslovaním RBAC_1 a RBAC_2, v skutočnosti nejde medzi týmito modelmi o následnú závislosť. Je možné do modelu RBAC_0 zaviesť alebo obmedzenia alebo hierarchie rolí (vzťahy medzi RBAC_1 a RBAC_2 sú na Obrázku 7.10 a nedajú sa navzájom zrovnávať). Obmedzenia sú dôležitým aspektom RBAC a niekedy sa o nich tvrdí, že sú hlavnou motiváciou pre zavedenie politiky RBAC. Bežným príkladom sú vzájomne disjunktné roly v organizácii, ako napríklad manažér nákupu (objedná nákup a nákup prevezme) a manažér účtarne (platí faktúry za nákupy). Všeobecne platí, že tá istá osoba nemôže patriť do oboch rolí, pretože vytvára sa tak možnosť spáchania podvodu (sám so sebou je ľahká dohoda). Tejto známej a uznávanej zásade sa hovorí oddelenie povinností.

Obmedzenia sú silným mechanizmom pri koncipovaní politiky organizácie na vyššej úrovni. Keď sa určité roly stanovia ako vzájomne sa vylučujúce, použije sa mechanizmus obmedzenia pri priradení jednotlivých používateľov k rolám. Priradenie používateľov je možné delegovať a decentralizovať bez obáv z ohrozenia celkových cieľov politiky organizácie.

Vo vzťahu k RBAC_0 sa obmedzenia môžu aplikovať na relácie PP a PO a pre relácie re z množiny relácií Re na funkcie používateľov a rolí. Ak sa použijú obmedzenia, predikáty vyhodnocujúce riadenie prístupu môžu vrátiť hodnotu „akceptovateľný“ alebo „neakceptovateľný“. Intuitívne sa na obmedzenia dá lepšie pozerať podľa ich typu a povahe. Obmedzenia sa môžu napríklad považovať za vety vo formálnom jazyku. Pretože o obmedzeniach hovoríme neformálne, odráža to aj nasledujúca definícia.

Definícia modelu RBAC_2. Model je rovnaký ako RBAC_0 až na to, že sú zavedené obmedzenia na stanovenie akceptovateľnosti rôznych komponentov RBAC_0. Povolené budú iba akceptovateľné hodnoty.

Z pohľadu implementácii RBAC sa vo všeobecnosti vyžadujú jednoduché obmedzenia, ktoré je možné efektívne skontrolovať a vynútiť. Našťastie v RBAC môžu jednoduché obmedzenia trvať dlhý čas. Ďalej analyzujme niektoré obmedzenia, ktoré považujeme za rozumné implementovať. Pretože väčšina obmedzení aplikovaných na reláciu priradenia používateľa má náprotivok v relácii priradenia oprávnení, je potrebné analyzovať obmedzenia na týchto dvoch komponentoch paralelne. Nižšie si podrobnejšie opíšeme tieto tri obmedzenia: vzájomne vylučujúce sa roly, kardinalita a predpokladané roly.

Vzájomne vylučujúce sa roly. Najbežnejším obmedzením v politike RBAC sú vzájomne sa vylučujúce roly. Rovnakému používateľovi je možné priradiť najviac jednu rolu vo vzájomne sa vylučujúcej množine. To podporuje oddelenie povinností, ktoré je ďalej zabezpečené obmedzením vzájomného vylúčenia pri prideľovaní oprávnení.

Duálne obmedzenie pre priraďovania oprávnení poskytuje ďalšiu záruku oddelenia povinností. Toto duálne obmedzenie vyžaduje, aby bolo rovnaké oprávnenie pridelené najviac jednej role vo vzájomne sa vylučujúcej množine. Uvažujeme napríklad dve navzájom sa vylučujúce roly, a to manažér nákupu a manažér účtarne. Vzájomné vylúčenie z hľadiska priradenia používateľov špecifikuje, že ani jeden z nich nemôže patriť do oboch rolí. Vzájomné vylúčenie z hľadiska priradenia oprávnení špecifikuje, že napríklad obidvom rolám nemožno priradiť rovnaké oprávnenia (napríklad zaplatiť faktúru). Takéto oprávnenie by sa zvyčajne pridelilo role manažér účtarne. Obmedzenie vzájomného vylúčenia zo strany priradenia používateľov by zabránilo neúmyselnému alebo zlomyseľnému priradeniu oprávnenia k role manažér nákupu. Presnejšie povedané, obmedzenia vylúčenia pri priradení oprávnení obmedzujú distribúciu „silných“ oprávnení. Nemusí napríklad záležať na tom, či rola A alebo rola B dostane podpisové právo pre konkrétny účet, dôležité však je, že toto oprávnenie dostane iba jedna z dvoch rolí. Vo všeobecnosti možno zakázať rôzne kombinácie rolí. Používateľ môže napríklad patriť do role programátora aj do role testera v rôznych projektoch, ale v rámci toho istého projektu to je neakceptovateľné. Podobne môžu byť zakázané rôzne kombinácie oprávnení.

Kardinalita. Ďalším obmedzením priraďovania používateľov do roly je maximálny počet členov v role. Iba jedna osoba môže vykonávať rolu vedúceho oddelenia; podobne môže byť tiež obmedzený počet rolí, do ktorých môže jeden používateľ patriť. Toto sú obmedzenia kardinality, ktoré je možné príslušne použiť na priradenie oprávnení na riadenie distribúcie „silných“ oprávnení. Na druhej strane môže byť ťažké implementovať obmedzenia minimálnej kardinality. Ak si napríklad rola vyžaduje minimálny počet členov, pre systém by bolo ťažké zistiť, či jeden z členov „zmizol“, a odpovedať primerane.

Predpokladané roly. Koncept predpokladaných rolí je založený na právomoci a vhodnosti, pričom používateľa je možné priradiť k role A, iba ak je už užívateľ priradený k role B. Napríklad iba používatelia už priradení k role člena projektu, môžu byť priradení k role testovania v danom projekte. Predpokladaná (projektová) rola člena projektu je nižšia (juniorská) ako nová (testovacia) rola. V praxi je menej pravdepodobné, že sa vyskytnú predpoklady medzi nekompatibilnými rolami.

Dvojité obmedzenie priraďovania oprávnení sa uplatňuje skôr na roly ako na relácii priradenia oprávnení. Z dôvodu konzistencie môže byť oprávnenie opr_1 priradené k role iba vtedy, ak táto rola už má oprávnenie opr_2. V mnohých systémoch napríklad oprávnenie na čítanie súboru vyžaduje oprávnenia na čítanie adresára, v ktorom sa súbor nachádza. Pridelenie prvého oprávnenia bez druhého oprávnenia by bolo neúplné.

Konsolidovaný model – $\mathbf{RBAC_3}$

Model $RBAC_3$ zahrňuje hierarchie rolí aj obmedzenia, pretože kombinuje $RBAC_1$ a $RBAC_2$. Kombinácia oboch konceptov prináša niekoľko problémov, z ktorých najdôležitejšie sú obmedzenia na hierarchiu rolí a interakcie.

Obmedzenia na hierarchii rolí. Obmedzenia sa môžu sa vzťahovať na samotnú hierarchiu rolí. Hierarchia rolí musí predstavovať čiastočné usporiadanie (obmedzenie vlastné tomuto modelu). Ďalšie obmedzenia môžu obmedziť počet vyšších alebo nižších rolí, ktoré daná rola môže mať. Dve alebo viac rolí možno tiež obmedziť tak, aby nemali žiadnu spoločnú seniorskú (alebo juniorskú) rolu. Takéto obmedzenia sú užitočné, keď je oprávnenie na zmenu hierarchie

rolí decentralizované, ale hlavný administrátor systému chce obmedziť spôsob, akým sa zmeny vykonávajú.

Interakcie. Medzi obmedzeniami a hierarchiami vznikajú jemné interakcie. Predpokladajme, že roly testovacieho inžiniera a programátora sa v kontexte Obrázku 7.13 vzájomne vylučujú. Rola vedúceho projektu porušuje toto obmedzenie vzájomného vylúčenia. Takéto porušenie rolou vedúceho projektu môže alebo nemusí byť akceptovateľné. Model by mal preto vyhovieť obom možnostiam. Podobná situácia sa týka obmedzenia kardinality. Predpokladajme, že používateľ môže byť priradený najviac do jednej role. Porušuje pridelenie roly testovacieho inžiniera na Obrázku 7.13 toto obmedzenie? Inými slovami, uplatňujú sa obmedzenia kardinality iba na priame členstvo, alebo sa uplatňujú aj na zdedené členstvo?

7.4.3 Model Čínskeho múru

Model Čínskeho múru podľa Brewera a Nasha zachytáva pravidlá prístupu k informáciám v konzultačnej spoločnosti. Analytici spoločnosti sa musia vyhnúť konfliktu záujmov pri práci pre rôznych klientov [3]. Ku konfliktom dochádza preto, že klienti konzultačnej spoločnosti sú priamymi konkurentmi na rovnakom segmente trhu alebo z dôvodu vlastníctva spoločností. Pre analytikov spoločnosti musí platiť takáto bezpečnostná politika: Nesmie dochádzať k toku informácií, ktorý spôsobuje konflikt záujmov.

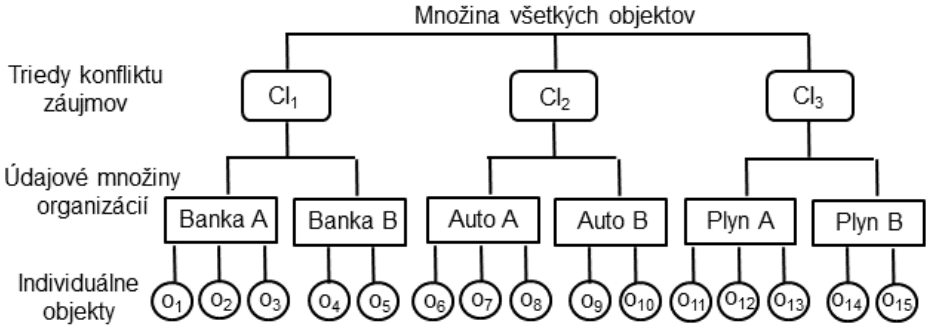
Príkladom z finančného sveta je trhový analytik pracujúci pre finančnú organizáciu poskytujúcu korporátne obchodné služby. Analytikovi sa nesmie povoliť poskytovať poradenstvo danej organizácii, ak má dôverné informácie (zasvätené interné informácie) o plánoch alebo postavení jej konkurenta. Analytik však môže radiť viacerým organizáciam, ktoré si navzájom nekonkurujú, a využívať informácie o trhu, ktoré sú prístupné verejnosti.

Pri modelovaní politiky Čínskeho múru pomocou množiny stavov modelu Bell – LaPadula je potrebné vykonať v modeli tejto politiky určité mierne úpravy:

- Subjekty: Analytici konzultačnej spoločnosti sú subjekty s a S je množina subjektov.
- Množina organizácií je označená C.
- Informácie: Informácie organizácií sú usporiadané do hierarchie s tromi úrovňami
  - Objekty: Jednotlivé položky informácií o_i, z ktorých každá sa týka jedinej organizácii. Súbor objektov o_i všetkých organizácií je označený O.
  - Údajová množina DS (DS – Data Set): všetky objekty o_i, ktoré sa týkajú tej istej organizácie. Funkcia $y : O \to C$ udáva údajovú množinu každej organizácie.
  - Trieda konfliktu záujmu CI (CI – Conflict of Interest): všetky údajové súbory, ktorých firmy súťažia. Funkcia $x : O \to P(C)$ udáva pre každý objekt triedu konfliktu záujmov, teda množinu všetkých organizácií, ktoré by sa nemali dozvedieť o obsahu objektu.
- Bezpečnostné návestie objektu o_i je dvojica $(x(o_i), y(o_i))$.
- Sanované informácie sú informácie, ktoré boli očistené od citlivých detailov a nepodliehajú obmedzeniam prístupu. Bezpečnostné návestie sanovaného objektu o_i je $(\emptyset, y(o_i))$.

- Pravidlá prístupu: Pravidlá prístupu na čítanie a zápis.

Obrázok 7.14 uvádza príklad. Sú k dispozícii údajové množiny (objekty o_i) reprezentujúce banky, automobilky a plynárenské spoločnosti. Všetky údajové množiny bánk sú v jednej triede konfliktu záujmu CI, všetky údajové súbory automobiliek v druhom CI, atď.



Obr. 7.14: Príklad s tromi triedami konfliktu záujmov

Na rozdiel od doteraz študovaných modelov, model Čínskeho múru nepriradzuje bezpečnostné úrovne subjektom a objektom, a preto to nie je skutočný viacúrovňový bezpečnostný model. Základom politiky Čínskeho múru je to, že subjekty majú prístup iba k informáciám, ktoré nie sú v konflikte s akýmikoľvek už získanými inými informáciami. Keď subjekt pristupuje k informáciám z jednej údajovej množiny, potom je nastavený múr na ochranu informácií z iných údajových množín v rovnakom CI. Subjekt má prístup k informáciám na jednej strane múru, ale nemá prístup k informáciám na druhej strane. Ďalej sa informácie v iných CI spočiatku nepovažujú za informácie na jednej alebo druhej strane múru, ale sa považujú za voľné. Ak rovnaký subjekt vykoná ďalšie prístupy do ďalších CI, tvar múru sa zmení s cieľom zachovať požadovanú ochranu. Každý subjekt je ďalej ovládaný svojím vlastným múrom – múry sú pre rôzne subjekty rôzne.

Konflikt záujmov nevzniká iba z objektov, ku ktorým subjekt pristupuje v súčasnosti, ale aj z objektov, ktoré boli subjektu sprístupnené v minulosti. Potrebujeme preto údajovú štruktúru, ktorá by zaznamenávala históriu pristupovania subjektov k objektom. Tomuto účelu slúži booleovská matica $S \times O$ s prvkami $N_{s,o}$, kde $N_{s,o}$ nadobúda hodnotu $TRUE$, ak subjekt s mal prístup k objektu o, a hodnotu $FALSE$, ak subjekt s nikdy nemal prístup k objektu o. Iniciálne nastavenie prvkov matice $N_{s,o}$ je $FALSE$ pre všetky $s \in S$ a všetky $o \in O$. Tento iniciálny stav splňuje bezpečnostné vlastnosti uvedené nižšie.

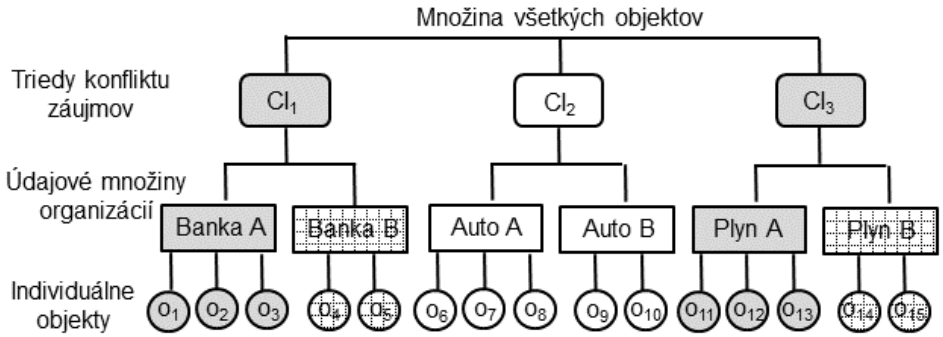
Jednoduchá bezpečnostná vlastnosť

Pravidlo jednoduchej bezpečnostnej vlastnosti sa zaoberá priamym tokom informácií. Chceme zabrániť tomu, aby bol subjekt vystavený konfliktu záujmov. Prístup je preto udelený iba vtedy, ak požadovaný objekt patrí do údajovej množiny organizácie, ktoré používateľ už má, alebo do údajovej množiny organizácie inej triedy konfliktu záujmov.

Uvedenú politiku môžeme formálne vyjadriť pravidlom jednoduchej bezpečnostnej vlastnosti (ss-vlastnosť). Pravidlo ss-vlastnosť: Subjekt s má povolený prístup k objektu o iba vtedy,

ak pre všetky objekty o_i, pre ktoré platí $N_{s,o} = TRUE$ je $y(o) = y(o_i)$ alebo $y(o)$ nie je prvkom množiny $x(o_i)$.

Na vyššie uvedenom príklade vysvetlíme fungovanie tohto pravidla. Predpokladajme, že v určitom okamihu podal Ján prvú žiadosť o prečítanie akéhokoľvek objektu o v údajovej množine Banka A, $o \in DS_{B,A}$. Pretože Ján predtým nepristúpil k žiadnemu objektu v inej DS v CI_1, prístup sa udelí. Ďalej si musí systém pamätať to, že prístup bol povolený, takže akákoľvek následná žiadosť o prístup k objektu v údajovej množine $DS_{B,B}$ organizácie Banka B bude zamietnutá. Akákoľvek žiadosť o prístup k iným objektom v údajovej množine $DS_{B,A}$ organizácie Banka A je povolená. Neskôr Ján požiada o prístup k objektu v údajovej množine $DS_{P,A}$ organizácie Plyn A. Pretože nejde o konflikt, je tento prístup povolený, ale je postavený múr, ktorý zakazuje následný prístup k údajovej množine $DS_{P,B}$ organizácie Plyn B, ako je to znázornené na Obrázku 7.15. Za múrom sú pre Jána údajové množiny vyplnené mrežami.



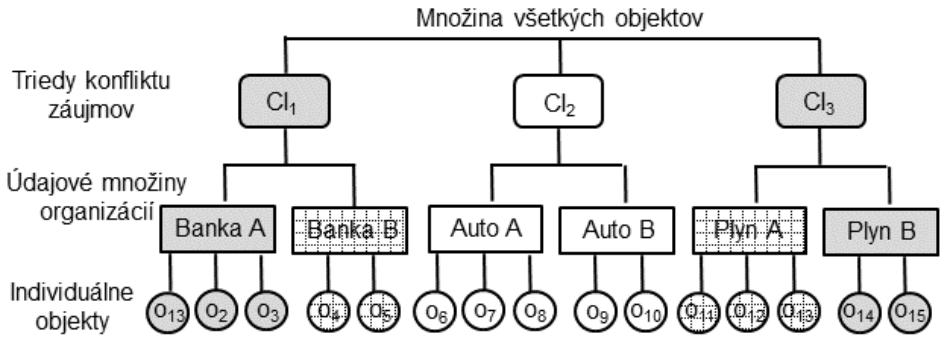
Obr. 7.15: Ján má prístup k objektom z $DS_{P,A}$ organizácie Plyn A a k objektom z $DS_{B,A}$ organizácie Banka A

Hviezdičková bezpečnostná vlastnosť

Na Obrázku 7.16 je zaznamenaná alternatívna história prístupu Márie. Jednoduché bezpečnostné pravidlo nebráni nepriamemu toku informácií, ktorý by mohol spôsobiť konflikt záujmov. V našom príklade má Ján prístup k objektom z $DS_{P,A}$ organizácie Plyn A a k objektom z $DS_{B,A}$ organizácie Banka A. Mária má prístup k objektom z $DS_{P,B}$ organizácie Plyn B a k objektom z $DS_{B,A}$ organizácie Banka A. Ak má Ján povolenie čítať z objektov z údajovej množiny $DS_{P,A}$ organizácie Plyn A a zapisovať do objektov údajovej množiny $DS_{B,A}$ organizácie Banka A, môže Ján prenášať informácie z údajovej množiny $DS_{P,A}$ organizácie Plyn A do údajovej množiny $DS_{B,A}$ organizácie Banka A, čo je indikované zmenou hodnoty prvého objektu o_1 z údajovej množiny $DS_{B,A}$ organizácie Banka A na o_{13}. Údaje môže potom následne Mária prečítať.

Mária by tak mala prístup k informáciám o organizáciách Plyn A aj o Plyn B, čo by viedlo ku konfliktu záujmov. Aby sa tomu zabránilo, má model Čínskeho múru druhé pravidlo. Pravidlo *-vlastnosť: Subjektu s je udelený prístup zápisu do objektu o iba vtedy, ak s nemá prístup čítania objektu o_i, pričom $y(o) \neq y(o_i)$ a $x(o_i) \neq \emptyset$.

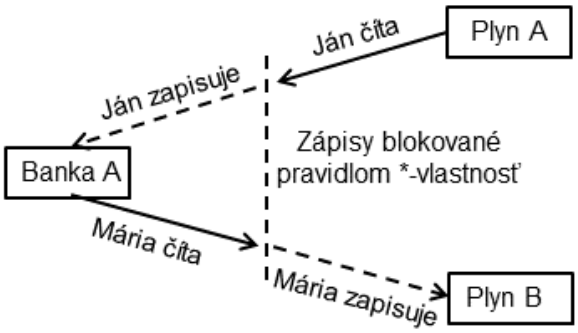
Podľa tohto pravidla prístup zápisu do objektu je povolený iba vtedy, ak nemôže byť čítaný žiadny iný objekt patriaci množine údajov inej organizácii, pričom objekt obsahuje nesanované informácie. Inak povedané, alebo subjekt nemôže zapísať vôbec alebo prístup subjektu (čítanie



Obr. 7.16: Mária má prístup k objektom z $DS_{P,B}$ organizácie Plyn B a k objektom $DS_{B,A}$ organizácie Banka A

aj zápis) je obmedzený na jednu údajovú množinu. Na predchádzajúcich obrázkoch by teda ani Ján ani Mária nemali mať prístup na zápis do žiadnych objektov v celkovom rozsahu údajov.

Pravidlo *-vlastnosť je dosť reštriktívne. V mnohých prípadoch však používateľ potrebuje iba prístup na čítanie, pretože používateľ vykonáva určitú analytickú úlohu. Model do určitej miery uľahčuje zápis a zavádza pojem sanácie údajov. Akékoľvek údajové množiny DS pozostávajúce výlučne zo sanovaných údajov nemusia byť chránené múrom. Preto sa na takéto údajové množiny DS nevzťahujú tieto dve pravidlá modelu Čínskeho múru.



Obr. 7.17: Operácie zápisu blokované pravidlom *-vlastnosť

Pre uvedený príklad je na Obrázku 7.17 znázornené blokovanie obidvoch operácií zápisu prostredníctvom pravidla *-vlastnosť. Táto vlastnosť zastaví nesanované informácie vytekajúce z množiny údajov organizácie.

Na rozdiel od modelu Bell-LaPadula, kde sa zvyčajne predpokladá statické pridelenie prístupových práv, v modeli Čínskeho múru musia byť prístupové práva pridelované v každom stavovom prechode.

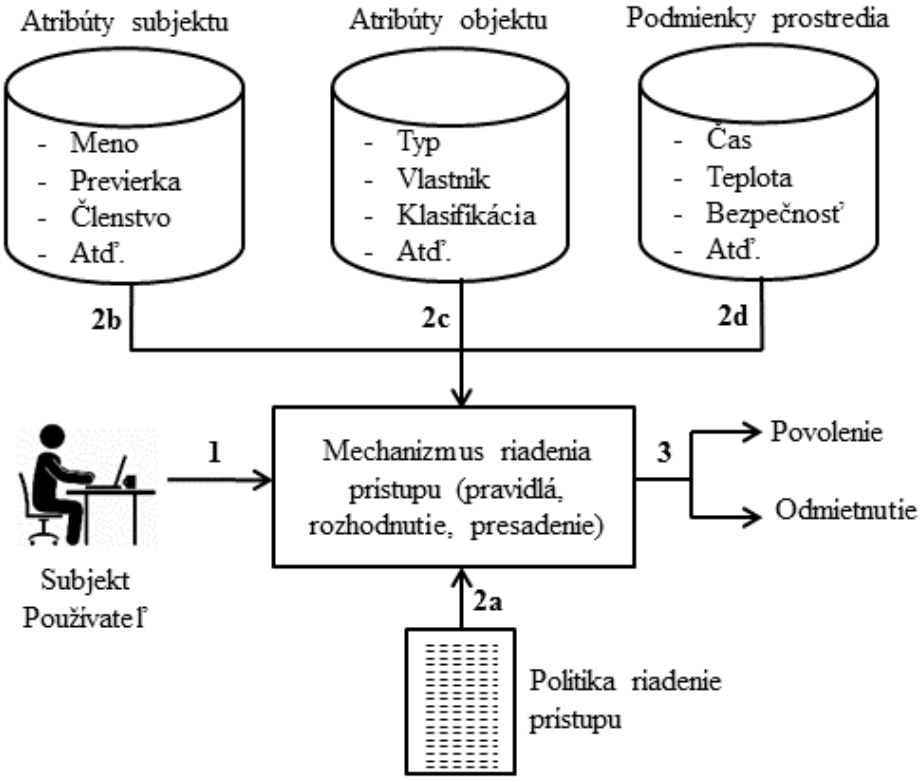
7.4.4 Model riadenia prístupu založený na atribútoch

Riadenie prístupu založené na atribúte ABAC (Attribute Based Access Control) je metóda riadenia prístupu, pri ktorej je žiadostiam subjektu o vykonanie operácií nad objektmi vyhovené

alebo zamietnuté na základe pridelených atribútov subjektu, pridelených atribútov objektu, podmienok prostredia a množiny politík, ktoré sú vyjadrené v termínoch týchto atribútov a podmienok. Počiatočné práce k problematike ABAC nožno nájsť v publikáciách [14], [13], [5]. Podrobnejší a systematický opis politiky prístupu ABAC možno nájsť v publikácii [6].

Atribúty sú charakteristiky subjektu, objektu alebo podmienok prostredia. Atribúty obsahujú informácie dané dvojicou (názov, hodnota).

Logická architektúra a vysokoúrovňová štruktúra systému ABAC je znázornená na Obrázku 7.18, kde mechanizmus riadenia prístupu ABAC prijíma žiadosti subjektu o prístup, potom preskúma atribúty subjektu a objektu vo vzťahu s konkrétnou politikou. Mechanizmus riadenia prístupu potom určuje, aké operácie môže subjekt vykonávať na objekte.



Obr. 7.18: Základný koncept ABAC

Proces rozhodnutia o povolení/odmietnutí prístupu subjektu k objektu v systéme ABAC je možné vyjadriť týmito krokmi:

1. Subjekt žiada o prístup k objektu.

2. Mechanizmus riadenia prístupu na stanovenie rozhodnutia povolenie/odmietnutie prístupu vyhodnocuje: Pravidlá politiky riadenia prístupu (2a), Atribúty subjektu (2b), Atribúty objektu (2c), Podmienky prostredia (2d).

3. Subjektu sa poskytuje prístup k objektu v prípade, že je pre prístup povolený.

Z logickej architektúry je zrejmé, že na rozhodnutie o riadení prístupu existujú štyri nezávislé zdroje informácií. Návrhár systému sa môže rozhodnúť, ktoré atribúty sú dôležité pre riadenie prístupu vzhľadom na subjekty, objekty a podmienky prostredia. Návrhár systému alebo iná systémová autorita (vlastník systému alebo administrátor) potom môže definovať politiky riadenia prístupu vo forme pravidiel pre akúkoľvek požadovanú kombináciu atribútov subjektu, objektu a podmienok prostredia. Je zrejmé, že tento prístup je veľmi silný a flexibilný. Je však pravdepodobné, že náklady tak z hľadiska komplexnosti návrhu a implementácie ako aj z hľadiska dopadu na výkonnosť prevýšia náklady iných konceptov riadenia prístupu. Toto je kompromis, ktorý musí vykonať systémová autorita.

Atribúty subjektu

Mnoho atribútov používateľa (subjektu) je zvyčajne poskytnutých pri vstupe do zamestnania v organizácii a môžu byť zabezpečené niekoľkými rôznymi útvarmi (ľudské zdroje, bezpečnosť, vedenie organizácie, atď.). Z týchto dôvodov sú spôsoby získania autoritatívnych (overených) údajov dobre známe. Napríklad iba útvary bezpečnosti by mali byť schopné poskytovať a uplatňovať atribúty bezpečnostnej previerky a hodnoty týchto atribútov na základe overených informácií o bezpečnostnej previerke používateľa. Používateľ by nemal byť schopný zmeniť svoju vlastnú hodnotu atribútu bezpečnostnej previerky. Medzi ďalšie atribúty subjektu môžu patriť aktuálne úlohy, fyzické umiestnenie subjektu a zariadenie, z ktorého sa odosiela požiadavka. Je potrebné vytvoriť procesy na hodnotenie a zabezpečenie kvality týchto údajov o atribútoch subjektu.

Atribúty objektu

Atribúty objektov sú zvyčajne poskytované pri vytváraní objektu. Atribúty môžu byť viazané na objekt alebo externe uložené a referencované. Dá sa očakávať, že útvary manažujúce riadenie prístupu nemôžu podrobne sledovať všetky udalosti. Tieto informácie sú často riadené nezabezpečenými procesmi a požiadavkami. Sú nevyhnutné vhodné údaje o atribútoch, ktoré podporujú rozhodnutia o správnom prístupe. Ďalej sa musia zaviesť opatrenia na zabezpečenie toho, aby sa atribúty objektov prideľovali a overovali procesmi, ktoré vlastník alebo administrátor objektu považuje za vhodné a autoritatívne. Napríklad atribúty objektu nesmia byť modifikovateľné subjektom, aby manipuloval s výsledkom rozhodnutia o riadení prístupu. Atribúty objektov musia byť dostupné mechanizmom riadenia prístupu pre vytvorenie rozhodnutia o prístupe. V prípade atribútov objektu ide o atribúty zdrojov systému. Môžu obsahovať atribúty o metaúdajoch týkajúcich sa objektu, ako napríklad údaje o autorovi, dátumu vytvorenia, poslednej zmene, veľkosti, type súboru, úrovni zabezpečenia atď., alebo obsah objektu, napríklad meno pacienta (napr. pre zdravotné záznamy), číslo študenta (napr. pre záznamy študentov), názov kapitoly atď.

Podmienky prostredia

Podmienky prostredia sa týkajú kontextových informácií, ktoré vo všeobecnosti nie sú spojené so žiadnym konkrétnym subjektom alebo objektom, ale sú požadované v rozhodovacom procese. Líšia sa od atribútov subjektu a objektu v tom, že nie sú administratívne vytvárané a manažované, ale sú inherentné a musia byť detekovateľné systémom ABAC. Podmienky prostredia, ako napríklad aktuálny dátum, čas, umiestnenie, hrozba a stav systému, sa zvyčajne pri autorizácii žiadosti o prístup hodnotia na základe aktuálnych odpovedajúcich premenných

prostredia. Podmienky prostredia umožňujú politikám ABAC špecifikovať výnimočné alebo dynamické pravidlá riadenia prístupu, ktoré nemožno opísať iba pomocou atribútov subjektu alebo objektu. Pri zostavovaní pravidiel ABAC s podmienkami prostredia je dôležité zabezpečiť, aby premenné podmienky prostredia a ich hodnoty boli globálne prístupné, chránené proti neoprávnenej manipulácii a relevantné pre prostredie, kde sa používajú.

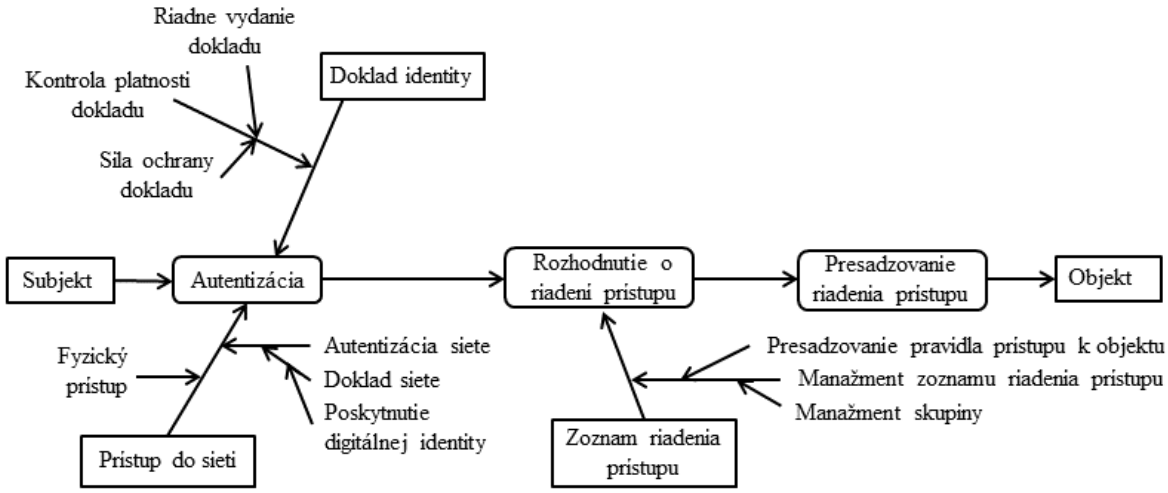
Pravidlá politiky riadenia prístupu

V systéme ABAC musia všetky pravidlá riadenia prístupu obsahovať určitú kombináciu atribútov a prípustných operácií. Môžu tiež obsahovať podmienky, hierarchické dedenie a komplexnú logiku. Spolu poskytujú pri implementácii ABAC bohatú škálu možností. Množiny pravidiel a ich aplikácia na objekty musia vhodne manažované. Pravidlá musia presne a úplne odrážať vysokoúrovňovú politiku riadenia prístupu a musia byť autoritatívne vypracované (niektoré organizáciami, iné vlastníkmi zdrojov), uplatňované, udržiavané, zdieľané a presadzované. ABAC umožňuje viacero pravidiel od viacerých zainteresovaných strán. Na koordináciu a dosiahnutie správnej rovnováhy medzi zdieľaním a ochranou sú potrebné nové techniky. V niektorých nastaveniach je možné obmedziť viditeľnosť pravidiel, ktoré pravidlá sa vzťahujú na ktoré objekty, a obmedziť tak pravdepodobnosť, že neoprávnené subjekty budú manipulovať s atribútmi s cieľom získať autorizáciu. V opačnom prípade by subjekty, ktorým bol zamietnutý prístup, mali metódu na overenie alebo nápravu okolností, ktoré spôsobili zamietnutie. Niektoré organizácie môžu chcieť sledovať zamietnutia, aby zistili, či sú pravidlá vhodné. Definovanie pravidiel a použité mechanizmy a procesy by podobne mali obsahovať robustné pravidlo riešenia konflikov (konflikt vzniká vtedy, ak použitie pravidiel nevedie k jednoznačnému rozhodnutiu o prístupe), schopnosť určovať konflikty pravidiel a procesy na ich riešenie.

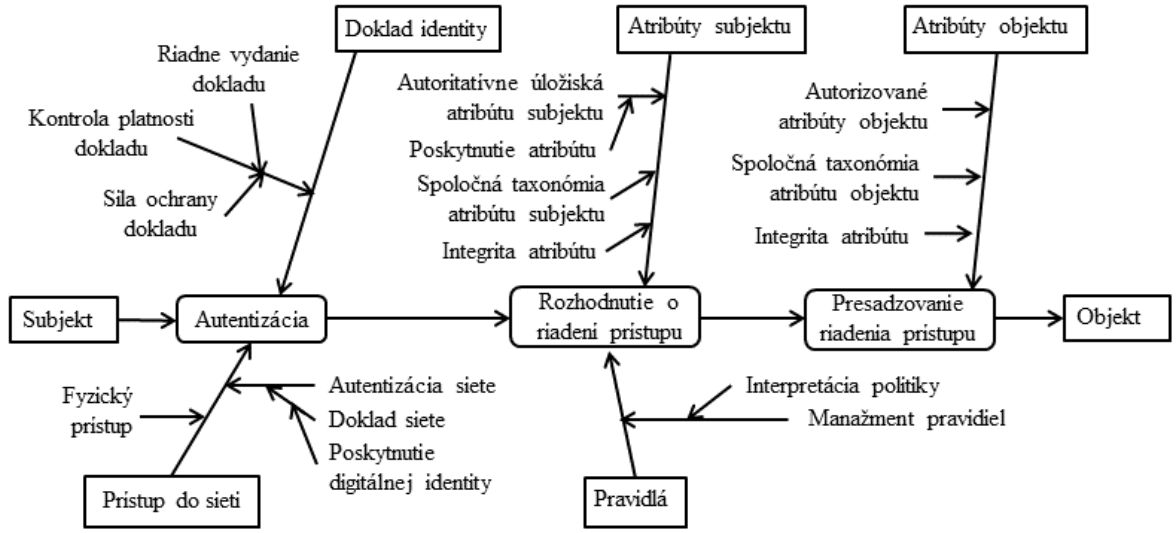
Scenár ABAC

Obrázky 7.19 a 7.20 sú prevzaté z aktualizovaného dokumentu [6] a poskytujú užitočný spôsob uchopenia rozsahu modelu ABAC v porovnaní s modelom DAC využívajúcim zoznamy riadenia prístupu (ACL). Toto porovnanie ilustruje nielen relatívnu zložitosť oboch modelov, ale tiež objasňuje požiadavky na dôveru v oboch modeloch. Porovnanie reprezentatívnych vzťahov dôvery (označených spojnicami so šípkami) pre použitie ACL a pre použitie ABAC ukazuje, že existuje omnoho viac zložitejších vzťahov dôvery, ktoré sú potrebné pre správne fungovanie systému ABAC. Ignorovaním spoločných znakov v oboch uvedených obrázkov je možné pozorovať, že v ACL je koreň dôveryhodnosti vlastník objektu, ktorý v konečnom dôsledku vynucuje pravidlá prístupu k objektu poskytnutím prístupu k objektu prostredníctvom pridania používateľa do zoznamu ACL. V systéme ABAC je koreň dôveryhodnosti odvodený z mnohých zdrojov, nad ktorými vlastník objektu nemá žiadnu kontrolu, ako napríklad autorita atribútov subjeku, tvorcovia politiky a vydavatelia dokladov. V súlade s tým dokument [6] odporučil, aby bol vytvorený riadiaci útvar organizácie, ktorý bude riadiť všetky nasadenia a prevádzku riadenia identity, dokladov a manažment spôsobilostí prístupu a aby každá podriadená organizácia (v prípade rozsiahleho podniku) mala podobný orgán na zabezpečenie konzistentnosti pri manažmente nasadenia a zmeny paradigmy súvisiacej s implmentáciou ABAC v organizácii. Okrem toho sa odporúča, aby organizácia vytvorila model dôvery, ktorý možno použiť na ilustráciu vzťahov dôvery a na pomoc pri určovaní vlastníctva a zodpovednosti za informácie a služby, potreby dodatočnej politiky a riadenia a požiadaviek na technické riešenia na potvrdenie alebo presadzovanie vzťahov dôvery.

Model dôvery sa môže použiť na ovplyvnenie organizácií, aby sa podelili o svoje informácie s jasnými očakávaniami o tom, ako sa tieto informácie budú používať a chrániť, a aby boli schopní dôverovať informáciám a atribútovým a autorizačným tvrdeniam pochádzajúcich z iných organizácií.



Obr. 7.19: Reťaz dôvery pre ACL.



Obr. 7.20: Reťaz dôvery pre ABAC.

Literatúra

[1] D. E. Bell a L. J. LaPadula. *Computer security model: Unified exposition and multics interpretation*. Technical Report ESD-TR-76-372, MTR-3153. The MITRE Corporation, Bedford, MA, jún 1975. URL: https://csrc.nist.gov/csrc/media/

publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/bell76.pdf (citované na strane 142).

[2] K. Biba. *Integrity consideration for secure computer systems*. Technical Report ESD-TR-76-372, MTR-3153. The MITRE Corporation, Bedford, MA, apr. 1977. URL: https://ban.ai/multics/doc/a039324.pdf (citované na strane 146).

[3] D. F. C. Brewer a M. J. Nash. „The Chinese Wall security policy“. Publik.: *Proceedings of the 1989 IEEE Symposium on Security and Privacy*. IEEE Computer Society. 1989, s. 206–214. URL: http://www.facweb.iitkgp.ac.in/~shamik/spring2015/i&ss/papers/the%20Chinese%20wall%20security%20policy.pdf (citované na strane 154).

[4] C. S. S. Centre. *The Canadian Trusted Computer Product Evaluation Criteria. Version 3.0e*. Jan. 1993 (citované na strane 146).

[5] I. F. Cruz, R. Gjomemo, B. Lin a M. Orsini. „A Constraint and Attribute Based Security Framework for Dynamic Role Assignment in Collaborative Environments“. Publik.: *Collaborative Computing: Networking, Applications and Worksharing, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 10*. Springer. 2009, s. 322–329. URL: https://doi.org/10.1007/978-3-642-03354-4_24 (citované na strane 158).

[6] V. C. Hu, D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller a K. Scarfone. *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*. NIST SP 800-162 (aktualizácia k 8.2.2019). National Institute of Standards and Technology (NIST), jan. 2014. URL: https://doi.org/10.6028/NIST.SP.800-162 (citované na stranách: 158, 160).

[7] C. Paulsen a R. Byers. *Glossary of Key Information Security Terms*. NIST IR 7298 Rev. 3. National Institute of Standards and Technology (NIST), júl 2019. URL: https://doi.org/10.6028/NIST.IR.7298r3 (citované na stranách: 132, 133).

[8] R. Ross, V. Pillitteri, K. Dempsey, M. Riddle a G. Guissanie. *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*. NIST SP 800-171 Rev. 2. National Institute of Standards and Technology (NIST), feb. 2020. URL: https://doi.org/10.6028/NIST.SP.800-171r2 (citované na strane 126).

[9] P. Samarati a S. de Capitani di Vimercati. „Access Control: Policies, Models, and Mechanisms“. Publik.: *R. Focardi and R. Gorrieri (Eds.): FOSAD 2000, LNCS 2171*. Springer. 2001, s. 137–196. URL: http://spdp.di.unimi.it/papers/sam-fosad.pdf (citované na stranách: 134, 141).

[10] R. S. Sandhu, E. J. Coynek, H. L. Feinsteink a C. E. Youmank. „Role-Based Access Control Models“. Publik.: *IEEE Computer* 29 (feb. 1996), s. 38–47. URL: https://profsandhu.com/journals/computer/i94rbac(org).pdf (citované na strane 147).

[11] R. S. Sandhu, D. Ferraiolo a R. Kuhn. „The NIST model for role-based access control: towards a unified standard“. Publik.: *ACM workshop on Role-based access control 2000*. ACM. 2000, s. 47–63. URL: https://web2.utc.edu/~Li-Yang/cpsc4660/rbac-00.pdf (citované na strane 147).

[12] R. S. Sandhu a P. Samarati. „Access Control: Principles and Practice“. Publik.: *IEEE Communications Magazine* 32 (sept. 1994), s. 40–48. URL: https://www.profsandhu.com/cs5323_s18/SS-1994.pdf (citované na strane 133).

[13] L. Wang, D. Wijesekera a S. Jajodia. „A Logic-based Framework for Attribute Based Access Control“. Publik.: *Proceedings of the 2004 ACM workshop on Formal Methods in Security Engineering, FMSE '04*. ACM. 2004, s. 45–55. URL: https://doi.org/10.1145/1029133.1029140 (citované na strane 158).

[14] E. Yuan a J. Tong. „Attributed Based Access Control (ABAC) for Web Services“. Publik.: *Proceedings of the 2005 IEEE International Conference on Web Services, ICWS 2005*. IEEE Computer Society. 2005, s. 561–569. URL: https://doi.org/10.1109/ICWS.2005.25 (citované na strane 158).

Kapitola 8

Siete, Internet a telekomunikácie

Ladislav Hudec

8.1 Úvod

Táto kapitola učebných textov sa venuje bezpečnosti počítačových sietí a Internetu. Pokiaľ boli počítače samostojace zariadenia bez pripojenia do iných systémov, bolo možné ich bezpečnosť zaistiť najmä prostriedkami fyzickej bezpečnosti, prípadne antivírusovými nástrojmi na kontrolu používaných externých pamäťových médií (napríklad pružný disk). Snaha o spoločné využívanie najmä drahších zariadení (napríklad farebná tlačiareň) doviedla návrhárov počítačov k potrebe vytvorenia možnosti komunikácie medzi jednotlivými samostojacimi počítačmi a k vytvoreniu počítačových sietí. Pripojenie jednotlivých počítačov do zostavy počítačovej siete prinieslo samozrejme ďalšie a nové bezpečnostné problémy. Rozľahlosť dnešných počítačových sietí možno nájsť v mierke od počítačovej siete v rámci jednej kancelárie alebo budovy až po svetovú počítačovú sieť vytvorenú s podporou telekomunikačných zariadení prakticky po celom svete. A práve táto rozľahlosť počítačových sietí a Internetu predstavuje zvýšené možnosti pre škodlivé aktivity, pretože ponúka veľa miest prístupu do sieti.

Tématicky možno túto kapitolu rozdeliť na päť častí. Tieto časti pokrývajú relevantné oblasti bezpečnosti v počítačových sieťach a v Internete. V prvej časti sú vysvetlené základné vlastnosti systému doménových mien (DNS) a príklady útokov na tento systém. DNS predstavuje základný stavebný kameň počítačových sietí a Internetu, pretože bez neho nebudú fungovať alebo fungovať iba s ťažkosťami najpoužívanejšie sieťové služby ako je elektronická pošta a webové servery (systémy www). Druhá časť je venovaná opisu elektronickej pošty. Od základnej funkcionality, kedy správy elektronickej pošty mohli byť iba obyčajné texty napísané v kóde US-ASCII, cez vylepšenú verziu MIME až po bezpečnú verziu S/MIME. V tretej časti je opísaný protokol HTTP. Tento protokol je asi najviac používaným aplikačným protokolom v Internete, pretože okrem iného zabezpečuje komunikáciu klienta do sídel celosvetovej pavučiny www. Štvrtá časť je venovaná vysvetleniu základných koncepcií virtuálnych privátnych sietí. Koncept VPN je dôležitý pri bezpečnom a cenovo efektívnom pripájaní klienta k počítačovej sieti organizácie, pri vzdialenom prístupe k vybratým prostriedkom počítačovej sieti organizácie ako aj pri prepájaní intranetov geograficky vzdialených súčastí jednej organizácie. V poslednej piatej časti sú opísané princípy fungovania nástrojov na detekciu alebo prevenciu pred prienikmi IDPS do počítačovej sieti. Či sa už jedná o pevnú sieť alebo bezdrôtovú sieť. Sú analyzované detekčné vlastnosti a možnosti nástrojov IDPS takisto ako ich umiestnenie v

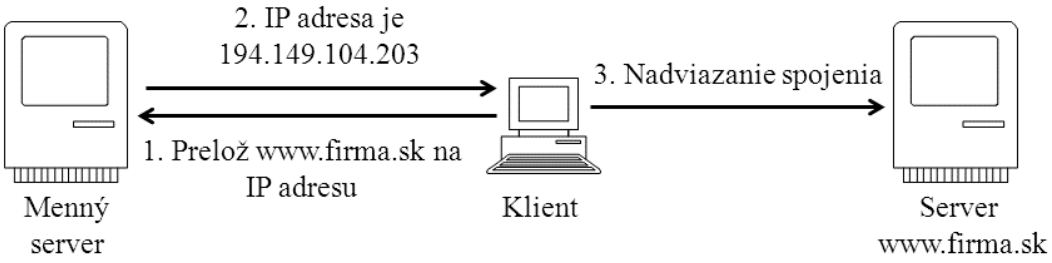
štruktúre sieti. Za každou časťou učebných textov sú uvedené zdroje, z ktorých čerpal autor a ktoré si môže čitateľ prípadne preštudovať. Autor si nekladie za cieľ vyčerpávajúcim spôsobom opísať všetky aspekty vybratých tém bezpečnosti počítačových sietí a Internetu. Orientuje sa na výklad základných princípov, ktoré vychádzajú najmä z iniciálnych dokumentov RFC (Request For Comments) pracovných skupín IETF (Internet Engineering Task Force) v daných oblastiach.

Výber tém ako aj študijný text je napísaný tak, že predpokladá znalosti zo sieťových technológií aspoň na úrovni základných univerzitných kurzov sieťových technológií, prípadne znalostí základných kurzov CCNA (Cisco Certified Network Associate) spoločnosti CISCO.

8.2 Systém DNS

Smerovanie komunikácie v počítačových sieťach medzi dvomi koncovými počítačmi sa vykonáva na základe adries IP. Ináč povedané, komunikujúce koncové uzly sa identifikujú adresami IP. Číselné vyjadrenie adresy IP je pre človeka obtiažne na zapamätanie a navyše adresa IP toho istého sieťového rozhrania počítača sa môže občas aj zmeniť. Preto sa namiesto adresy IP sieťového rozhrania zavádza meno sieťového rozhrania. Pre každú adresu IP máme teda zavedené meno sieťového rozhrania (počítača), presnejšie povedané **doménové meno** (domain name). Toto doménové meno môžeme používať namiesto adresy IP okrem identifikácie samotného **menného servera** (name server), kde sa musí použiť IP adresa. Treba ešte poznamenať, že jedna IP adresa môže mať priradených aj niekoľko doménových mien.

Meno sieťového rozhrania počítača a jemu pridelaná adresa IP je definovaná v databáze DNS (Domain Name System). DNS je celosvetovo distribuovaná databáza. Jednotlivé časti tejto databáze sú umiestnené na tzv. **name (menných) serveroch**. Základná koncepcia systému DNS je špecifikovaná v dokumentoch [34] a [35] iniciatívnej skupiny IETF (Internet Engineering Task Force, iniciatívna skupina tvorby internetových štandardov RFC). Princíp činnosti systému DNS je na Obrázku 8.1.



Obr. 8.1: Princíp činnosti systému DNS

8.2.1 Domény, subdomény a zóny

Prostriedky Internetu sú rozdelené do tzv. **domén**. Koncepciu vytvárania domén možno demonštrovať na príklade veľkej organizácie, ktorá je registrovaná na Slovensku. Na čele organizácie je generálny riaditeľ. Pretože však on nemôže robiť všetko, bude organizácia pravdepodobne rozdelená na sekcie. Každá sekcia má určitú obmedzenú autonómiu. Riaditeľ sekcie má právomoc urobiť priame rozhodnutie bez toho, aby si pýtal povolenie od generálneho riaditeľa.

Podobne riaditeľ sekcie nemôže robiť v sekcii všetko, bude sekcia pravdepodobne rozdelená na odbory. Každý odbor má určitú obmedzenú autonómiu. Riaditeľ odboru má právomoc urobiť priame rozhodnutie bez toho, aby si pýtal povolenie od riaditeľa sekcie.

Doménové mená sú tvorené podobným spôsobom a budú často odrážať hierarchické delegovanie právomocí. Uvažujme napríklad meno:

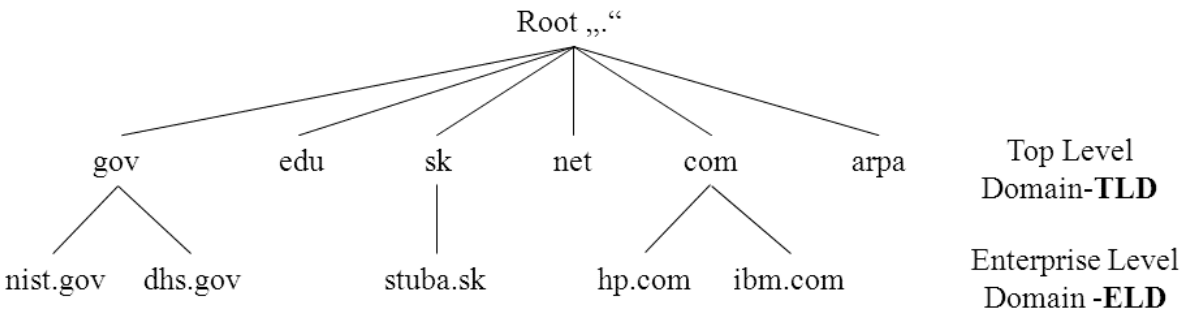
mojpocitac.mojeoddelenie.mojodbor.mojasekcia.mojaorganizacia.sk.

V tomto príklade vieme, že existuje jedno meno uzla mojpocitac, ktorý sa nachádza v subdoméne mojeoddelenie.mojodbor.mojasekcia.mojaorganizacia.sk. Subdoména

mojeoddelenie.mojodbor.mojasekcia.mojaorganizacia.sk

je jednou sudbdoménou domény mojodbor.mojasekcia.mojaorganizacia.sk, atď. Nakoniec je subdoména mojaorganizacia.sk jedna zo subdomén domény sk.

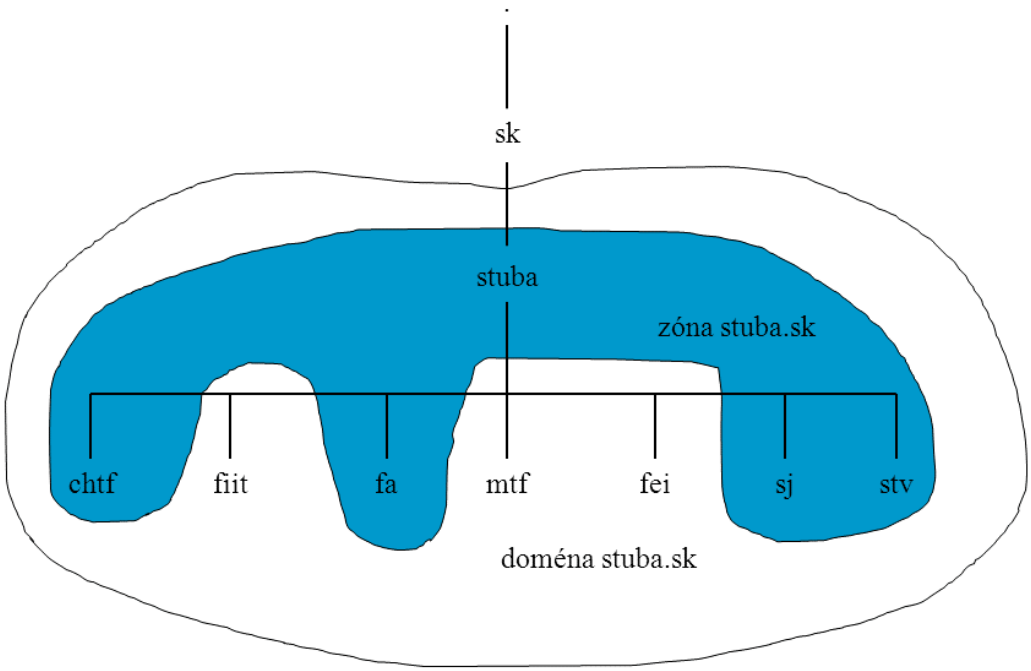
Keby sme chceli zovšeobecniť vyššie uvedený príklad, tak môžeme povedať, že meno domény sa uvádza v bodkovej notáci a má všeobecnú syntax: **reťazec. reťazec. reťazec.... reťazec.**, kde prvý reťazec je meno počítača (rozhrania), ďalší reťazec je meno najnižšej vnorenej domény, ďalší vyššej domény atď. Pre jednoznačnosť sa na konci uvádza tiež bodka, vyjadrujúca **koreňovú doménu** (root domain).



Obr. 8.2: Hierarchické usporiadanie domén

Na Obrázku 8.2 je naznačené hierarchické usporiadanie domén. V koreni stromu je koreňová doména. Požiadavky na jej prevádzku sú špecifikovaná v [4]. Subdomény koreňovej domény, tiež nazývané **domény najvyššej úrovni** (TLD – Top Level Domain), sú dvojakého typu. Jednak sú to **domény štátov** ako je napríklad Slovenská republika (meno domény sk), Česká republika (meno domény cz). Mená domén štátov sú dvojpísmenové podľa medzinárodných kódov štátov v zmysle normy [23]. Potom sú to tak zvané **generické domény**. Tieto domény boli zavedené v počiatkoch Internetu a zachovali sa doposiaľ. Príkladom generickej domény je americká vládna doména (meno domény gov) alebo doména vzdelávacích inštitúcií (meno domény edu). Domény štátov sú spravované národnými autoritami a registráciu domén druhej úrovni, tiež nazývané aj **domény podnikovej úrovne** (ELD – Enterprise Level Domain), zabezpečujú tieto národné autority. Domény druhej úrovne si väčšinou spravujú na svojich menných serveroch majitelia domény alebo ich poskytovatelia internetových služieb. Údaje pre

doménu druhej úrovne napr. [stuba.sk] nie sú na rovnakom name serveri ako doména sk. Sú rozložené na mnoho menných serverov. Údaje o doméne uložené na jednom mennom serveri sú nazývané **zónou** (zone file). Zóna teda obsahuje iba časť domény. Zóna je časť priestoru mien, ktorú obhospodaruje jeden menný server.



Obr. 8.3: Zóna stuba.sk

Na Obrázku 8.3 je znázornené, ako môže byť (hypoteticky) v doméne stuba.sk decentralizovaná kompetencia (delegovanie) na nižšie správne celky. Takže doména **stuba.sk** obsahuje v sebe všetky subdomény, ale zóna stuba.sk delegovala na iné menné servery právomoci na zóny **fiit.stuba.sk**, **mtf.stuba.sk** a **fei.stuba.sk**. Takže zóna stuba.sk obsahuje doménu stuba.sk až na tri uvedené výnimky. Ďalšie podrobnosti možno nájsť v [37, 39, 50].

8.2.2 Preklad mena domény

Proces prekladu (rezolvencie) mena domény na adresu IP možno zhrnúť do týchto krokov:

1. Používateľský program zadá požiadavku operačnému systému (komponentu s názvom resolver) na preklad mena domény na adresu IP (prípadne preklad adresy IP na meno domény).

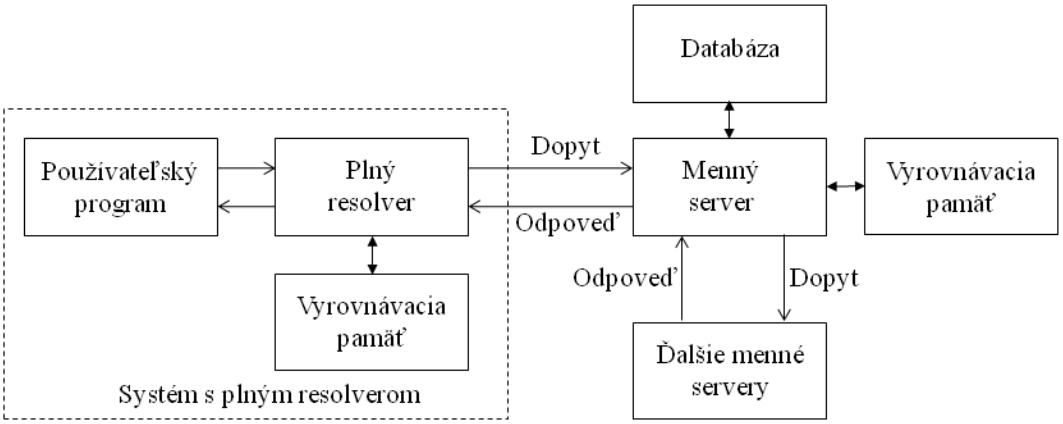
2. Resolver sformuluje dopyt na menný server. Plnohodnotný (full) resolver má vyrovnávaciu pamäť (pamäť cache), do ktorej ukladá výsledky predošlých dopytov na menný server. Zistí, či vo vyrovnávacej pamäti má odpoveď na zadaný dopyt. Ak áno, odpoveď uloženú v cache použije. Pahýľový (stub) resolver vyrovnávaciu pamäť nemá.

3. Menný server skontroluje, či sa odpoveď na dopyt resolvera nachádza v jeho lokálnej autoritatívnej databáze (databáza obsahuje autoritatívne - nespochybniteľné údaje) alebo

vo vyrovnávacej pamäti, a ak áno, potom vráti resolveru túto odpoveď. Ak nie, potom sa menný server dopytuje ďalších dostupných menných serverov, počnúc koreňom stromu DNS smerom nadol alebo tak vysoko v strome ako je to možné.

4. Používateľský program nakoniec dostane odpovedajúcu adresu IP (alebo meno domény) alebo chybovú správu v prípade, že na dopyt sa nedá odpovedať. Štandardne sa programu neposiela zoznam menných serverov, ktorí sa podieľali na preklade.

Preklad mena domény je proces klient/server. Funkcia klienta (nazvaná resolver alebo menný resolver) je pre používateľa transparentná a je volaná aplikáciou na preklad symbolických vysoko úrovňových mien na reálne adresy IP (alebo naopak). Menný server (označovaný aj doménový menný server) je serverová aplikácia zabezpečujúca preklad medzi vysoko úrovňovými menami počítačov a adresami IP. Správy dopytu a odpovede pri komunikácii resolvera s menným serverom a medzi mennými servermi sú prenášané protokolom TCP alebo UDP.

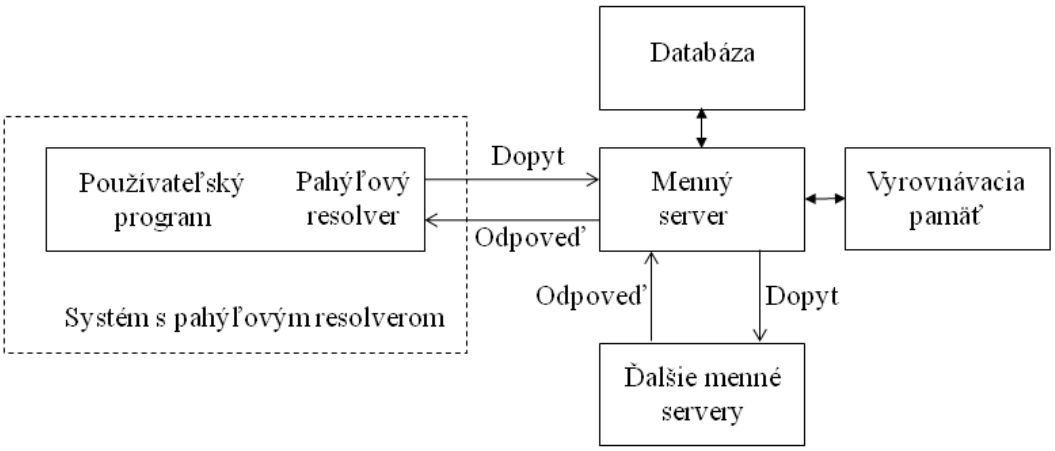


Obr. 8.4: Použitie plného resolvera na preklad mena domény

Na Obrázku 8.4 je znázornený princíp funkcie programu operačného systému s plným resolverom. Používateľský program žiada plný resolver o preklad a ten potom (ak nemá odpoveď vo svojej vyrovnávacej pamäti) prípadne ďalej žiada menný server o preklad. Odpovede na dopyty plný resolver odovzdá používateľskému programu a tiež si odpoveď uloží do vyrovnávacej pamäti pre budúce použitie.

Na Obrázku 8.5 je znázornený princíp funkcie programu operačného systému s pahýľovým resolverom. Pahýľový resolver je rutina nalinkovaná s používateľským programom a postupuje dopyty mennému serveru na preklad. Odpovede na dopyty si ukladá menný server do cache (a nie pahýľový resolver). Na väčšine platforiem je pahýľový resolver implementovaný knižničnými rutinami a tento typ resolvera sa vyskytuje oveľa viac ako plný resolver.

Dopyty na meno domény môžu byť dvojakého typu a to **rekurzívne** alebo **iteratívne**. Príznak v dopyte na meno domény indikuje, či si klient požaduje rekurzívny dopyt a príznakový bit v odpovedi určuje, či server podporuje rekurzívne dopyty. Rozdiel medzi rekurzívnym a iteratívnym dopytom sa ukáže v prípade, keď menný server dostane žiadosť, na ktorú nemôže úplnú odpoveď poskytnúť sám. Rekurzívny dopyt požaduje, aby server sám vydal dopyt na zistenie požadovaných informácií a vrátil klientovi úplnú odpoveď. Iteratívny dopyt znamená,



Obr. 8.5: Použitie pahýľového resolvera na preklad mena domény

že menný server vráti klientovi také informácie, ktoré má k dispozícii, a klientovi vráti tiež zoznam ďalších serverov, ktoré by mal klient kontaktovať na skompletizovanie dopytu.

Odpovede na meno domény môže byť dvojakého typu a to **autoritatívne** alebo **neautoritatívne**. Príznakový bit v odpovedi indikuje o aký typ odpovedi ide. Keď menný server dostane dopyt pre doménu v zóne, nad ktorou má oprávnenia (autoritu), menný server vráti všetky požadované informácie v odpovedi s nastaveným príznakom **autoritatívna odpoveď**. Keď obdrží dopyt pre doménu, nad ktorou nemá oprávnenia (autoritu), jeho akcie sú závislé na nastavení príznaku požiadavky rekurzie v dopyte:

- Keď príznakový bit požiadavky rekurzie je nastavený a server podporuje rekurzívne dopyty, server bude smerovať svoj dopyt na ďalší menný server. Bude to buď autoritatívny menný server pre doménu špecifikovanú v dopyte alebo to bude jeden z koreňových menných serverov. V prípade, že druhý server nevráti autoritatívnu odpoveď (napríklad, ak delegoval autoritu na iný server), proces sa opakuje.
- Keď server (alebo program plného resolvera) dostane odpoveď, odpoveď uloží do vyrovnávacej pamäti z dôvodu zlepšenie priepustnosti pre opakované dopyty. Odpoveď je vo vyrovnávacej pamäti uložená na pôvodcom odpovede určenú maximálnu dobu, ktorá je obsiahnutá v 32 bitovom poli odpovede s názvom TTL (Time To Live). Typická hodnota TTL je 86400 sekúnd (jeden deň).
- Keď príznakový bit požiadavky rekurzie nie je nastavený alebo server nepodporuje rekurzívne dopyty, server vráti akékoľvek informácie (relevantné dopytu) zo svojej vyrovnávacej pamäti a tiež vráti zoznam ďalších menných serverov, ktoré musia byť kontaktované pre autoritatívne informácie.

Menný server nemusí mať autoritu nad žiadnou zónou, ale môže mať autoritu nad jednou alebo viacerými zónami. V zásade je možné vyčleniť tri typy menných serverov:

- **Primárny** menný server. Tento server načíta informácie o zóne z disku a má autoritu nad zónou.

- **Sekundárny** menný server. Tento menný server má autoritu nad zónou, ale získava informácie o zóne od primárneho servera prostredníctvom procesu zónového prenosu (zone transfer). Aby boli informácie o zóne na primárnom a sekundárnom serveri synchronizované, sekundárny server žiada pravidelne o zónový prenos (spravidla raz za niekoľko hodín) a primárny server aktivuje zónový prenos v prípade aktualizácie informácií o zóne. Menný server môže fungovať buď ako primárny alebo sekundárny nmenný server pre viac domén alebo ako primárny pre niektoré domény a ako sekundárny pre ostatné. Primárny alebo sekundárny menný server plní všetky funkcie caching – only menného servera (takýto menný server má iba vyrovnávajúcu pamäť).

- **Caching – only** menný server. Tento server nemá autoritu nad žiadnou zónou. Všetky údaje získava podľa potreby od primárnych alebo sekundárnych menných serverov. To si vyžaduje, aby obsahoval aspoň jeden záznam NS (záznam o mennom serveri), ktorý ho odkazuje na menný server, z ktorého môže iniciálne získať informácie.

8.2.3 Zdrojové záznamy DNS

Distribuovaná databáza DNS sa skladá zo záznamov, ktorým hovoríme **zdrojové záznamy RR** (Resource Record). Základné typy zdrojových záznamov sú definované v [35], niektoré ďalšie nové v [9]. Tieto záznamy sú rozdelené do tried. Nás bude zaujímať iba trieda internetových záznamov. Zdrojové záznamy zabezpečujú mapovanie medzi menami domén a sieťovými objektami. Najbežnejšie sieťové objekty sú adresy internetových uzlov (hostov), ale systém DNS je navrhnutý tak, aby obsiahol široký rozsah rôznych objektov.

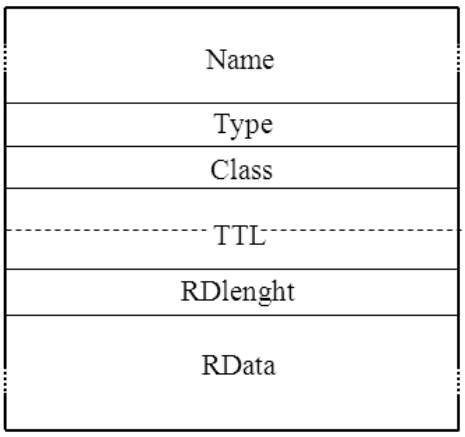
Zóna sa skladá zo skupiny zdrojových záznamov začínajúci záznamom SOA (Start Of Authority). Záznam SOA identifikuje doménové meno zóny. Bude sa tam nachádzať záznam o mennom serveri NS (Name Server) pre primárny menný server pre túto zónu. Tiež by sa tam mohli nachádzať záznamy NS pre sekundárne menné servery. Záznamy NS sa využívajú na identifikáciu autoritatívnych menných serverov.

Na Obrázku 8.6 je všeobecný formát zdrojového záznamu. Jednotlivé polia vo formáte majú tento význam:

- **Name** je pole pre meno domény. Meno domény musí byť definované. Aj keď systém DNS má veľmi všeobecné pravidlá na vytvorenie doménových mien odporúča syntax pre doménové mená tak, aby minimalizovala pravdepodobnosť chybnej interpretácie doménových mien aplikáciami, ktoré používajú resolver DNS. Doménové meno rešpektujúce odporúčanú syntax by sa malo skladať z postupnosti reťazcov, ktoré pozostávajú z alfanumerických znakov alebo pomlčky, pričom každý reťazec má dĺžku 1 až 63 znakov začínajúc písmenom. Každý pár reťazcov je oddelený bodkou. Doménové mená nie sú citlivé na veľkosť písmen.

- **Type** definuje typ zdroja v tomto zázname. Existuje viacero možných hodnôt, ale niektoré z nich sú bežnejšie používané. Napríklad typ A (hodnota 1) predstavuje adresu IPv4 hosta, typ NS (2) je autoritatívny manný server, typ CNAME (5) je kanonické meno pre alias, typ SOA (6) je označenie začiatku zóny autority, typ KEY (25) je verejný kľúč zviazaný s menom DNS, typ AAAA (28) je záznam adresy IPv6, atď.

- **Class** je označenie triedy rodinu protokolu. Jedinou bežne používanou hodnotou je IN (Internet systém).
- **TTL** (Time To Live) je čas v sekundách, počas ktorého je platný zdrojový záznam vo vyrovnávacej pamäti menného servera. Tento čas je uložený ako 32-bitové číslo bez znamienka. Typická hodnota pre záznamy ukazujúce na adresy IP je 86400 (jeden deň).
- **RDlength** je celé 16-bitové číslo bez znamienka, ktoré špecifikuje v počte bajtov dĺžku poľa RData.
- **RData** je reťazec bajtov s premenlivou dĺžkou, ktorý opisuje zdroj. Formát týchto informácií sa líši podľa typu a triedy zdrojového záznamu.



Obr. 8.6: Všeobecný formát zdrojového záznamu

8.2.4 Správy DNS

Všetky správy v protokole DNS používajú jeden formát. Tento formát je zobrazený na Obrázku 8.7. Správu v tomto formáte posiela resolver mennému serveru. Resolver z tohto formátu využíva iba hlavičku správy (polia IDentification, Parameters, QDcount, ANcount, NScount, ARcount) a sekciu otázky (Question Section). Odpovede a odovzdávanie dopytu využívajú ten istý formát a s tým, že doplňujú sekciu odpovedi, sekciu autority a sekciu ďalších informácií (Answer Section, Authority Section a Additional Information Section).

Hlavička správy má pevnú dĺžku 12 bajtov. Dĺžky ostatných sekcií formátu správy sú premenlivé. Jednotlivé polia v hlavičke správy majú tento význam:

- **IDentification** (ID) je 16 bitové identifikačné číslo správy. Tento identifikátor je prekopírovaný do odpovedi na dopyt (párovanie dopytu a odpovedi) a môže byť použitý na rozpoznanie odpovedi pri viacerých dopytoch zadaných v rovnakom čase.
- **Parameters** je 16 bitové pole parametrov v takejto štruktúre:
  - Bit 0: príznak **QR** identifikuje dopyt (príznak nastavený na 1) alebo odpoveď (príznak nastavený na 0)

  - Bity 1-4: príznak **Op code** je 4 bitové pole špecifikujúce typ dopytu: 0 je štandardný dopyt (QUERY), 1 je inverzný dopyt (IQUERY), 2 je žiadosť o stav servera (STATUS)
  - Bit 5: príznak **AA** je príznak autoritatívnej odpovedi. Ak je nastavený v odpovedi na 1, potom špecifikuje, že odpovedajúci menný server je autoritou pre meno domény, ktorá bola poslaná v dopyte
  - Bit 6: príznak **TC** je príznak skrátenia odpovedi. Príznak je nastavený, ak správa bola dlhšia ako je dovolená dĺžka použitého transportného protokolu UDP.
  - Bit 7: príznak **RD**] je príznak požadujúci rekurziu. Tento bit signalizuje mennému serveru, že sa požaduje rekurzívny preklad. Príznak je prekopírovaný do odpovedi.
  - Bit 8: príznak **RA** je príznak dostupnosti rekurzie. Príznak indikuje, či menný server podporuje rekurzívny preklad.
  - Bity 9-11: pole **ZERO** - 3 bity rezervované pre budúce použitie, musia byť nastavené na 0
  - Bity 12-15: pole **Rcode** - 4 bitový kód odpovede. Možné hodnoty tohto poľa sú 0 pre bezchybnú operáciu, 1 pre chybu formátu (server nebol schopný interpretovať správu), 2 pre poruchu servera (správa nebola spracovaná z dôvodov problémov servera), 3 pre chybu mena (meno domény v dopyte neexistuje, toto platí iba pri nastavenom príznaku AA v odpovedi), 4 pre nie je implementované (požadovaný typ dopytu nie je na mennom serveri implementovaný), 5 pre odmietnutie (server odmieta odpovedať z dôvodov nastavenej politiky)

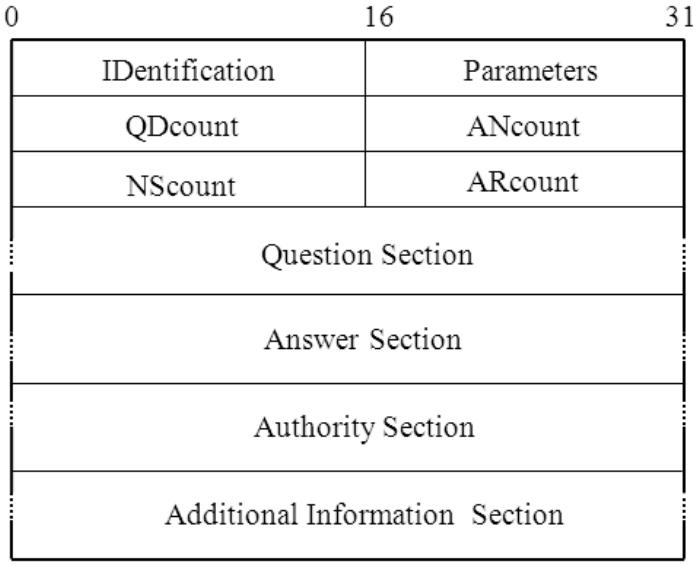
- **QDcount** – 16 bitové celé číslo bez znamienka definujúce počet položiek v sekcii otázky
- **ANcount** – 16 bitové celé číslo bez znamienka definujúce počet zdrojových záznamov v sekcii odpovedi
- **NScount** – 16 bitové celé číslo bez znamienka definujúce počet zdrojových záznamov s mennými servermi v sekcii autority
- **ARcount** – 16 bitové celé číslo bez znamienka definujúce počet zdrojových záznamov v sekcii dodatočných informácií

Pole sekcie otázok (Question Section) vo formáte správy DNS obsahuje dopyty pre menný server, obsahuje QDcount (zvyčajne 1) položiek. Ďalšie tri polia sekcií odpovede, autority a ďalších informácií (Answer Section, Authority Section a Additional Information Section) obsahujú premenlivý počet zdrojových záznamov. Ich počet je definovaný v odpovedajúcich poliach klavičky správy.

8.2.5 Útoky na DNS – Man in the Middle

Analýzou základných útokov na systém DNS sa zaoberá štúdia [47] (Security Associates Institute). V nasedujúcich častiach sú uvedené niektoré z nich.

V prípade, že **útočník je schopný odchytávať komunikáciu medzi klientom a DNS serverom**, potom útočník vie tiež odchytávať dopyty klienta na preklad mena a poslať klientovi (namiesto DNS servera) falošnú odpoveď, ktorá mapuje meno domény na nesprávnu adresu IP.



Obr. 8.7: Formát správy DNS

Tento útok je založený na **súbehu odpovedí**, a to falošnej odpovedi od útočníka a odpovedi oprávneného DNS servera. Útočník musí na dopyt klienta na preklad mena odpovedať skorej ako odpovie oprávnený DNS server. Zdržanie odpovedi (ak je to nevyhnutné) oprávneného DNS servera je možné vykonať zaslatím viacerých dopytov na preklad (simulácia útoku DoS na DNS server) alebo požiadavkou klienta na rekurzívny dopyt.

Demonštrácia útoku je na Obrázku 8.8 a skladá sa z týchto krokov:

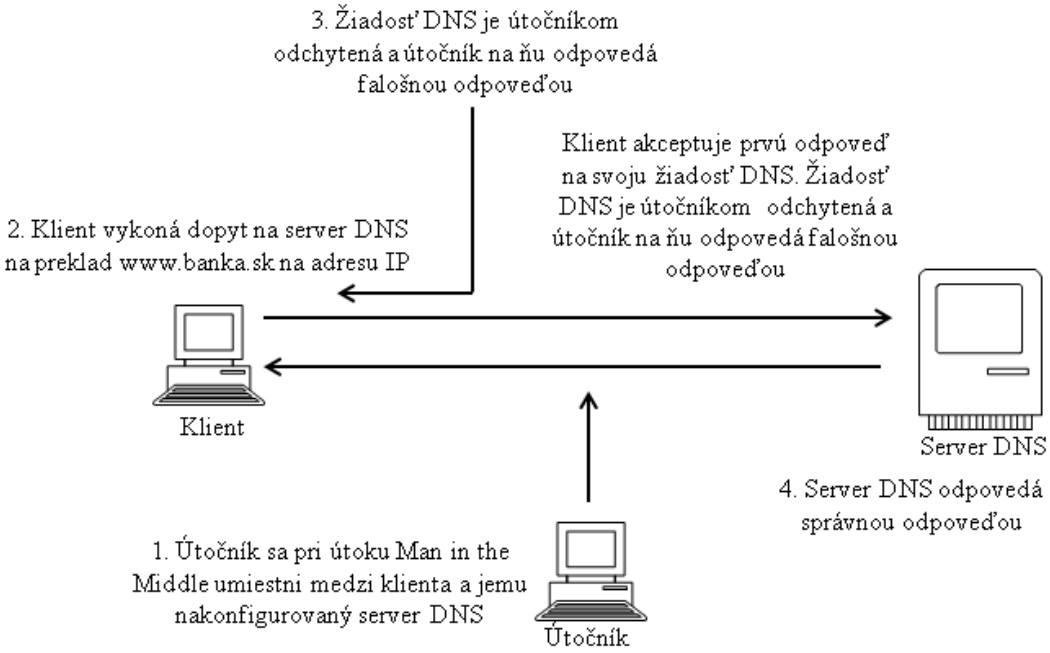
1. Útočník sa umiestni v štruktúre sieti medzi klienta a menný server (sieťová kolízna doména s klientom alebo na segment, kde je umiestnený menný server).
2. Klient vykoná dopyt DNS na preklad mena domény www.banka.sk.
3. Dopyt je odchytený útočníkom, ktorý odpovedá falošnou informáciou.
4. Server DNS odpovedá správnou informáciou, ale túto informáciu klient neakceptuje, pretože už dostal a akceptoval informáciu od útočníka.

Na realizáciu takéhoto útoku existujú voľne šíriteľné nástroje.

8.2.6 Útoky na DNS – cache poisoning

Ak klient v doméne **stuba.sk** vykoná dopyt na preklad mena domény **www.banka.sk**, typicky sa vykoná takáto sekvencia udalostí, ktoré sú dokumentované na Obrázku 8.9:

1. Klient kontaktuje jemu nakonfigurovaný DNS server a požiada ho o preklad mena domény www.banka.sk na adresu IP. Tento dopyt bude obsahovať informáciu o klientovom čísle zdrojového portu UDP, adrese IP a ID transakcie DNS.



Obr. 8.8: Útok na DNS typu Man in the Middle

2. Klientov DNS server, pretože nie je autoritatívnym pre doménu banka.sk, prostredníctvom dopytov cez Internetové koreňové servery DNS kontaktuje banka.sk server DNS a získa odpoveď na dopyt.

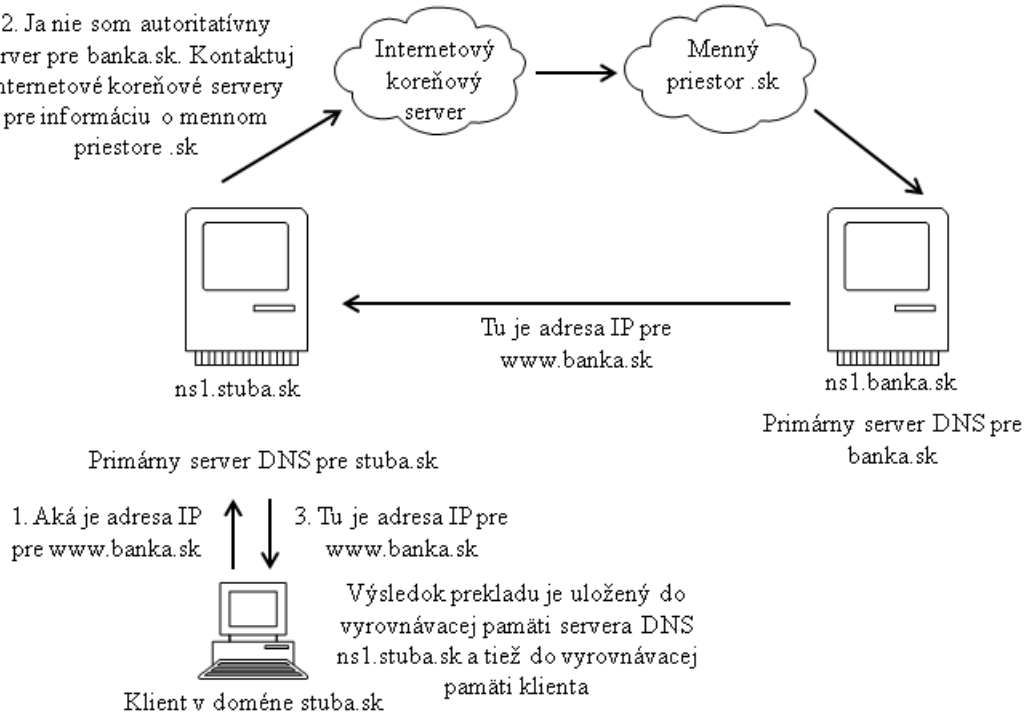
3. Tento úspešný dopyt potom DNS server pošle klientovi naspäť a aj server DNS aj klient si túto informáciu **uložia do vyrovnávacej pamäti**.

Na uvedenej sekvencii udalostí si treba všimnúť tieto skutočnosti:

1. V kroku 3 klient akceptuje iba takú spätnú odpoveď od servera DNS, v ktorej server DNS použije správne číslo zdrojového portu, adresy IP a ID transakcie tak ako boli použité pri dopyte v kroku 1. Tieto tri položky sú jedinou formou autentizácie použitej na akceptáciu odpovedí DNS.

2. Spätná odpoveď od servera DNS domény www.banka.sk je uložená do cache na serveri DNS ns1.stuba.sk a tiež do vyrovnávací pamäti na klientovi (v prípade plného resolvera) a to po dobu špecifikovanú parametrom TTL. Ak iný klient požiada server DNS ns1.stuba.sk o preklad doménového mena www.banka.sk počas platnosti tohto záznamu (daný TTL), potom server DNS na tento dopyt vráti informáciu zo svojej vyrovnávací úamäti a nebude posielať dopyty na iné menné servery (koreňový, .sk a ns1.banka.sk).

Je potrebné rozlišovať ID medzi transakciou medzi klientom a menným serverom a medzi transakciou medzi mannými servermi. V skutočnosti ide o dve rôzne transakcie DNS, teda **ID transakcií bude samozrejme rôzne**.



Obr. 8.9: Preklad mena domény na adresu IP

Vyššie uvedené kroky môžu byť útočníkom zneužité na umiestnenie falošnej informácie do vyrovnávací pamäti ns1.stuba.sk. Na Obrázku 8.10 sa útočník snaží správne uhádnuť ID transakcie (16 bitov) použitej pri komunikácii name serverov.

Aby to útočník dosiahol, urobí toto:

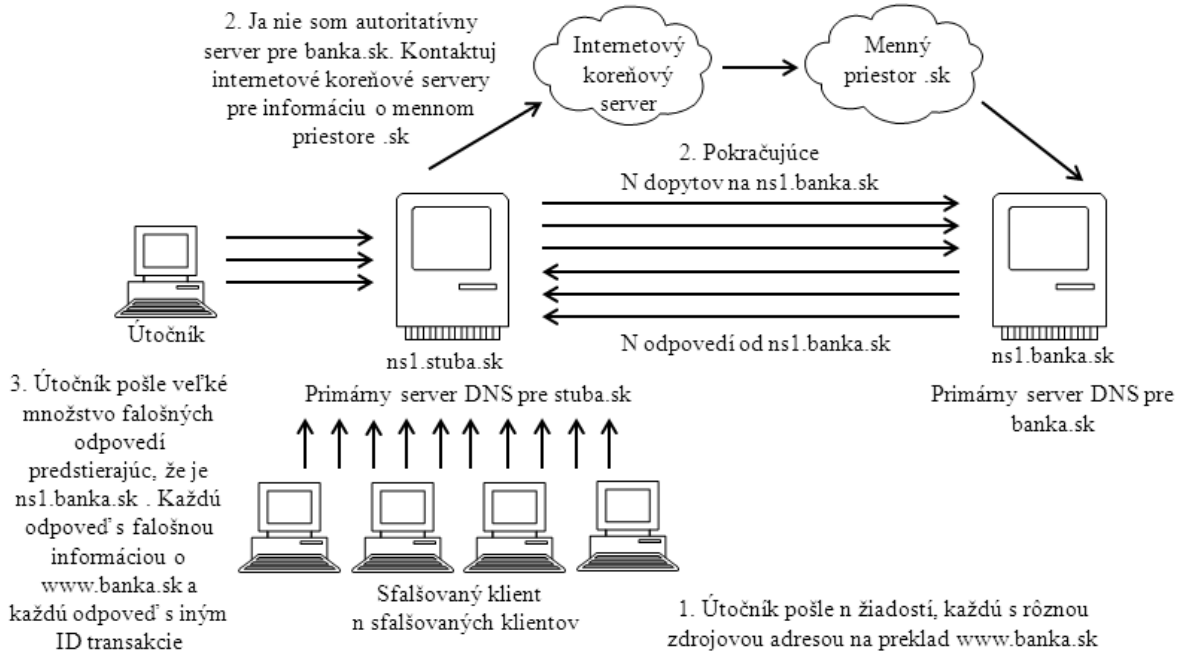
1. Pošle veľké množstvo žiadostí mennému serveru ns1.stuba.sk o preklad, každá žiadosť má inú falošnú zdrojovú adresu IP, mena domény www.stuba.sk na adresu IP. Dôvodom na poslatie veľkého počtu žiadostí je to, že každej žiadosti bude pridelené jedinečné ID transakcie a aj keď všetky žiadosti sú pre to isté meno domény, každá žiadosť bude spracovávaná nezávisle.

2. Menný server ns1.stuba.sk pošle každú z týchto žiadostí na ďalšie servery DNS a eventuálne ns1.banka.sk. To znamená, že menný server ns1.stuba.sk očakáva veľké množstvo odpovedí od menného servera ns1.banka.sk.

3. Útočník využije tento čakací interval na bombardovanie servera ns1.stuba.sk falošnými odpoveďami od servera ns1.banka.sk udávajúcimi, že doméne www.banka.sk odpovedá adresa IP, ktorá je pod kontrolou útočníka (falošná adresa, falošná infomácia). Každá falošná odpoveď má iné ID transakcie. Útočník dúfa, že uhádne správne ID transakcie, t.j. také ako bolo použité mennými servermi.

Ak je útočník úspešný, **bude falošná informácia** (falošná IP adresa) **uložená do varovnávacej pamäti servera DNS ns1.stuba.sk**. Treba poznamenať, že tento útok je viac menej

útokom na menný server, ktorý má dopad na klienta používajúceho cieľový menný server s falošnými informáciami.



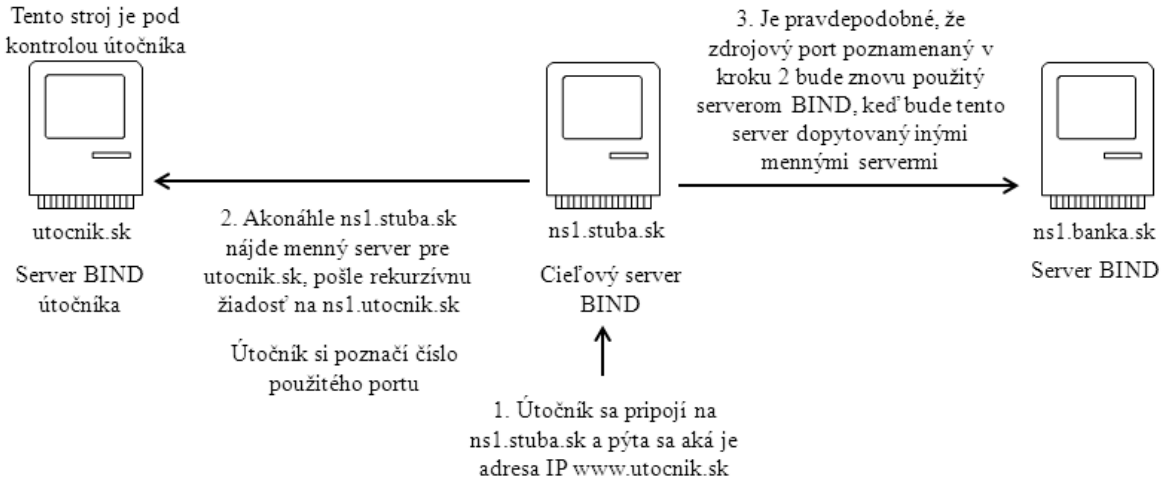
Obr. 8.10: Scenár útoku na DNS – cache poisoning

Teraz sa opäť vráťme k trom autentizačným položkám dopytu a odpovede, t.j. ID transakcie, zdrojovej adrese IP a číslu zdrojového portu. Zistenie zdrojovej adresy IP menného servera je priamočiare, pretože poznáme IP adresu menného servera, ktorému klient posiela dopyty. Zistenie **čísla zdrojového portu je obťažnejšie**.

Častejšie áno ako nie, softvér BIND (program omplementujúci DNS protokoly) **znovupoužíva to isté číslo zdrojového portu na dopyty toho istého klienta, t.j. menného servera BIND**. To znamená, že ak útočník má pod kontrolou nejaký BIND autoritatívny menný server (ns1.utocnik.sk), môže ako prvé zadať dopyt na cieľový menný server na preklad doménového mena z útočníkovej domény (napr. www.utocnik.sk) a keď príde paket s rekurzívnym dopytom na ns1.utocnik.sk, môže útočník zistiť číslo zdrojového portu na cieľovom mennom serveri. Je pravdepodobné, že bude použité to isté číslo zdrojového portu aj keď obeť pošle dopyty pre doménu, ktorá bude unesená (hijacked). Odchytávaním výstupov troch po sebe idúcich dopytov pre rôzne doménové mená bolo napríklad zistené:

- 172.16.1.2.22343 > 128.1.4.100.53
- 172.16.1.2.22343 > 23.55.3.56.53
- 172.16.1.2.22343 > 42.14.212.5.53

Pri dopytoch na tri rôzne menné servery všetky tri dopyty použili číslo zdrojového portu 22343. Zistenie číslo zdrojového portu je dokumentované na Obrázku 8.11.



Obr. 8.11: Zistenie čísla zdrojového portu na DNS BIND

BIND v4 a 8 používa sekvenčné prideľovanie ID pre transakcie. Zo znamená, že útočník môže ľahko nájsť aktuálne ID jednoducho vykonaním dopytu na server a zistením čísla ID a znalosťou, že nasledujúci dopyt BIND na ďalší name server sa vykoná s ID+1. BIND v9 prideľuje transakciám čísla ID náhodne a neposiela viacnásobné rekurzívne dopyty pre tie isté mená domén.

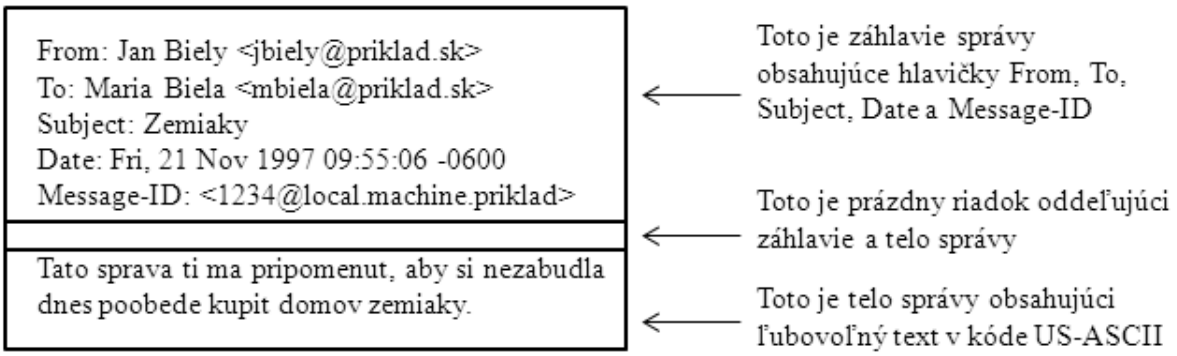
8.3 Bezpečná elektronická pošta

Prakticky vo všetkých distribuovaných prostrediach je elektronická pošta najviac používaná sieťová aplikácia. Používatelia očakávajú, že budú môcť odosielať správy elektronickej pošty iným používateľom, ktorí sú pripojení priamo alebo nepriamo k Internetu, bez ohľadu na typ operačného systému počítača alebo komunikačného vybavenia. S rastúcou dôležitosťou elektronickej pošty rastie aj požiadavka na jej **bezpečnosť** najmä na **autentickosť** a **dôvernosť** služieb elektronickej pošty.

Bezpečná elektronická pošta **S/MIME** (Secure/Multipurpose Internet Mail Extension) je bezpečnostné vylepšenie internetového štandardu formátu elektronickej pošty MIME. Vylepšenie je založené na využití technológie hašovacích funkcií a kryptografie. Hoci aj bezpečná pošta PGP (Pretty Good Privacy) je zaradená medzi štandardy IETF (Internet Engineering Task Force, iniciatívna skupina tvorby internetových štandardov RFC), je vysoko pravdepodobné, že S/MIME sa stane priemyselným štandardom pre obchodné a inštitucionálne použitie, zatiaľ čo PGP zostane voľbou pre osobné používanie bezpečnej elektronickej pošty mnohých používateľov. S/MIME je definovaná v rade dokumentov, najdôležitejšie sú [21, 22, 43, 44].

Aby sme porozumeli bezpečnej elektronickej pošte S/MIME, musíme mať najprv všeobecnú predstavu o základnom formáte správy elektronickej pošty **MIME**. Ale k pochopeniu významu MIME sa musíme vrátiť k tradičnému formátu správy elektronickej pošty definovanom v štandarde [5]. Formát e-mailu v tomto formáte sa ešte dnes bežne používa. Najnovšia verzia tejto tradičnej špecifikácii formátu je [45]. Preto sa najprv budeme zaoberať týmito dvomi štandardmi a až potom sa vrátime k formátu S/MIME.

Štandard [45] definuje formát textových správ, ktoré sú odosielané pomocou elektronickej pošty. V kontexte [45] je správa videná ako obálka a obsah. Obálka obsahuje akékoľvek informácie, ktoré je potrebné preniesť a doručiť. Obsah vytvára objekt, ktorý je doručený príjemcovi. Štandard [45] sa vzťahuje len na obsah. Avšak štandard pre obsah zahrňuje sadu hlavičiek, ktoré môže použiť poštový systém na vytvorenie obálky. Štandard je určený na uľahčenie získavania týchto informácií pomocou programov.



Obr. 8.12: Základná štruktúra správy elektronickej pošty

Celková štruktúra správy podľa [45] je veľmi jednoduchá. Správa sa skladá z určitého počtu riadkov záhlavia (header) a nasleduje neobmedzený text tela správy (body). Záhlavie je oddelené od tela prázdnym riadkom. Inak povedané, správa je text US-ASCII (7 bitový kód) a všetky riadky až do prvého prázdneho riadku sú považované za riadky záhlavia, ktoré využíva časť používateľského klienta poštového systému. Riadok záhlavia sa obvykle skladá z hlavičky, ktorá je nasledovaná dvojbodkou a ďalej nasledovaná argumentom hlavičky. Formát dovoľuje, aby bol jeden dlhý riadok rozdelený do niekoľkých riadkov. Najčastejšie používané hlavičky sú **From** (Od), **To** (Komu), **Subject** (Predmet) a **Date** (dátum). Ďalšou bežne sa vyskytujúcou hlavičkou v záhlaví podľa [45] je **Message ID** (ID správy). Táto hlavička obsahuje jedinečný identifikátor spojený s touto správou. Na Obrázku 8.12 je zobrazenie základnej štruktúry správy s príkladom správy.

8.3.1 Elektronická pošta MIME

Formát MIME je rozšírením rámca podľa [45], ktorý bol určený na riešenie niektorých problémov a obmedzení použitia protokolu SMTP (Simple Mail Transfer Protocol, tradičný protokol elektronickej pošty definovaný v [40]). Hlavné obmedzenie schémy protokolu **SMTP** podľa [45] je to, že nemôže prenášať textové údaje, ktoré obsahujú znaky národných abecied, pretože tie sú reprezentované 8 bitovým kódom s hodnotami desiatkovo 128 a viacej a SMTP je obmedzený iba na znaky reprezentované 7 bitovým kódom ASCII. Ďalším obmedzením je, že SMTP nemôže prenášať spustiteľné súbory alebo iné binárne objekty. Používa sa veľa schém na konverziu binárnych súborov do textovej formy, ktorá jediná je použiteľná poštovým systémom s protokolom SMTP. Bohužiaľ žiadna z týchto schém nie je štandardom alebo aspoň „de facto“ štandardom.

Špecifikáciu MIME (vyjadrená najmä v [13–17]) možno charakterizovať nasledovne. Je definovaných **päť nových hlavičiek** pre záhlavie správy podľa [45]. Tieto hlavičky poskytujú

informácie o tele správy. Je definovaný rad **nových formátov obsahu** na štandardizáciu reprezentácie, ktoré podporujú **multimediálnu elektronickú poštu**. Sú definované **schémy kódovania prenosu** umožňujúce konverziu akéhokoľvek formátu obsahu do tvaru, ktorý je chránená pred zmenou poštovým systémom.

V MIME je definovanch päť nových hlavičiek:

- **MIME-Version:** Musí mať hodnotu parametra 1.0. Toto pole indikuje, že správa je v súlade s [14] a [16].
- **Content-Type:** Opisuje dostatočne detailne údaje obsiahnuté v tele tak, že klient elektronickej pošty príjemcu môže vybrať vhodný prostriedok alebo mechanizmus na reprezentáciu údajov príjemcovi alebo inak pracovať s údajmi vhodným spôsobom.
- **Content-Transfer-Encoding:** Označuje typ transformácie, ktorý bol použitý na reprezentáciu tela správy spôsobom, ktorý je prijateľný pre prenos pošty.
- **Content-ID:** Používa sa na jednoznačnú identifikáciu entít MIME v rôznych kontextoch.
- **Content-Description:** textový opis objektu v tele správy. Je to užitočné v prípade, keď objekt nie je čitateľný (napr. audio údaje).

Neskoršie bola v [49] dodefinovaná hlavička **Content-Disposition**, ktorá určuje, či prenášané údaje v tele správy sú určené na automatické zobrazenie príjemcovi (inline) alebo nie sú určené k automatickému zobrazeniu príjemcovi (attachment), t.j. príjemca ich má spracovávať ručne (napr. sa jedná o súbor, ktorý má byť uložený na lokálnom disku).

Niektoré alebo všetky tieto hlavičky sa môžu objaviť v normálnom záhlaví [45]. **Kompliantná implementácia MIME musí podporovať hlavičky** MIME-Version, Content-Type a Content-Transfer-Encoding. Hlavičky Content-ID a Content-Description a Content-Disposition sú voliteľné a môže byť príjemcom ignorované.

Prevažná časť špecifikácie MIME sa týka definície rôznych typov obsahu. To odráža potrebu zabezpečiť štandardizované spôsoby zaobchádzania s najrôznejšími reprezentáciami v multimediálnom prostredí. Existuje sedem rôznych hlavných typov obsahu a celkom 15 podtypov. Vo všeobecnosti typ obsahu deklaruje všeobecný typ údajov a podtyp určuje určitý formát pre tento typ údajov.

Pre telo typu **Text** nie je potrebný žiadny špeciálny softvér na získanie plného významu textu okrem podpory uvedeného súboru znakov. Primárny podtyp je **Plain** (obyčajný text), čo je jednoducho reťazec znakov ASCII alebo znakov [24]. Podtyp **Enriched** (obohatený text, definovaný v [46]) umožňuje väčšiu flexibilitu formátovania.

Typ **message** poskytuje rad dôležitých funkcií MIME.

- Podtyp **rfc822** indikuje, že telo je celá správa elektronickej pošty vrátane hlavičky a tela. Bez ohľadu na meno tohto podtypu zapúzdrená správa môže byť nielen jednoduchá správa [45], ale tiež lubovoľná správa MIME.

- Podtyp **partial** umožňuje fragmentáciu veľkej správy do niekoľkých menších častí, ktoré treba na mieste určenia znovu poskladať. Pre tento podtyp sú špecifikované v hlavičke Content-Type: Message/Partial ďalšie tri parametre: identifikátor **id**, je rovnaký pre všetky fragmenty, číslo sekvencie **sequence number**, je jedinečné číslo každého fragmentu a číslo **total** je celkový počet fragmentov.

- Podtyp **external-body** indikuje, že skutočné údaje, ktoré by sa mali prepravovať v tejto správe nie sú obsiahnuté v tele správy. Namiesto toho je v tele správy informácia potrebná na prístup k údajom. Tak ako pri ostatných typoch message má aj podtyp external-body vonkajšie záhlavie a vnorenú správu so svojim vlastným záhlavím. Jediné potrebné pole vo vonkajšom záhlaví je hlavička Content-Type, ktorá stanovuje podtyp external-body. Vnútorné záhlavie je záhlavie správy pre vnorenú správu. Hlavička Content-Type vo vonkajšom záhlaví musí obsahovať parameter prístupu **access-type**, ktorý udáva spôsob prístupu ako je napríklad protokol FTP (File Transfer Protocol).

Typ **image** špecifikuje obrázok. Obsahom tela správy je obrázok. K jeho prezentácii je treba odpovedajúci prehliadač. Podtyp **jpeg** indikuje, že obraz je vo formáte JPEG, kódovanie JFTF. Podtyp **gif** indikuje, že obraz je vo formáte GIF.

Typ **audio** špecifikuje zvuk. Na prezentáciu je treba odpovedajúci prehrávač. Podtypom je **basic**, mono so vzorkovacím kmitočtom 8 kHz.

Typ **video** špecifikuje video. Implicitný podtyp je **mpeg**, video vo formáte MPEG.

Typ **application** odpovedá ďalším typom údajov, typicky alebo neinterpretovateľným binárnym údajom alebo informáciam, ktoré budú spracované poštovou aplikáciou.

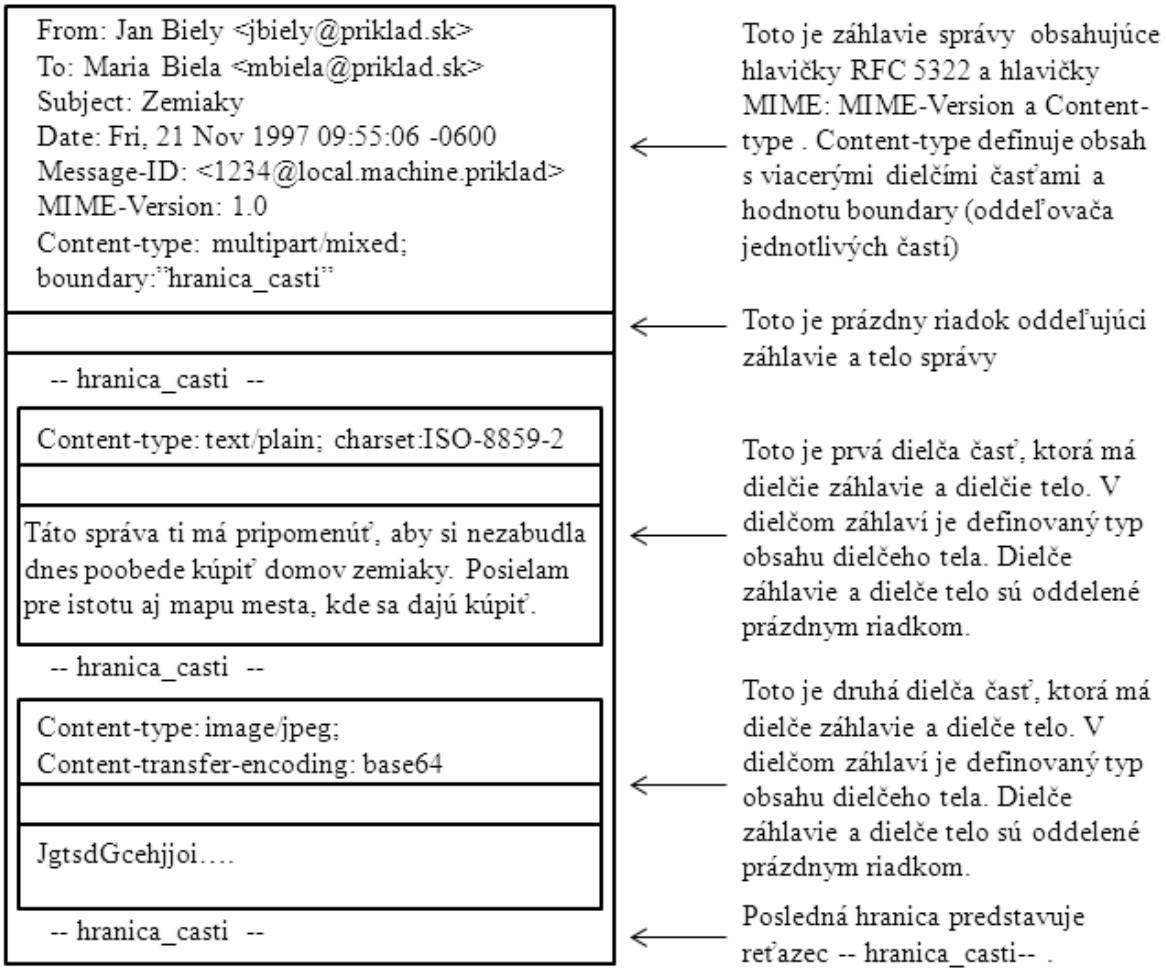
Typ **multipart** indikuje, že telo správy obsahuje viacero nezávislých častí (kompozitná správa). Hlavička **Content-Type** obsahuje parameter **boundary** (hranica), ktorý definuje oddeľovač medzi časťami tela. Táto hranica by sa nemala vyskytovať v žiadnej časti správy. Každá hranica v tele správy začína na novom riadku a pozostáva z dvoch pomlčiek nasledovaných reťazcom znakov parametra boundary. Posledná hranica v tele správy označujúca koniec poslednej časti má aj na konci príponu dvoch pomlčiek. V každej časti môže byť voliteľne obyčajné záhlavie MIME. Na Obrázku 8.13 je schematicky znázornený príklad štruktúry správy typu multipart.

Existujú štyri podtypy typu **multipart**, každý z nich má rovnakú celkový syntax.

- Podtyp **mixed** sa používa vtedy, ak telo správy sa skladá z viacerých nezávislých častí a tieto časti sú spojené v určitom poradí.

- Pre podtyp **parallel** nie je poradie jednotlivých častí tela správy významný. Ak je príjemcov systém na to vybavený, jednotlivé časti správy sú prezentované paralelne. Mohlo by ísť napríklad o správu s dvomi časťami. Jedna časť obsahuje obrázok, druhá časť obsahuje hlasový komentár k obrázku. Ak je na to príjemcov systém uspôsobený, po otvorení správy sa mu zobrazí obrázok a súčasne sa prehrá zvukový komentár.

- Pre podtyp **alternative** sú rôzne časti reprezentáciou rovnakej informácie. Na Obrázku 8.14 je uvedený príklad správy s podtypom alternative. V tomto podtype sú časti tela správy uložené usporiadane v poradí zvyšovania preferencií. Nech sa telo správy skladá z



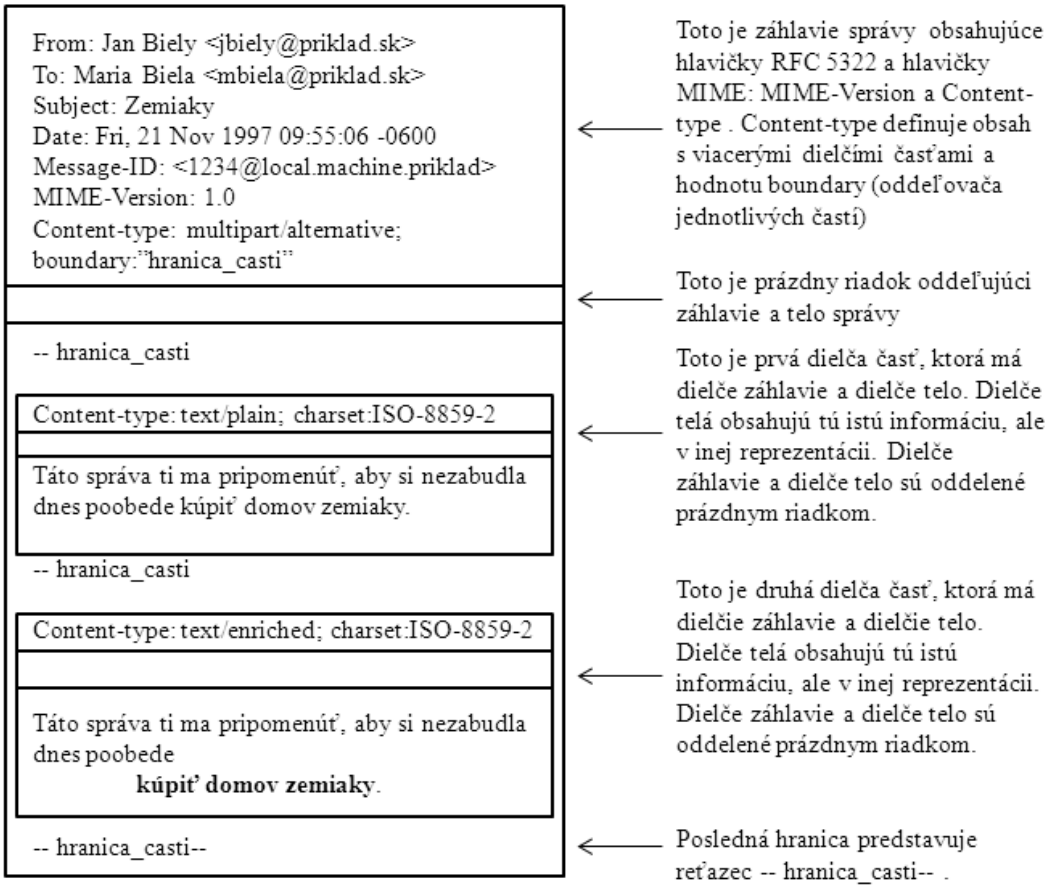
Obr. 8.13: Príklad štruktúry správy typu multipart s podtypom mixed

dvoch rovnakých textových častí, prvá časť obsahuje hlavičku Content-Type: text/plain a druhá časť obsahuje hlavičku Content-Type: text/enriched. Ak príjemcov systém je schopný zobrazovať správu vo formáte text/enriched, potom sa tak urobí. V opačnom prípade sa použije formát obyčajného textu text/plain.

- Podtyp **digest** sa používa vtedy, keď každá z častí tela je interpretovaná ako správa [45] so záhlavím. Tento podtyp umožňuje konštrukciu správy, ktorej časti sú individuálne správy. Napríklad moderátor skupiny zbiera správy elektronickej pošty od účastníkov, spojí tieto správy a pošle ich v jednej zapúzdrenej správe MIME.

Kánonický tvar je dôležitý koncept v MIME a S/MIME. Kánonický tvar je formát zodpovedajúci typu obsahu, ktorý je štandardizovaný na použitie medzi systémami. To je na rozdiel od natívneho tvaru, ktorý predstavuje formát charakteristický pre konkrétny systém.

Kódovanie tela správy pri prenose vo formáte MIME je ďalším vážnym komponentom špecifikácie MIME. Cieľom je zabezpečiť spoľahlivé doručenie cez najširšiu škálu prostredí.



Obr. 8.14: Príklad štruktúry správy typu multipart s podtypom alternative

Štandard MIME definuje dve metódy kódovania údajov. Hlavička **Content-Transfer-Encoding** môže v skutočnosti nadobúdať šesť hodnôt. Tri z týchto hodnôt (7 bitové, 8 bitové a binárne) naznačujú, že nebolo vykonané žiadne kódovanie, ale tieto hodnoty poskytujú niektoré informácie o charaktere údajov. Pre prenos SMTP je bezpečné používať 7 bitový tvar. 8 bitový a binárny tvar môže byť použiteľný v iných súvislostiach prenosu pošty. Ďalšie hodnota hlavičky Content-Transfer-Encoding je **x-token** vyjadrujúca, že je použité iné kódovanie, ktoré môže byť špecifikované dodávateľom alebo konkrétnou aplikáciou. Dve skutočné definované kódovacie schémy sú **quoted-printable** a **base64**. Tieto dve kódovacie schémy sú definované tak, aby zabezpečili výber medzi technikou prenosu, ktorá je v podstate človeku čitateľná a tým, aby boli bezpečné pre všetky typy údajov pri rozumnej miere kompaktnosti.

Kódovanie prenosu **quoted-printable** je užitočné v prípade, keď údaje väčšinou pozostávajú prevažne z oktetov, ktoré zodpovedajú tlačiteľným znakom ASCII. Znaky, ktoré nie sú bezpečné (nenachádzajú sa v 7 bitovom kóde ASCII) sú reprezentované svojou hexadecimálnou reprezentáciou, pred ktorú sa vloží znak = (mäkká zarážka). Napríklad reťazec „Ján Vojačik“ by sa kódovalo ako „J=E1n Voja=E8ik“, pretože hexadecimálny kód pre á je E1 a pre č je E8 a ostatné znaky sú obsiahnuté v 7 bitovom kóde ASCII. Mäkká zarážka sa použije aj na ukončenie dlhého riadku správy tak, aby obmedzil dlžku riadku správy na 76 znakov.

Kódovanie prenosu **base64** je bežne používané kódovanie ľubovoľných binárnych dát takým spôsobom, aby boli nepoškoditeľné pri spracovaní programom na prenos pošty. Je to kódovanie rovnaké ako radix-64 s tým, že radix-64 prikladá aj kontrolný súčet kódovaných údajov. Kódovanie znakov podľa schémy base64 je na Obrázku 8.15.

6 bitová hodnota	Kódovaný znak	6 bitová hodnota	Kódovaný znak	6 bitová hodnota	Kódovaný znak	6 bitová hodnota	Kódovaný znak
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/
						výplň 00_2	=

Obr. 8.15: Kódovacia tabuľka base64

Jednoduchá demonštrácia fungovania kódovania podľa schémy base64 sa ukáže na príklade. Predpokladajme, že vstupné údaje sú tri slabiky (bajty) vyjadrené binárne ako 10101010 01010101 11001100. Pri kódovaní base64 sa táto postupnosť rozdelí na skupiny po šiestich bitoch. To znamená, že preskupením dostaneme 101010 100101 010111 001100, čo v dekadickom vyjadrení je 42 37 23 12 a v kóde base64 je to postupnosť znakov qlXM (bez medzier medzi znakmi).

8.3.2 Funkcie S/MIME

Bezpečná elektronická pošta S/MIME ponúka možnosť podpísania a/alebo šifrovania správ prostredníctvom týchto funkcií:

- **Enveloped data** (obálkované údaje): Skladá sa zo zašifrovaného obsahu lubovoľného typu a zašifrovaného kľúča (ktorým sa zašifroval obsah) a to pre každého príjemcu.
- **Signed data** (podpísané údaje): Digitálny podpis je vytvorený tak, že sa vytvorí kontrolná suma podpisovaného obsahu a tento kontrolný súčet sa zašifruje privátnym kľúčom podpisovateľa. Obsah a podpis sú potom zakódované pomocou schémy base64. Správu s podpísaným obsahom môže vidieť iba príjemca s funkcionalitou S/MIME.

- **Clear-signed** data (iba podpísané údaje): Je vytvorený digitálny podpis obsahu rovnako ako pri podpísaných údajoch. V tomto prípade je iba digitálny podpis kódovaný pomocou schémy base64. Výsledkom je, že príjemcovia bez funkcionalít S/MIME sú schopní prečítať obsahu správy aj keď nemôže overiť podpis.

- **Signed and enveloped data** (podpísané a obálkované údaje): iba podpísané a iba šifrované entity môžu byť vnorené. To znamená, že zašifrované údaje môžu byť podpísané a podpísané údaje alebo iba podpísané údaje môžu byť zašifrované.

S/MIME zavádza niekoľko nových typov obsahu MIME. Všetky nové typy aplikácií používajú označenie PKCS (špecifikácie kryptografie s verejným kľúčom vydaných spoločnosťou RSA Laboratories a sprístupnené pre S/MIME).

S/MIME zabezpečuje entity MIME pomocou podpisu, šifrovaním alebo obojím. Entita MIME môže byť celá správa (s výnimkou záhlaví [45] alebo ak typ obsahu MIME je multipart, potom entita MIME je jedna alebo viac podčastí správy. Entita MIME je vytvorená podľa štandardných pravidiel vytvárania správ MIME. Potom entita MIME plus niektoré údaje súvisiace s bezpečnosťou (identifikácia algoritmov a certifikáty) sú spracované S/MIME s výsledkom vytvorenia PKCS objektu. S PKCS objektom sa potom zaobchádza ako s obsahom správy a je zabalený do MIME (vybavená vhodnými hlavičkami MIME).

Vo všetkých prípadoch je odoslaná správa konvertovaná do **kánonického tvaru**. Najmä pre daný typ a podtyp je použitý vhodný kánonický tvar pre obsah správy. Pre správu typu multipart je použitý vhodný kánonický tvar pre každú podčasť.

Použitie kódovania prenosu si vyžaduje osobitnú pozornosť. Vo väčšine prípadov bude výsledkom použitia bezpečnostného algoritmu vytvorený objekt, ktorý je čiastočne alebo úplne vyjadrený ako ľubovoľné binárne údaje. Tento objekt bude potom zabalený vo vonkajšej správe MIME a kódovanie prenosu môže byť použité v tomto bode, štandardne base64. Avšak v prípade správy multipart/signed je obsah správy v jednej z podčastí bezpečnostným procesom nezmenený. Ak nie je tento obsah 7 bitový, prenos by mal byť kódovaný schémou base64 alebo quoted-printable tak, aby nebolo žiadne nebezpečenstvo zmeny obsahu, na ktorý bol podpis aplikovaný.

Základné typy obsahu S/MIME sú:

- Pre typ **multipart** je podtyp **Signed**: iba podpísaná správa, ktorá sa skladá z dvoch častí. Prvá časť je správa a druhá je podpis.

- Pre typ **application** je podtyp **pkcs7-signature**: typ obsahu pre podčasť podpisu správy multipart/signed.

- Pre typ **application** je podtyp **pkcs7-mime**. Bližšiu špecifikáciu určuje parameter **smime**. Parameter smime=signedData označuje podpísanú entitu S/MIME. Parameter smime=envelopedData označuje zašifrovanú entitu S/MIME. Parameter smime= degenerate signedData označuje, že entita S/MIME obsahuje iba certifikáty.

Podtyp **application/pkcs7-mime** sa používa pre jednu z troch kategórií spracovania S/MIME, každú s jedinečným parametrom **smime-type** (parameter smime-type nadobúda hodnoty sig-

nedData, envelopedData, degenerate signedData). Vo všetkých prípadoch výsledná entita (ďalej len objekt) je reprezentovaná vo forme známej ako BER (Basic Encoding Rules), ktorá je definovaná v ITU-T Odporúčaniach X.209. Formát BER sa skladá z ľubovoľných oktetových reťazcov a predstavuje teda binárne dáta. Takýto objekt by mal byť kódovaný pri prenose schémou base64 vo vonkajšej správe MIME.

Postup na vytvorenie entity MIME typu **envelopedData** je:

1. Generuj pseudonáhodný relačný kľúč pre konkrétny symetrický šifrovací algoritmus (napríklad triple DES).
2. Pre každého príjemcu zašifruj relačný kľúč jeho verejným kľúčom z certifikátu. Pre každého príjemcu sa vytvorí blok označený **RecipientInfo**, ktorý obsahuje identifikátor (ID) certifikátu verejného kľúča príjemcu, identifikátor (ID) algoritmu použitého na zašifrovanie relačného kľúča a zašifrovaný relačný kľúč.
3. Zašifruj obsah správy relačným kľúčom a vlož do štruktúry envelopedData.

Bloky RecipientInfo sú nasledované zašifrovaným obsahom a vytvárajú envelopedData. Táto informácia je potom zakódovaná schémou base64. Na Obrázku 8.16 je znázornená schéma vytvorenia entity typu envelopedData pre dvoch príjemcov.

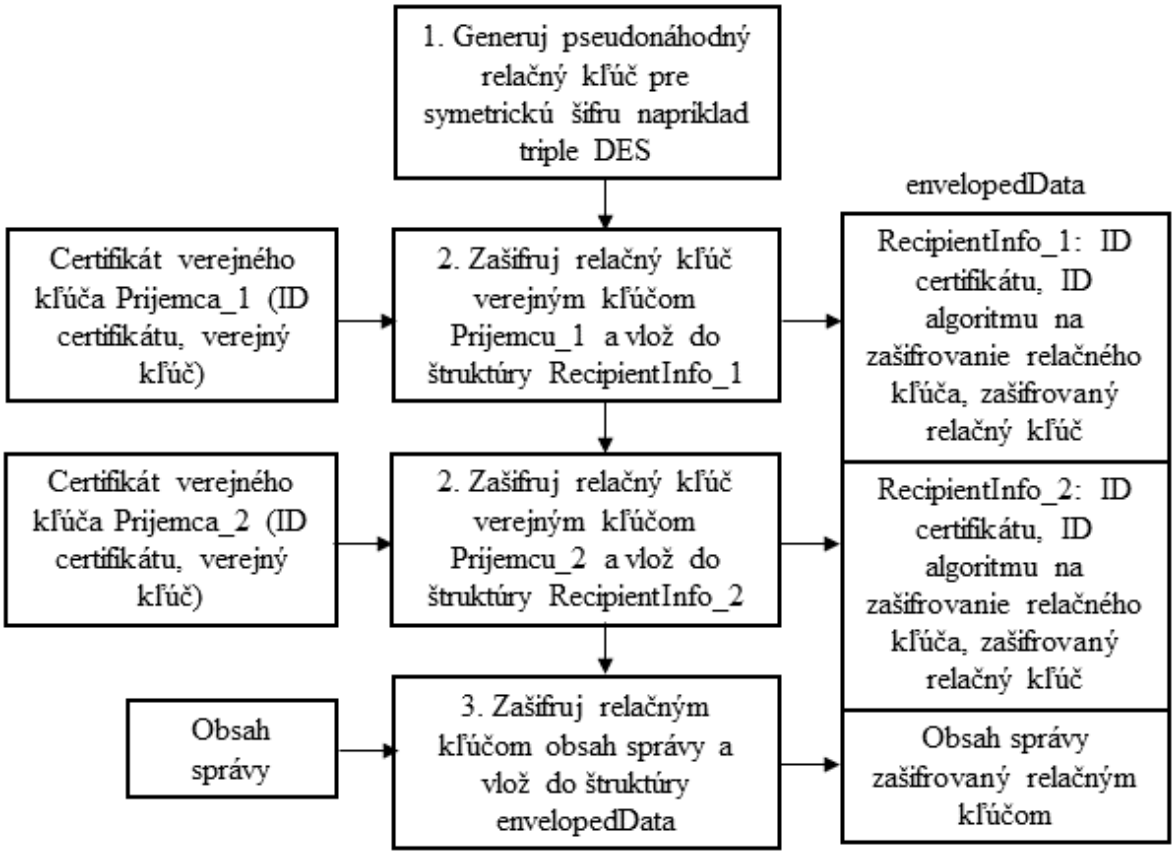
Na znovuzískanie zašifrovanej správy príjemca najprv dešifruje správu podľa schémy base64. Potom príjemca použije svoj privátny kľúč a dešifruje relačný kľúč. Nakoniec je obsah správy dešifrovaný relačným kľúčom.

Typ smime označený **signedData** (parameter smime-type=signedData) môže byť použitý s jedným alebo viacerými podpisovateľmi. Pre názornosť sa uvedie opis prípadu s jedným podpisovateľom. Postup na vytvorenie entity MIME typu signedData je:

1. Vyber algoritmus na vytvorenie kontrolného súčtu (napríklad SHA) a vypočítaj kontrolnú sumu (hash hodnotu) obsahu, ktorý má byť podpísaný.
2. Zašifrujte kontrolnú sumu privátnym kľúčom podpisovateľa.
3. Priprav blok označený ako **SignerInfo**, ktorý obsahuje certifikát verejného kľúča podpisovateľa, identifikáciu algoritmu na výpočet kontrolnej sumy, identifikátor šifrovacieho algoritmu kontrolnej sumy a zašifrovanú kontrolnú sumu.

Entita signedData sa skladá z radu blokov vrátane identifikátora algoritmu na výpočet kontrolnej sumy správy, podpísanej správy a SignerInfo. Entita signedData môže ešte obsahovať sadu certifikátov verejných kľúčov od dôveryhodnej alebo koreňovej certifikačnej autority, ktoré sú potrebné na overenie platnosti podpisu. Táto informácia je potom zakódovaná schémou base64.

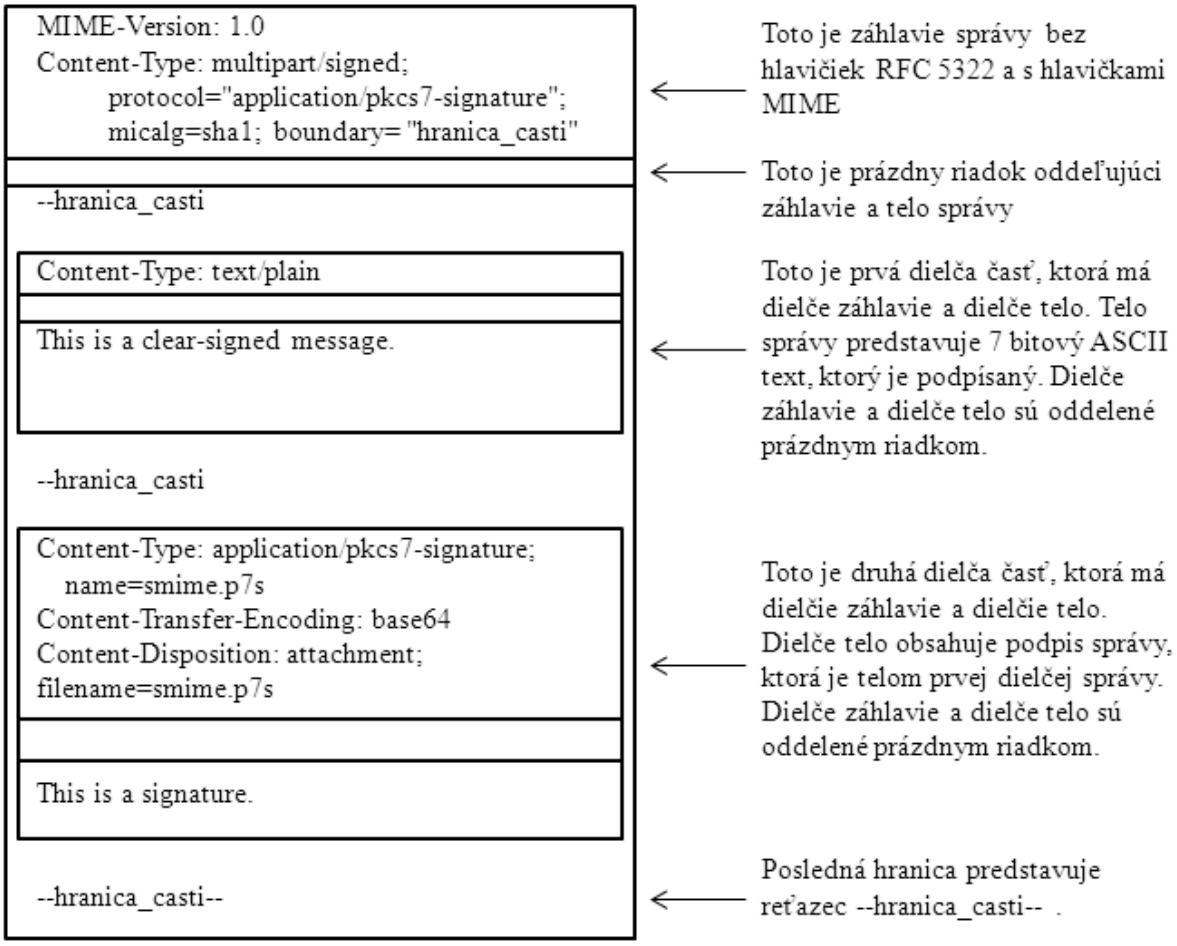
Na obnovenie podpísanej správy a overenie podpisu, príjemca najprv odkóduje base64. Potom príjemca overí platnosť podpisu tak, že overí platnosť certifikátu a verejným kľúčom dešifruje zašifrovanú kontrolnú sumu správy. Ďalej vypočíta kontrolný súčet podpísanej správy. Ak sa rovnajú kontrolné súčty, jeden vytvorený príjemcom z podpísanej správa a druhý zistený dešifrovaním zašifrovaného kontrolného súčtu podpísanej správy, potom je podpis správy overený.



Obr. 8.16: Postup vytvorenia entity envelopedData pre dvoch príjemcov

Iba podpísanie (clear-signed) je dosiahnuté pomocou typu obsahu **multipart** a podtypu **signed**. Ako už bolo spomenuté, tento proces podpisovania nezahŕňa transformáciu správy, ktorá je podpísaná, takže správa je odoslaná v pôvodnom tvare. Takže príjemcovia s funkciami MIME, ale nie s funkciami S/MIME, sú schopní prečítať prichádzajúcu správu. Správa multipart/signed má dve časti. Prvá časť môže byť akýkoľvek typ MIME, ale musí byť vytvorená tak, že sa nebude meniť v počas prenosu od zdroja k cieľu. To znamená, že ak prvá časť nie je 7 bitová, potom je potrebné, aby sa prvá časť zakódovala schémou base64 alebo quoted-printable. Potom je táto časť spracovaná rovnakým spôsobom ako signedData, ale v tomto prípade je vytvorený objekt vo formáte signedData, ktorý má prázdne pole obsahu správy. Tento objekt je oddelený podpis. Potom je kódovaný na prenos schémou base64 a stane sa druhou časťou správy multipart/signed. Táto druhá časť má **type** obsahu MIME **application** a podtyp **pkcs7-signature**. Na Obrázku 8.17 je ukážka štruktúry správy.

Parameter **protocol** označuje, že sa jedná o entitu iba podpísanú (clear-signed) s dvomi časťami. Parameter **micalg** udáva typ použitej funkcie na výpočet kontrolného súčtu. Príjemca môže overiť podpis tým, že vypočíta kontrolný súčet prvej časti a porovnaním ho s kontrolným súčtom získaným z druhej časti.



Obr. 8.17: Štruktúra správy clear-signed

8.4 Protokol HTTP

Úspešné fungovanie svetovej pavučiny www (world wide web) je výsledkom efektívnosti a užitočnosti celého hypermediálneho systému, ktorý implementuje. Okrem nástrojov HTML a URL je **protokol HTTP** (Hypertext Transfer Protocol) pravdepodobne najdôležitejšou súčasťou webu. Tento protokol vlastne prenáša hypertextové dokumenty a ďalšie súbory medzi webovými servermi a webovými klientmi. Tvorcovia protokolu http si „vypožičali“ koncepciu hlavičiek a typov médií zo špecifikácie elektronickej pošty [5, 13–17].

V súčasnosti sa najviac používa verzia 1.1 protokolu HTTP, skrátene sa zapisuje HTTP/1.1. Táto verzia je špecifikovaná v dokumente [10]. Bezpečnostné a autentizačné problémy sú špecifikované v dokumente [12]. Pri opise protokolu HTTP sa bude vychádzať z týchto špecifikácií. Špecifikácia HTTP/1.1 zabezpečuje spätnú kompatibilitu so staršími verziami protokolu HTTP/1.0 a HTTP/0.9.

8.4.1 Základná koncepcia protokolu

Protokol HTTP je typu **klient/server**. Vo svojej najjednoduchšej podobe prevádzka protokolu HTTP zahrňuje klienta protokolu HTTP, reprezentovaného zvyčajne internetovým prehliadačom na klientskom počítači, a server protokolu HTTP, reprezentovaného zvyčajne webovým serverom. Po vytvorení spojenia TCP sa pri komunikácii realizujú dva kroky. Klient pošle správu so žiadosťou vo formáte podľa pravidiel štandardu HTTP – **žiadosť HTTP** (HTTP Request). Táto správa udáva zdroj na serveri HTTP, ktorý si klient želá získať, alebo obsahuje informácie, ktoré majú byť poskytnuté serveru. Server HTTP prevezme a interpretuje žiadosť klienta. Vykoná akcie týkajúce sa žiadosti a vytvorí správu **odpovede HTTP** (HTTP Response), ktorú pošle späť klientovi. Správa odpovede indikuje či žiadosť bola úspešná a ak je to vhodné, môže tiež obsahovať obsah klientom požadovaného zdroja.

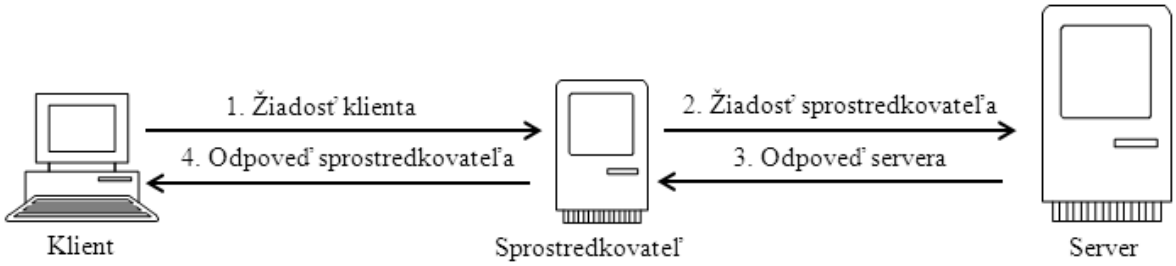
V protokole HTTP/1.0 každé spojenie TCP obsahuje iba jednu takúto výmenu, v protokole HTTP/1.1 je možných takýchto výmen v rámci jedného spojenia TCP viacero. Treba tiež poznamenať, že server môže v niektorých prípadoch odpovedať jednou alebo predbežnou odpoveďou, predým než odošle úplnú odpoveď. Táto situácia môže nastať v prípade, že server odošle predbežné odpoveď použitím stavového kódu 100 Continue pred skutočnou odpoveďou.

Jednoduchá dvojica žiadosť HTTP / odpoveď HTTP medzi klientom a serverom sa stáva zložitejšou, keď sú vo virtuálnej komunikačnej ceste medzi klientom a serverom umiestnení **sprostredkovatelia** (intermediary). Ide o také zariadenia ako **proxy**, **brány** alebo **tunely**, ktoré sa používajú na zvýšenie výkonu (priepustnosti), zaisteniu bezpečnosti alebo vykonávajú iné potrebné funkcie pre konkrétnych klientov alebo servery. Proxy servery sa bežne používajú na webe, pretože môžu výrazne zlepšiť čas odozvy pre skupinu podobných klientskych počítačov.

Keď je v komunikácii medzi klientom a serverom HTTP zapojený sprostredkovateľ HTTP komunikácie, tak **klient komunikuje so serverom prostredníctvom sprostredkovateľa**. To znamená, že všetka premávka (traffic) medzi klientom a serverom prechádza sprostredkovateľom. Táto skutočnosť **umožňuje sprostredkovateľovi vykonávať rôzne funkcie nad prechádzajúcou premávkou**, napríklad ukladanie do vyrovnávacej pamäti (cache) sprostredkovateľa, preklad, agregácie alebo zapúzdrenie. Na Obrázku 8.18 je demonštrovaný príklad komunikácie medzi klientom a serverom HTTP prostredníctvom jedného sprostredkovateľa. Jednoduchá dvojica žiadosť HTTP / odpoveď HTTP sa zmení na dve dvojice (štyri kroky):

1. Klient HTTP odošle správu žiadosti sprostredkujúcemu zariadeniu.
2. Sprostredkovateľ žiadosť spracuje, vykoná v prípade potreby zmeny v žiadosti, a potom pošle žiadosť na server.
3. Server HTTP prečíta a interpretuje žiadosť, vykoná príslušné akcie a odošle odpoveď. Pretože dostal svoju žiadosť od sprostredkovateľa, jeho odpoveď ide späť sprostredkovateľovi.
4. Sprostredkovateľ odpoveď spracuje, opäť prípadne urobí zmenu, a potom ju pošle klientovi.

Uvedený príklad možno zovšeobecniť na viacero sprostredkovateľov pri komunikácii medzi klientom a serverom.



Obr. 8.18: Komunikácia klient/server cez sprostredkovateľa

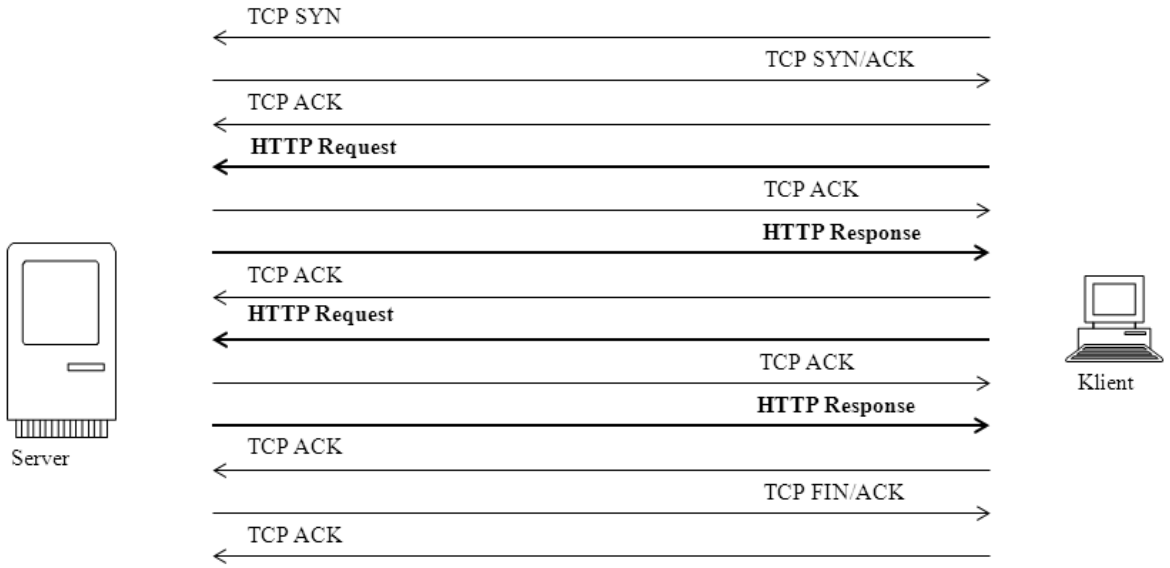
Pri komunikácii medzi klientom a serverom cez sprostredkovateľa pôsobí sprostredkovateľ vo vzťahu ku klientovi ako server a vo vzťahu k serveru ako klient. Mnohí sprostredkovatelia sú navrhnutí tak, aby boli schopní odpočúvať rôzne protokoly TCP/IP. Väčšina protokolov nevie o existencii vloženého sprostredkovateľa. Protokol HTTP však obsahuje špeciálnu podporu pre určitých sprostredkovateľov, ako sú **proxy servery**, ktorým poskytuje nástroje (hlavičky) na narábanie so žiadosťami a odpoveďami HTTP.

Model normálnej komunikácie HTTP je možné zmeniť prostredníctvom odkladania žiadostí klientov a odpovedí serverov na tieto žiadosti do vyrovnávacej pamäti **cache** (tejto metóde sa hovorí caching). Ukladanie nedávno získaných zdrojov do pamäti cache je aplikované rôznymi zariadeniami na webe, napríklad sprostredkovateľmi typu proxy. Tieto zdroje je možné znovu rýchle získať z pamäti cache, keď je zadaná takáto žiadosť. Klient si sám do svojej pamäti cache ukladá nedávno získané dokumenty z webu tak, že ak o ne požiada opäť, môžu mu byť zobrazené aj bez zadania žiadosti na server. Ak je zadanie žiadosti skutočne nevyhnutné (požadovaný dokument sa v pamäti cache klienta nenachádza), môže každý sprostredkovateľ uspokojiť požiadavku na dokument, pokiaľ ho sprostredkovateľ má vo svojej pamäti cache.

Protokoly HTTP/0.9 a HTTP/1.0 podporovali iba **prechodné spojenie** medzi klientom a serverom HTTP, čo znamená, že v jednom spojení TCP bolo možné vykonať jedinú výmenu žiadosť HTTP/odpoveď HTTP. Takýto model spojenia je veľmi neefektívny pre moderný web, v ktorom klienti často potrebujú vykonať desiatky žiadostí na server. Protokol HTTP/1.1 funguje štandardne s **trvalými spojeniami**. Po vytvorení spojenia TCP môže klient poslať na server veľa žiadostí a jeden po druhom prijímať odpovede. Tento model spojenia umožňuje rýchlejšie získanie súborov, šetrí prostriedky servera a šetrí šírku pásma internetového pripojenia. Klient môže dokonca **zreťaziť** (pipeline) svoje žiadosti odosielaním druhej žiadosti ešte predtým, ako by musel najprv čakať na odpoveď na prvú žiadosť. Protokol HTTP/1.1 stále podporuje prechodové spoje z dôvodu spätnej kompatibility, keď je to potrebné. Na Obrázku 8.19 je príklad trvalého spojenia klienta a servera HTTP.

8.4.2 Formát správy žiadosti

Všetky správy HTTP sú v súlade so štruktúrou nazývanou **formát generickej správy**. Tento formát je založený na štandardoch správ elektronickej pošty [5, 13–17], aj keď sa HTTP presne neriadi týmito formátmi. Každá správa HTTP začína **štartovacím riadkom**, potom obsahuje rad **hlavičiek správy** nasledovaný **prázdnym riadkom** a prípadne **telom správy**. Telo správy môže voliteľne obsahovať zdroj ako je napríklad **súbor**, ktorý je prenášaný medzi



Obr. 8.19: Príklad trvalého spojenia klienta a servera HTTP

klientom a serverom, a **ukončenie správy** (trailer). Tomuto zdroju sa hovorí **entita**.

Žiadosť HTTP používa formát správy vychádzajúci z generického formátu správy a obsahuje v poradí tieto časti: riadok žiadosti, všeobecné hlavičky, hlavičky žiadosti, hlavičky entity, prázdny riadok, prípadne telo správy a ukončenie (trailer) správy.

Generický štartovací riadok, ktorým začínajú všetky správy HTTP sa v prípade formátu správy žiadosti HTTP nazýva **riadok žiadosti**. Tento riadok má trojaký účel: indikuje príkaz alebo akciu, ktorú chce klient vykonať, špecifikuje zdroje, nad ktorými by sa mala táto akcia vykonať a indikuje serveru, akú verzia protokolu HTTP používa klient. Formálna syntax riadka žiadosti je <METHOD> <request-uri> <HTTP-VERSION>, kde

- **METHOD** je typ akcie, ktorú požaduje klient, aby bola vykonaná serverom. Je vždy uvedená veľkými písmenami. V HTTP/1.1 existuje osem štandardných metód, z ktorých tri sú bežne používané, a to: GET, HEAD a POST.

- **request-uri - žiadosť URI** (Uniform Resource Identifier) je identifikátor prostriedku, ktorého sa žiadosť týka. Zatiaľ čo URI môže teoreticky odkazovať na URL (Universal Resource Locator) alebo URN (Uniform Resource Name), v súčasnej dobe je URI takmer vždy URL HTTP, ktoré rešpektuje pravidlá štandardnej syntaxe Web URL. Štandardný spôsob určenia zdroja v žiadosti je zahrnúť cestu a názov súboru v riadku žiadosti, zatiaľ čo špecifikáciu hosta v osobitnej hlavičke **Host**, ktorá musí byť použitá v žiadostiach HTTP/1.1.

- **HTTP-VERSION** oznamuje serveru, akú verziu klient používa a teda, ako interpretovať žiadosť a to, čo má poslať a čo neposielať klientovi vo svojej odpovedi.

Metóda **GET** žiada, aby server vyhľadal zdroj určený adresou URL na riadku žiadosti HTTP a zdroj odoslal v odpovedi klientovi. Metóda **HEAD** je rovnaká ako GET s tým rozdielom, že server neodošle vlastné telo správy. To znamená, že odpoveď bude obsahovať všetky hlavičky ako by boli v odpovedi na ekvivalentnú GET správu. Metóda **POST** umožňuje klientovi poslať entitu na spracovanie na server, ktorá obsahuje ľubovoľné údaje. Bežne sa používa na zaslanie napríklad interaktívneho formulára HTML na server, program na serveri tento formulár spracuje a vykoná akcie na základe vstupov z formulára a klientovi pošle odpoveď. Metóda **OPTIONS** umožňuje klientovi požiadať server, aby poslal informáciu o podporovaných komunikačných možnostiach. Zdroj na serveri je špecifikovaný URI. V prípade, že sa dopyt týka vlastností celého servera, potom sa namiesto URI použije hviezdička. Metóda **PUT** žiada server, aby uložil entitu z tela žiadosti na URL, ktoré je uvedené v riadku žiadosti. Rozdiel medzi metódami PUT a POST je ten, že v metóde PUT URI identifikuje v žiadosti entitu, zatiaľ čo v POST URI identifikuje program určený pre spracovanie entity v žiadosti. Metóda **DELETE** požaduje zrušenie špecifikovaného zdroja na serveri. Metóda **TRACE** umožňuje klientovi obdržať späť kópiu žiadosti, ktorú sám poslal na server. Používa sa na diagnostické účely.

Po riadku žiadosti sa v správe nachádzajú **hlavičky**, ktoré klient chce zahrnúť do správy. Všetky hlavičky používajú rovnakú štruktúru, ale sú rozdelené do kategórií na základe funkcií, ktorým slúžia:

- **Všeobecné hlavičky** sa týkajú hlavne samotnej správy, na rozdiel od jeho obsahu, a slúžia na ovládanie jej spracovania alebo poskytuje príjemcovi ďalšie informácie. Nie sú to špecifické hlavičky pre správu žiadosti alebo odpovedi.
- **Hlavičky žiadosti** oznamujú serveru ďalšie podrobnosti o povahe žiadosti klienta a dávajú klientovi väčšiu kontrolu nad tým, ako je spracovaná žiadosť.
- **Hlavičky entít** opisujú entity obsiahnuté v tele žiadosti, ak existujú. Sú opísané v nasledujúcej časti.

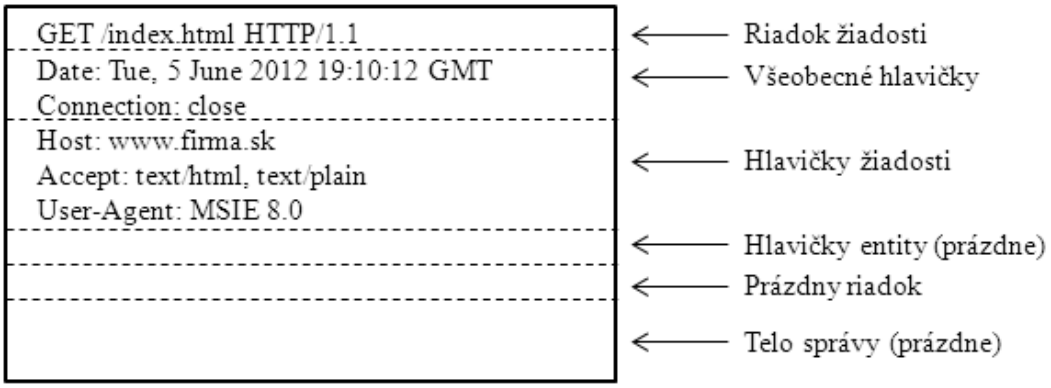
Hlavičky žiadosti sú samozrejme použité iba v správach žiadostí, ale všeobecné hlavičky a hlavičky entity sa môže objaviť buď v správach žiadostí alebo v správach odpovedí.

Všeobecné hlavičky HTTP sa môže vyskytnúť v každej správe žiadosti alebo odpovedi HTTP. Používajú sa na komunikáciu informácií o samotnej správe a nie k jej obsahu. Všeobecné hlavičky sa používajú pre funkcie na stanovenie dátumu a času správy, na riadenie ukladania správy do pamäti cache (caching) a na uvedenie metódy kódovania prenosu správy. Ďalej sú stručne opísané najdôležitejšie všeobecné hlavičky. Hlavička **Cache-control** špecifikuje direktívy pre správu realizácie ukladania správ žiadostí a odpovedí HTTP do pamäti cache. Hlavička **Connection** obsahuje inštrukcie, ktoré sa týkajú len tohto konkrétneho spojenia a nesmú byť uložené na proxy a použité pre ďalšie spojenie. Najčastejšie použitie tejto hlavičky je s parametrom „close“ (Connection: close). Táto hlavička má prednosť pred predvoleným správaním HTTP/1.1 „trvalé spojenie“ a po odpovedi servera vnúti ukončenie spojenia. Hlavička **Date** označuje dátum a čas vzniku správy. Typickým príkladom môže byť: Date: Tue 05 Jun 2012 19:41:41 GMT. Hlavička **Pragma** slúži na povolenie implementačne špecifických direktív vzťahujúcich sa na všetky zariadenia v reťazci žiadosť/odpoveď. Bežné použitie tejto hlavičky v správe je na potlačenie caching „Pragma: no-cache“. Hlavička **Transfer-Encoding**

indikuje aké kódovanie bolo použité na správu s cieľom korektného prenesu medzi zariadeniami. Hlavička **Upgrade** umožňuje zariadeniu klienta určiť ďalšie podporované protokoly. Ak server podporuje tiež jeden z protokolov uvedených klientom, potom sa môže so serverom dohodnúť na aktualizácii spripojenia prostredníctvom alternatívneho protokolu. Hlavička **Via** je doplnená sprostredkovateľom na indikáciu príjemcovi akými bránami, proxy a/alebo tunelmi mu bola dopravená žiadosť alebo odpoveď. Táto hlavička umožňuje jednoduché sledovanie cesty správy a zvládnutie aj potenciálne komplexného reťazca zariadení medzi klientom a serverom. Hlavička **Warning** sa používa v prípade potreby poskytnúť ďalšie informácie o stave správy.

Hlavičky žiadosti HTTP sa uplatňujú len v správach žiadosti HTTP. Umožňujú klientovi poskytnúť serveru informácie o sebe a poskytnúť viac podrobností o žiadosti a nad riadením jej vykonávania. Ďalej sú stručne opísané najdôležitejšie všeobecné hlavičky. Hlavička **Accept** umožňuje klientovi oznámiť serveru aké typy internetových médií je ochotný akceptovať v odpovedi. Hlavička môže obsahovať niekoľko rôznych typov a podtypov médií MIME [13–17], s ktorými vie klient narábať. Každá hlavička môže byť doplnená parametrom q (hodnota kvality) vyjadrujúcim preferenciu klienta. Hlavička **Accept-Charset** je podobná ako Accept. Stanovuje akú sadu znakov je klient v odpovedi ochotný akceptovať. Hlavička **Accept-Encoding** je podobná ako Accept a Accept-Charset. Stanovuje aké kódovanie obsahu je klient v odpovedi ochotný akceptovať. Hlavička **Accept-Language** je podobná ako predchádzajúce hlavičky Accept-type. Stanovuje zoznam označení jazykov indikujúci aké jazyky klient podporuje alebo očakáva, že server bude používať vo svojej odpovedi. Hlavičku **Authorization** používa klient na predloženie autentizačných informácií serveru. To nastáva iba v prípade, keď server vyžaduje autentizáciu, často zaslaním stavového kódu 401 Unauthorized v odpovedi na klientovu iniciálnu žiadosť. Hlavička **Expect** označuje určité typy akcií, ktoré očakáva klient, že server vykoná. Zvyčajne server akceptuje označené parametre, ak nie, server pošle odpoveď so stavovým kódom 417 Expectation Failed. Hlavička **From** obsahuje adresu elektronickej pošty používateľa. Hlavička **Host** špecifikuje internetový uzol prostredníctvom doménového mena DNS a môže tiež obsahovať špecifikáciu čísla portu. Táto hlavička je povinná v žiadosti HTTP/1.1. Hlavička **If-Match** robí metódu podmienečnou špecifikovaním príznaku entity týkajúci sa konkrétnej entity, ktorú klient chce pristúpiť. Hlavička **If-Modified-Since** robí metódu podmienečnou oznámením serveru, aby v odpovedi poslal entitu iba vtedy, ak bola zmenená od doby uvedenej v tejto hlavičke. Inak server odošle v odpovedi stavový kód 304 Not modified. Hlavička **If-None-Match** predstavuje hlavičkou s opačnou podmienkou ako hlavička If-Match. Hlavička **If-Range** je používaná v kombinácii s hlavičkou Range a má umožniť klientovi kontrolu či bola entita zmenená a požiadať server o zaslanie danej časti entity. Hlavička **If-Unmodified-Since** je logickým opakom hlavičky If-Modified-Since. Hlavička **Max-Forwards** stanovuje limit na počet postúpení ďalšiemu zariadeniu v reťazci žiadostí. Používa sa iba s metódami TRACE alebo OPTIONS. Hlavička **Proxy-Authorization** je ako hlavička Authorization, ale slúžia na predloženie autentizačných údajov proxy serveru. Hlavička **Range** umožňuje klientovi požadovať, aby mu server poslal iba časť entity tak, že zadá rozsah bajtov v entite. Ak požadovaný rozsah je platný, server odošle iba požadovanú časť entity so stavovým kódom 206 Partial Content. Hlavička **Referer** oznamuje serveru zdroj URL, z ktorého bola získaná adresa URL aktuálnej žiadosti. Hlavička **TE** poskytuje informáciu serveru o tom, ako si klient praje zabezpečiť kódovanie prenosu entít poslaných serverom. Hlavička **User-Agent** poskytuje informácie o klientovom softvéri. Zvyčajne ide o meno a číslo verzie webového prehliadača alebo iný program posielajúci žiadosť. Proxy neupravujú toto pole pri postúpení žiadosti ďalšiemu zariadeniu, ale používajú hlavičku Via.

Na Obrázku 8.20 sú ukázané elementy štruktúry formátu správy žiadosti HTTP a príklad typov hlavičiek, ktoré by mohla obsahovať. Podobne ako väčšina žiadostí HTTP ani táto nenesie žiadnu entitu, takže neexistujú žiadne hlavičky entity a telo správy je prázdne.



Obr. 8.20: Príklad formátu správy žiadosti HTTP

8.4.3 Formát správy odpovedi

Odpoveď HTTP používa formát správy vychádzajúci z generického formátu správy a obsahuje v poradí tieto časti: stavový riadok, všeobecné hlavičky, hlavičky odpovede, hlavičky entity, prázdny riadok, prípadne telo správy a ukončenie (trailer) správy .

Generický štartovací riadok, ktorým začínajú všetky správy HTTP sa v prípade formátu správy odpovede HTTP nazýva **stavový riadok**. Má dve funkcie: oznámiť klientovi akú verziu protokolu server používa a oznámiť výsledok spracovania žiadosti klienta. Formálna syntax stavového riadku je <HTTP-VERSION> <status-code> <reason-phrase>, kde

- **HTTP-VERSION** je položka v stavovom riadku, slúži rovnakému účelu ako je to v riadku žiadosti v správe žiadosti. Oznamuje klientovi číslo verzie protokolu, ktorú server používa pre svoju odpoveď.
- **Status Code and Reason Phrase** (Stavový kód a fráza dôvodu) poskytujú informácie o výsledkoch spracovania žiadosti klienta v dvoch rôznych formách. Stavový kód je trojmiestne číslo oznamujúce klientovi formálny výsledok vykonania jeho predchádzajúcej žiadosti (na základe tohto kódu môže softvér klienta vykonať príslušné akcie). Fráza dôvodu je ďalší opisný textový reťazec, ktorý môže byť zobrazený klientovi HTTP, aby klient videl ako server odpovedal.

Každá žiadosť poslaná klientom na server HTTP spôsobí jednu (alebo viacero) odpovedí servera. Prvý riadok odpovede servera je **stavový riadok**, ktorý obsahuje zhrnutie výsledkov spracovania žiadosti serverom. Stavový riadok obsahuje numerický stavový kód a text frázy dôvodu.

Stavový kód HTTP je trojciferná číslica začínajúca číslicou 1, 2, 3, 4 alebo 5. **Stavový kód 1xx je informačná správa**, ktorá poskytuje všeobecnú informáciu, neindikuje úspešné

vykonanie žiadosti HTTP alebo chybu. **Stavový kód 2xx je správa o úspešnom vykonaní žiadosti HTTP**, ktorá indikuje, že matóda uvedená v žiadosti bola serverom prijatá, pochopená a akceptovaná. **Stavový kód 3xx je správa o presmerovaní**, ktorá indikuje, že žiadosť priamo nezlyhala, ale je potrebná dodatočná akcia predtým než bude žiadosť úspešne vykonaná. **Stavový kód 4xx je správa o chybe klienta**, ktorá indikuje, že žiadosť HTTP je neplatná, obsahuje zlú syntax alebo nemôže byť vykonaná z nejakých iných dôvodov pre chybu klienta. **Stavový kód 5xx je správa o chybe servera**, ktorá indikuje, že žiadosť HTTP je platná, ale server nebol schopný ju vykonať z dôvodu jeho vlastného problému. Na Obrázku 8.21 sú uvedené stavové kódy aj s frázou dôvodu podľa [10].

Stavový kód	Význam (Fráza dôvodu)	Stavový kód	Význam (Fráza dôvodu)
100	Continue	404	Not Found
101	Switching Protocols	405	Method not Allowed
200	OK	406	Not Acceptable
201	Created	407	Proxy Authentication Required
202	Accepted	408	Request Timeout
203	Non-Authoritative Information	409	Conflict
204	No Content	410	Gone
205	Reset Content	411	Length Required
206	Partial Content	412	Precondition Failed
300	Multiple choices	413	Request Entity Too Large
301	Moved Permanently	414	Request-URI Too Long
302	Found	415	Unsupported Media Type
303	See Other	416	Requested Range Not Satisfiable
304	Not Modified	417	Expectation Failed
305	Use Proxy	500	Internal Server Error
306	(Unused)	501	Not Implemented
307	Temporary Redirect	502	Bad Gateway
400	Bad Request	503	Service Unavailable
401	Unauthorised	504	Gateway Timeout
402	Payment Required	505	HTTP Version Not Supported
403	Forbidden		

Obr. 8.21: Stavové kódy HTTP a frázy dôvodu

Správa odpovedi bude vždy obsahovať niekoľko hlavičiek poskytujúcich ďalšie informácie o správe. Hlavička správy odpovede spadajú do týchto kategórií:

- **Všeobecné hlavičky**, ktoré sa vzťahujú k samotnej správe a nie sú špecifické pre správy odpovede alebo entite v tele správy. Jedná sa o rovnaké ako všeobecné hlavičky ako sú generické hlavičky, ktoré sa môžu vyskytnúť v správach žiadostí. Tieto hlavičky sú opísané v predchádzajúcej časti
- **Hlavičky odpovedi** poskytujú dodatočné informácie, ktoré rozširujú výsledné informácie v stavovom riadku. Server môže tiež vracať ďalšie informácie o výsledkoch v tele správy a to najmä v prípade nastalej chyby.
- **Hlavičky entity** opisujú entity obsiahnuté v tele správy odpovedi, ak nejaká je. Ide o rovnaké hlavičky entity, ktoré sa môžu objaviť v správe žiadosti.

Hlavičky odpovede sú samozrejme použité iba v správe odpovedi, zatiaľ čo ostatné sú všeobecné s ohľadom na typ správy.

Hlavičky odpovedi HTTP sa vyskytujú v správach odpovedí HTTP. Poskytujú dodatočné informácie o funkciách a požiadavkách servera HTTP a výsledkoch spracovania žiadosti klienta. V štandarde HTTP/1.1 je definovaných deväť hlavičiek odpovedí. Hlavička **Accept-Ranges** oznamuje klientovi, či server prijíma alebo neprijíma žiadosti o čiastkový obsah prostredníctvom hlavičky Range, ak áno, akého typu. Typický príklad je Accept-Range: bytes v prípade, že server prijíma bajtový rozsah alebo Accept-Range: none, ak rozsah žiadosti nie je podporovaný. Hlavička **Age** oznamuje klientovi približný vek zdroja, ako bol vypočítaný zariadením posielajúcim odpoveď. Hlavička **Etag** špecifikuje značku entity obsiahnutej v odpovedi. Hlavička **Location** označuje nové URL, ktoré posiela server klientovi, aby ho klient použil namiesto URL, ktoré klient pôvodne požadoval. Hlavička **Proxy-Authenticate** je verzia hlavičky WWW-Authenticate hlavičky. Je obsiahnutá v odpovedi so stavovým kódom 407 Proxy Authentication Required a indikuje ako proxy vyžaduje od klienta vykonať autentizáciu. Hlavičku **Retry-After** niekedy obsahuje odpoveď na neúspešné žiadosti ako sú žiadosti s výsledkom so stavovým kódom 503 Service Unavailable. Hlavička **Server** je serverová verzia hlavičky User-Agent. Identifikuje typ a verziu softvéru servera generujúceho odpoveď. Proxy neupravuje toto pole pri posúvaní odpovedi, proxy vloží svoje identifikačné informácie do hlavičky Via. Hlavička **Vary** špecifikuje či je na žiadosť možné odpovedať odpoveďou z pamäti cache. Hlavička **WWW-Authenticate** je obsahnutá v odpovedi so stavovým kódom 401 Unauthorized a indikuje ako server vyžaduje od klienta vykonať autentizáciu.

Hlavičky entity HTTP sa vyskytujú v správach žiadostí alebo v správach odpovedí, ktoré prenášajú v tele správu entitu. Hlavičky opisujú povahu entity vrátane jej typu, jazyka a kódovania s cieľom zabezpečiť riadne spracovanie a prezentáciu entity prijímajúcim zariadením. V ďalšom sú stručne opísané hlavičky entity HTTP/1.1. Hlavička **Allow** zabezpečí zoznam všetkých metód podporovaných konkrétnym zdrojom. Hlavička **Content-Encoding** opisuje každú voliteľnú metódu, ktorá môže byť použitá na kódovanie entity. Hlavička **Content-Language** špecifikuje jazyk určený na použitie entity. Toto je voliteľná hlavička a nemusí byť vhodná pre všetky typy zdrojov. Hlavička **Content-Length** udáva veľkosť entity v bajtoch. Táto hlavička je dôležitá, pretože je používaná príjemcom na určenie konca správy. Hlavička **Content-Location** špecifikuje zdrojové umiestnenie entity a to v tvare absolútneho alebo relatívneho URL. Hlavička **Content-MD5** obsahuje hešovaciu hodnotu entity vypočítanú hešovacou funkciou MD5, používa sa na kontrolu integrity správy. Hlavička **Content-Range** je poslaná v prípade, keď správa obsahuje entitu, ktorá je len časťou celého zdroja. Napríklad fragment súboru poslaný v odpovedi na žiadosť HTTP s metódou GET obsahujúcu hlavičku Range. Hlavička **Content-Type** špecifikuje mediálny typ a podtyp entity a to spôsobom veľmi podobným ako sa používa v hlavičke MIME ([13–17]). Hlavička **Expires** špecifikuje dátum a čas, po uplynutí ktorého by mala byť entita v správe považovaná za „starú“ (stale). Môže byť použitá na identifikáciu určitých entít, ktoré by mali byť ponechané v pamäti HTTP cache na dlhšiu alebo kratšiu dobu než je obvyklé. Hlavička **Last-Modified** udáva dátum a čas poslednej zmeny entity. Táto doba je určená na základe informácií servera.

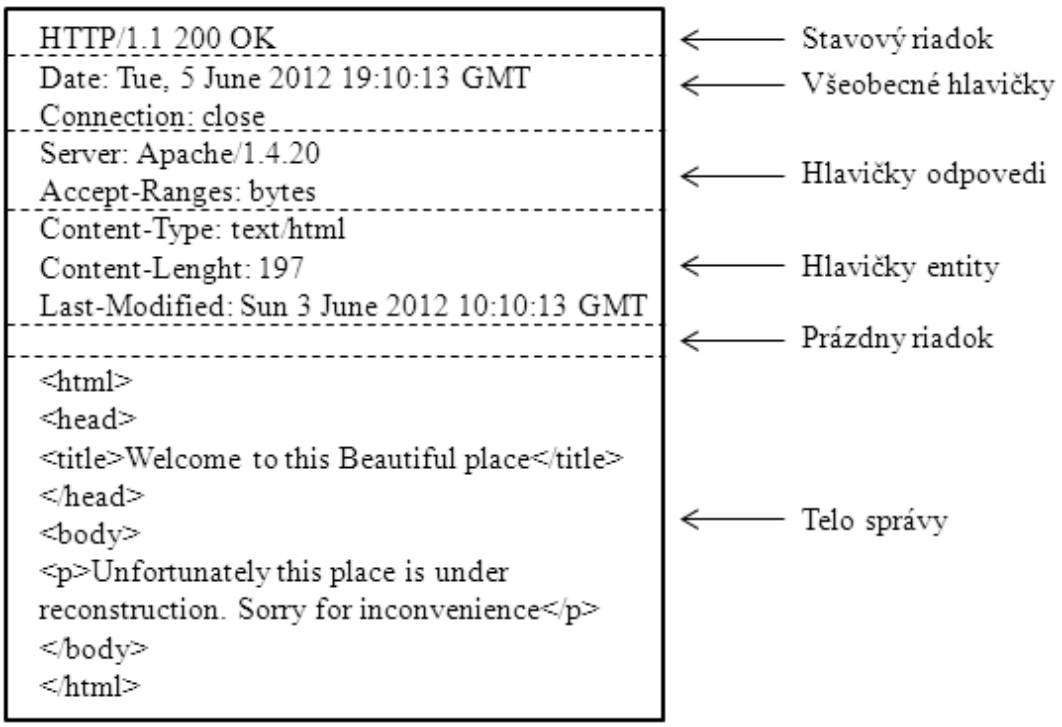
Protokol HTTP podporuje **dve úrovne kódovania prenosu údajov**. Prvý z nich je kódovanie obsahu (hlavička Content-Encoding), ktorý sa používa v niektorých prípadoch k transformácii entity prenášanej v správe HTTP. Druhý je kódovanie prenosu (hlavička Transfer-Encoding), ktorý sa používa na zakódovanie celej správy HTTP, aby sa zaistila jej bezpečná

preprava. Kódovanie obsahu je často používané v prípade, keď entity sú komprimované na zvýšenie účinnosti komunikácie, kódovanie prenosu sa používa predovšetkým na riešenie problému súvisiaceho s identifikáciou konca správy.

Vzhľadom k tomu, že HTTP/1.1 používa trvalé spojenie umožňujúce poslanie viacerých žiadostí a odpovedí v jednom spojení TCP, potrebujú klient a server nejaký spôsob identifikácie konca jednej správy a začiatku druhej správy. Jednoduchším riešením je použitie hlavičky Content-Length špecifikujúcej veľkosť správy. To však funguje len vtedy, keď sa veľkosť správy dá vopred ľahko určiť. Pre dynamický obsah alebo iné prípady, v ktorých nie je možné veľkosť správy ľahko vypočítať pred poslaním údajov, môže sa použiť špeciálne **blokové kódovanie prenosu**. V tomto prenose je telo správy poslané ako postupnosť blokov (chunk) a každý blok začína informáciou o dĺžke bloku.

Keď je použité blokové kódovanie prenosu, môže odosielateľ správy presunúť určité hlavičky zo začiatku na koniec správy, ktorým sa potom hovorí ukončenie. Príjemcom sú interpretované rovnakým spôsobom ako bežné hlavičky. V takýchto správach sa používa špeciálna hlavička **Trailer**, ktorá informuje príjemcu, aby po tele správy hľadal ukončenia.

Protokol HTTP obsahuje funkciu **dohadovanie obsahu**, ktorá umožňuje výber konkrétnej reprezentácie zdroja, pokiaľ má zdroj viac ako jednu reprezentáciu. Existujú dve techniky dohadovania: **serverom riadenú**, v ktorej klient vo svojej žiadosti uvedie hlavičky vyjadrujúce jeho preferencie a server sa snaží o výber najvhodnejšieho variantu, a **agentom riadenú**, v ktorej server odošle klientovi zoznam alternatív dostupných zdrojov a klient si vyberie jednu z nich.



Obr. 8.22: Príklad formátu správy odpovedi HTTP

Najčastejšie používaný typ dohadovania obsahu v protokole HTTP je serverom riadený typ. Klient odoslaním žiadosti môže uviesť až štyri rôzne hlavičky poskytujúce informácie o tom, ako by mal server vyplniť jeho žiadosť. Hlavičky môžu obsahovať voliteľné **hodnoty kvality**, ktoré určujú klientove relatívne preferencie medzi súborom alternatívnych charakteristík zdrojov ako je typ média, jazyk, znaková sada a kódovanie. Ako príklad možno uviesť hlavičku v žiadosti klienta **Accept: text/html, text/*;q=0.7, */*;q=0.1**. Touto hlavičkou klient vyjadruje takéto svoje preferencie: moja preferencia (q=1) je textový dokument HTML, ak nie je dostupný, potom preferujem nejaký iný typ dokumentu (q=0.7), ak nie je ani ten s preferenciou q=0.1 mi pošli iný typ dokumentu, ktorý je relevantný požadovanému zdroju.

Väčšina správ odpovedí obsahujú entitu v tele správy. V prípade úspešnej žiadosti na získanie zdroja, je v tele správy samotný zdroj. Odpovede indikujúce neúspešné žiadosti obyčajne obsahujú podrobné informácie o chybe v chybovej správe, ktorá je často vo formáte HTML.

Obrázok 8.22 ilustruje konštrukciu odpovede HTTP a obsahuje príklad oboch hlavičiek a tela. Stavový kód 200 znamená, že sa jedná o úspešnú odpoveď na žiadosť. Správa obsahuje v tele správy krátku textovú HTML entitu.

8.4.4 Bezpečnosť a privátnosť

Autentizačné metódy použité v protokole HTTP/1.1 sú podrobne riešené v dokumente [12]. Tento dokument vysvetľuje dve autentizačné metódy a to základnú (basic) a metódu digest (hešovacou hodnotou). **Základná autentizačná metóda** predstavuje klasickú autentizáciu menom a heslom. Keď klient odošle žiadosť na server, ktorý vyžaduje autentizáciu pre prístup k zdroju, server odošle na pôvodnú žiadosť klientovi odpoveď, ktorá obsahuje hlavičku WWW-Authenticate. Klient potom pošle novú žiadosť obsahujúcu hlavičku Authorization, ktorá obsahuje meno a heslo používateľa kódované schémou base64. **Autentizácia metódou digest** používa rovnaké hlavičky ako základná autentizačná metóda, ale využíva sofistikovanejšie techniky na výpočet hešovacej hodnoty (jednorázového hesla), ktoré chránia pred útočnikmi a zamedzujú odchyteniu autentizačných údajov. Metóda digest nie je považovaná za tak silnú ako je autentizácia certifikátom verejného kľúča, ale je oveľa lepšie ako základná autentizačná metóda. Podrobnosti možno nájsť v dokumente [12].

Protokol HTTP priamo neobsahuje **žiadny mechanizmus na ochranu privátnosti** prenášaných dokumentov alebo správ. Existujú však dva rôzne prístupy, ktorými sa to zvyčajne zabezpečuje. Najjednoduchší spôsob je šifrovanie zdroja na serveri a dodanie platného dešifrovacieho kľúča iba oprávneným používateľom. Aj keď útočník zachytí celú správu, entita sama bude stále zabezpečená. Úroveň ochrany entity tu závisí na kvalite použitého šifrovania. Ďalšou bežnejšou metódou je použitie dodatočného protokolu, ktorý je určený špeciálne pre zabezpečenie privátnosti transakcie HTTP. Veľmi často sa používa protokol SSL (Secure Sockets Layer). Servery používajú SSL na ochranu citlivých zdrojov, ako sú napríklad zdroje spojené s finančnými transakciami. Tieto sú prístupné pomocou schémy URL „https“ a nie „http“ vo webovom prehliadači. Verzia protokolu SSL prevzatá do dokumentov IETF sa nazýva protokol TLS (Transport Layer Security).

Protokol HTTP je **bezstavový protokol**, pretože server narába s každou klientovou žiadosťou nezávisle na predchádzajúcich žiadostiach. Táto charakteristika protokolu HTTP nie je problémom pre väčšinu bežného používania vo svetovej pavučine www, ale je to problém pre interaktívne aplikácie ako elektronické obchody. Používateľ si jednotlivými žiadosťami HTTP

v priebehu času vyberá tovar do nákupného košíka a server by mal sledovať, že do košíka ukladá tovar ten istý používateľ. Na podporu týchto aplikácií, väčšina implementácií HTTP obsahuje voliteľnú funkciu nazvanú **stavový manažment** podľa [2]. Ak je stavový manažment povolený, potom server odošle klientovi malé množstvo informácií nazvaných **cookie**. Cookie je uložený na klientskom počítači a obsahuje dôležité informácie relevantné konkrétnej webovej aplikácii ako je meno zákazníka, položky v nákupnom košíku alebo meno a heslo. Údaje z cookie sú posielané späť na server s každou následnou žiadosťou s tým, že sa serveru dovoľuje tieto informácie aktualizovať a opäť poslať klientovi späť. Cookies takto umožňujú serverom pamätať si používateľské údaje medzi žiadosťami.

Koncepcia cookies má aj svoje potenciálne problémy. Prvým problémom je **prenos citlivých informácií**. Nech napríklad používateľ používa systém internetbankingu. Používateľ sa prihlási na server, ktorý potom uloží meno konta a heslo (autentizačné údaje riadiace prístup k účtu) do cookie. Ak nie je aplikácia implementovaná starostlivo, môže byť správa obsahujúca cookie odchytená útočníkom a tento môže potom následne autentizačné údaje zneužiť. Alebo je možný iný scenár. Niekto znalý môže získať prístup do stroja používateľa a môže získať prístup do súboru, kde sú uložené cookie. Druhým problémom je **nežiadúce použitie cookies**. Teoreticky by cookie mali byť pre používateľa prínosom a nie problémom. Avšak každý server môže vytvoriť cookie z akéhokoľvek dôvodu. V niektorých prípadoch by mohol server nastaviť cookie pre účely monitorovania sídiel, ktoré používateľ navštívi. Takúto aktivitu servera môžu niektorí používatelia považovať za porušenie ich súkromia. Vzhľadom k tomu, že niektoré webové prehliadače neinformujú používateľa, keď sa vytvorí cookie, používateľ si nemusí byť toho ani vedomý. Tretím problémom sú **cookies tretej strany alebo neúmyselné cookies**. Zatiaľ čo väčšina používateľov si o cookies myslí, že cookies sú vytvorené v kontexte prostriedku, ktorý konkrétne požadujú, cookie môžu byť vytvorené ľubovoľným serverom, ktorému je zaslaná žiadosť. Napríklad pri odoslaní žiadosti http://www.firma.sk/index.htm môže táto stránka obsahovať odkaz na logo firmy, ktoré sa nachádza na serveri http://www.logafiriem.sk. Druhé sídlo môže vytvoriť cookie na počítači používateľa, aj keď používateľ nemal nikdy v úmysle k tomuto sídlu pristúpiť. Tomuto sa hovorí cookie tretej strany. Cookies tretích strán môžu byť použité on-line reklamnými spoločnosťami a inými na sledovanie sídiel, ktoré používateľ navštevuje. Z tohto dôvodu sú považované mnohými za nežiaduceho softvér s názvom spyware. Existuje mnoho voľne šíriteľných nástrojov, ktoré umožnia používateľovi identifikovať a odstrániť sledovacie cookie z počítača.

Miera kontroly cookie je veľmi závislá na kvalite a nastavených funkciách webového prehliadača. Mnoho prehliadačov neposkytujú kontrolu toho, ako a kedy sú cookies na stroji používateľa vytvorené, zatiaľ čo iné prehliadače sú v tomto ohľade oveľa lepšie. Niektoré prehliadače umožňujú cookies zakázať, ale zvyčajne po inštalácii prehliadača sú v preddefinovanom nastavení zapnuté. Najpozoruhodnejšie v tomto ohľade je populárny prehliadač Microsoft Internet Explorer, ktorý má preddefinované nastavenie cookies zapnuté. To znamená, že je štandardne nastavený tak, aby akceptoval všetky cookies bez obmedzenia a dokonca aj bez hlásenia.

Webový prehliadač Internet Explorer umožňuje vypnúť cookies, ale musí to urobiť používateľ. Tiež umožňuje rozlišovať medzi cookies prvej strany a cookies tretích strán, ale opäť si to musí zapnúť používateľ. Ostatné prehliadače majú sofistikovanejšie nastavenia, ktoré umožnia používateľovi predpísať podmienky, pri ktorých sa cookie môžu na používateľovom stroji vytvárať a pri ktorých nie. Niektoré prehliadače dokonca umožňujú používateľovi nastaviť nie-

ktoré lokality, od ktorých je možné prijať cookie a uložiť ho na používateľovom stroji a zároveň zakazuje im prijať cookie od ostatných. Lepšie prehliadače tiež dovoľujú používateľovi vizuálnu kontrolu cookies a selektívne vymazanie tých cookies, ktoré používateľ nechce na svojom stroji.

8.5 Virtuálne privátne siete VPN

Virtuálna privátna sieť VPN (Virtual Private Network) je rozšírenie privátnej siete organizácie (intranetu) cez verejné siete, ako je napríklad Internet alebo sieť poskytovateľa internetových služieb ISP (Internet Service Provider), vytvorením bezpečného privátneho spojenia. VPN bezpečne dopraví informácie cez Internet pripojením vzdialených používateľov, pobočiek organizácie a obchodných partnerov do rozšírenej siete organizácie. VPN je **virtuálna sieť**. To znamená, že fyzická infraštruktúra sieti musí byť transparentná pre každé spojenie VPN. Vo väčšine prípadov to tiež znamená, že fyzická sieť nie je vlastnená používateľom VPN, ale je to verejná sieť spoločne používaná s mnohými ďalšími používateľmi. Na podporu potrebnej transparentnosti pre vyššie vrstvy sa používajú techniky tunelovacích protokolov. VPN je **privátna sieť**, čo v tomto kontexte znamená zaistenie privátnosti premávky prenášanej cez VPN. VPN premávka sa často vykonáva cez verejné siete a preto musia byť realizované opatrenia na zaistenie potrebnej bezpečnosti, ktorá je požadovaná pre každý jednotlivý profil premávky cez spojenie VPN. Tieto bezpečnostné požiadavky sú na šifrovanie údajov, autentizáciu pôvodu údajov, bezpečnú generáciu a včasnú obnovu kryptografických kľúčov potrebných na šifrovanie a autentizáciu a na ochranu pred útokmi znovopsielaním paketov a falšovaním adresy. VPN je **sieť** a musí byť prakticky tak chápaná a musí byť s ňou narábané ako s rozšírením sieťovej infraštruktúry organizácie. To sa týka zariadení a aplikácií, ktoré ju vytvárajú, vrátane smerovania a adresovania.

V praxi je možné rozpoznať tri charakteristické scenáre používania VPN a to je pripojenie vzdialeného používateľa k zdrojom lokálnej počátačovej sieti (intranetu) organizácie (prepojenie typu host-brána), pripojenie vzdialeného používateľa z intranetu obchodného partnera do intranetu organizácie (prepojenie typu host-host) a prepojenie lokálnej počítačovej sieti pobočky organizácie a lokálnej počítačovej sieti v hlavnom sídle organizácie (prepojenie typu brána-brána).

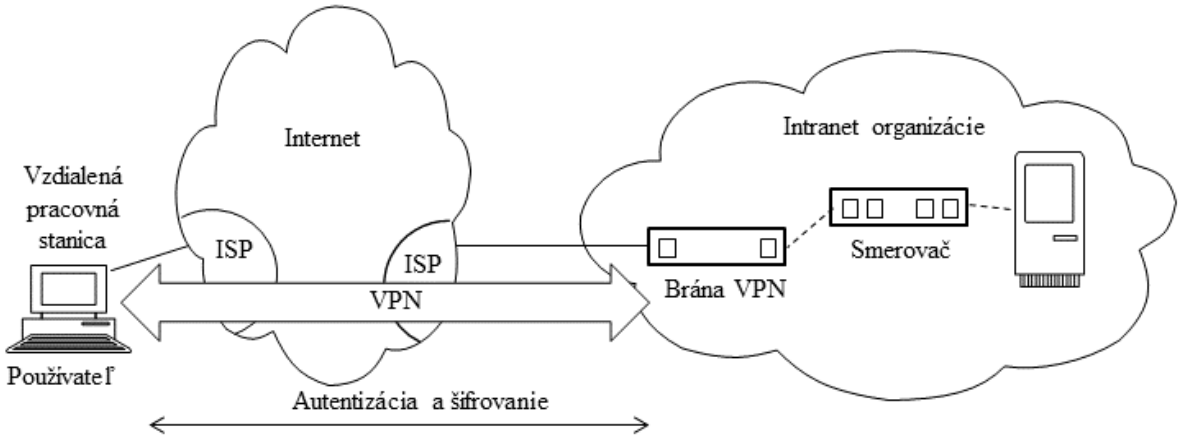
Na realizáciu bezpečného a autentizovaného prepojenia medzi koncovými uzlami VPN sa štandardne používajú bezpečnostné protokoly IPsec a SSL/TLS.

8.5.1 VPN s protokolom IPsec

Najbežnejšie používanou implementáciou protokolu IPsec je pre zriadenie sietí VPN [1]. VPN je virtuálna sieť postavená na existujúcich fyzických sieťach, ktorá môže poskytovať bezpečný komunikačný mechanizmus pre údaje prenášané medzi sieťami alebo medzi rôznymi uzlami (hostmi) v tej istej sieti. Vzdialený prístup pripojením VPN poskytuje flexibilné riešenie ako je napríklad zabezpečenie komunikácie medzi vzdialenými pracovníkmi a servermi organizácie. VPN možno vytvoriť aj v jedinej sieti tak, aby chránila obzvlášť citlivú komunikáciu pred ostatnými stranami v tej istej sieti alebo dokonca zriadila sieť spojení IPsec medzi všetkými uzlami v jednej sieti, aby sa v sieti nikdy neobjavili nezašifrované údaje.

Existujú tri primárne architektúry pre VPN založené na protokole IPsec a to prepojenie typu host-brána, prepojenie typu host-host a prepojenie typu brána-brána.

Typ prepojenia host-brána. Častou architektúrou VPN je architektúra vzdialeného prístupu. Organizácia nasadí do svojho intranetu bránu VPN a každý **používateľ so vzdialeným prístupom potom vytvorí spojenie VPN medzi svojim vzdialeným zariadením (hostom) a bránou VPN**. Vzdialený používateľ je k Internetu pripojený prostredníctvom svojho poskytovateľa internetových služieb ISP, intranet organizácie je k Internetu pripojený tiež prostredníctvom svojho ISP. Brána VPN môže byť dedikované zariadenie alebo súčasť iného sieťového zariadenia. Na Obrázku 8.23 je zobrazený príklad architektúry vzdialeného prístupu IPsec, ktorá poskytuje chránené pripojenie pre vzdialeného používateľa.



Obr. 8.23: Príklad architektúry VPN typu host-brána

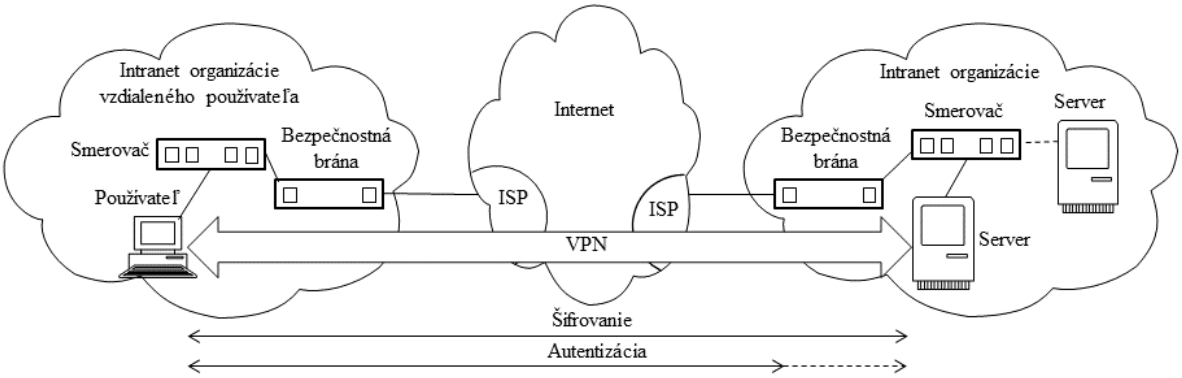
V tomto modele sa pripojenia protokolom IPsec vytvárajú podľa potreby pre každé jednotlivé vzdialené zariadenie, ktoré je konfigurované ako klient IPsec brány VPN organizácie. Ak vzdialený používateľ potrebuje použiť výpočtové prostriedky prostredníctvom siete VPN, host používateľa otvorí komunikáciu s bránou VPN. Brána VPN štandardne požiada používateľa o autentizáciu jeho identity predtým ako bude vytvorené spojenie. Brána VPN môže vykonať autentizáciu sama alebo sa obrátiť na dedikovaný autentizačný server, napríklad autentizačný server RADIUS umiestnený v štruktúre intranetu organizácie. Host vzdialeného používateľa (vzdialená pracovná stanica na Obrázku 8.23) a brána VPN si vymenia požadované údaje a vytvorí sa pripojenie IPsec. Používateľ má teraz prístup a môže používať výpočtové prostriedky organizácie. Sieťová premávka medzi hostom vzdialeného používateľa (vzdialená pracovná stanica používateľa na Obrázku 8.23) a bránou VPN bude chránená pripojením IPsec. Niektoré organizácie **nechcú prijímať všetku internetovú premávku generovanú hostom vzdialeného používateľa**. Ak vzdialený používateľ napríklad prezerá Internet, premávka cez pripojenie VPN môže byť zakázaná. Cez pripojenie VPN sa bude prenášať iba premávka pre samotnú organizáciu. Pre prístup na Internet v tomto prípade je potrebné samostatné pripojenie. Tejto skutočnosti sa hovorí **rozdelený tunel** (split tunnel) VPN. Niektoré organizácie nedôverujú vzdialeným hostom v prípade, keď hosty priamo komunikujú s Internetom prostredníctvom samostatného internetového pripojenia a súčasne sú tiež pripojení prostredníctvom VPN k intranetu organizácie. Takéto internetové pripojenie by mohlo byť **použité na útok alebo infiltráciu pripojenia VPN**. Ak má organizácia bezpečnostnú bránu s prísnymi pravidlami filtrovania, ktorá bráni neoprávnenému prístupu k počítačovým zdrojom intranetu organizácie zo strany hostov na lokálnej sieti, pravdepodobne organizácia má pravidlo zákazu obchádzania

bezpečnostnej brány pri prístupe na Internet aj pre vzdialene pripojených hostov. V takomto prípade **vzdialený host pristupuje aj k Internetu cez pripojenie VPN organizácie**, čím sa všetka sieťová premávka medzi vzdialeným hostom a bránou VPN chráni protokolom IPsec. Prijatú a dešifrovanú premávku bránou VPN, ktorá nie je určená pre zdroje intranetu organizácie, je možné odoslať na kontrolu do bezpečnostnej brány organizácie a potom ju ďalej odoslať prostredníctvom internetového pripojenia organizácie do Internetu. Podobne premávka odpovede z Internetu je poslaná späť cez bezpečnostnú bránu organizácie na bránu VPN a potom sa odosiela cez pripojenie VPN ku vzdialenému hostovi.

Ako je znázornené na Obrázku 8.23, sieť VPN so vzdialeným prístupom **neposkytuje úplnú ochranu údajov počas prenosu**. Prerušovaná čiara naznačuje, že **premávka medzi bránou a cieľovými hostmi** (napr. servermi, laptopmi, počítačmi v intranete organizácie) na pravej strane obrázku **nie je chránená**. Architektúra VPN pre vzdialený prístup sa najčastejšie používa pri pripájaní vzdialených hostov cez Internet z nezabezpečených sietí k zdrojom do zabezpečených sietí organizácie, napríklad pri pripájaní obchodného cestujúceho z externého prostredia zákazníka do centrály organizácie. Implementácia a údržba vzdialeného prístupu VPN je z hľadiska **manažmentu používateľov a hostov v podstate jednoduchá**. Brána VPN (alebo určené zariadenie) musí manažovať autorizačné údaje všetkých vzdialených zariadení (hostov) a ich oprávnených používateľov a tieto údaje sa môžu často meniť. VPN pre vzdialený prístup nie sú pre používateľov zvyčajne transparentné, pretože pred použitím VPN sa musia používatelia autentizovať. Vzdialené zariadenie používateľa musí tiež mať nakonfigurované pripojenie VPN. Niektoré zariadenia neumožňujú, aby bolo súčasne aktívnych viac ako jedno pripojenie VPN.

Typ prepojenia host-host. Architektúra VPN typu host-host sa používa z rôznych dôvodov. Z bezpečnostných dôvodov môžu niektoré hosty akceptovať iba pripojenia chránené sieťou VPN (napríklad vzdialený správca databázového servera). Vďaka tomu je pripojenie bezpečnejšie proti pokusom o neautentizovaný prístup. Ak softvér webového servera je napríklad zraniteľný voči konkrétnemu útoku, potom je tomuto útoku vystavený iba používateľom majúcim VPN prístup k serveru. Ďalším častým problémom je prítomnosť útočníkov vykonávajúcich skenovanie portov alebo slovníkové útoky proti metóde prihlásenia (napr. SSH). Pri VPN nie sú tieto porty útočníkom prístupné. V tomto prípade organizácia nakonfiguruje server tak, aby poskytoval služby VPN, a počítače správcov systému (alebo počítače iných napríklad vzdialených používateľov), aby fungovali ako klienti VPN. Správcovia systému používajú klienta VPN v prípade, keď potrebujú nadviazať chránené pripojenia k vzdialenému serveru. Obrázok 8.24 zobrazuje príklad sieťovej architektúry host-host s protokolom IPsec na zabezpečenie chráneného pripojenia vzdialeného správcu (alebo používateľa) k serveru. **Účelom pripojenia VPN typu host-host je chrániť premávku end-end t.j. z jedného konca prepojenia na druhý koniec.**

V tomto modele sa pripojenia IPsec vytvárajú podľa potreby pre každého jednotlivého vzdialeného správcu VPN alebo vzdialeného používateľa. Vzdialené hosty boli nakonfigurované tak, aby fungovali ako klienti IPsec. Ak si vzdialený používateľ alebo správca želá použiť alebo upraviť zdroje na serveri, potom host používateľa alebo správcu inicializuje komunikáciu IPsec so serverom. Tento server funguje ako server IPsec, ktorý pred nadviazaním spojenia požaduje autentizáciu identity. Host a server si vymieňajú informácie a ak je autentizácia úspešná, zriadi sa prepojenie IPsec. Používateľ alebo administrátor má teraz prístup na server a sieťová premávka medzi hostom a serverom je chránená prepojením IPsec.



Obr. 8.24: Príklad architektúry VPN typu host-host

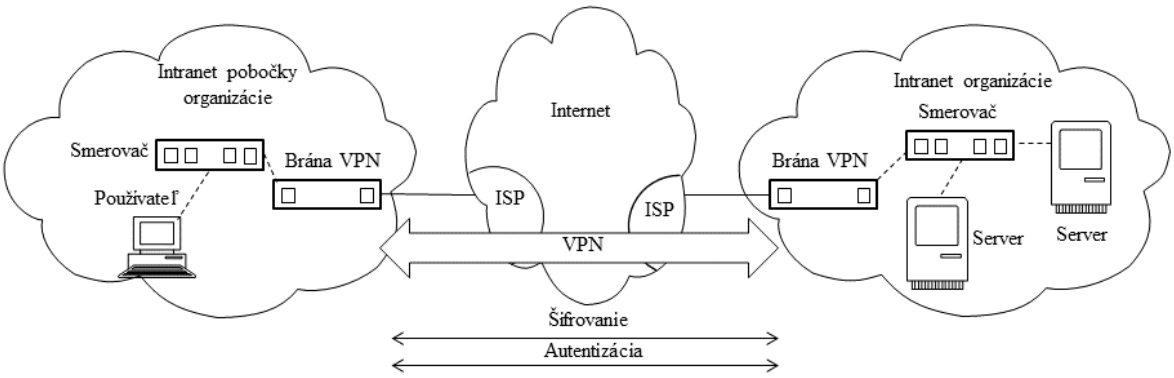
Ako je znázornené na Obrázku 8.24, **architektúra VPN typu host-host poskytuje ochranu údajov počas celého prenosu** (označené plnou čiarou). **To môže byť problém**, pretože bezpečnostné brány pracujúce na sieťovej vrstve, systémy detekcie prienikov a ďalšie **sieťové zariadenia nemôžu byť nasadené na kontrolu premávky počas prenosu**, čo v skutočnosti obchádza určité vrstvy zabezpečenia [41]. VPN typu host-host sa najčastejšie používa v prípade malého počtu dôveryhodných používateľov alebo správcov, ktorí musia pristupovať do systému zo vzdialených miest prostredníctvom nezabezpečených protokolov (napr. staršie systém) a systém je možné aktualizovať na poskytovanie služby VPN.

Manažment implementácie a údržby VPN typu host-host môže byť **náročný na zdroje pokiaľ ide o konfiguráciu**. Sieť VPN typu host-host nie je pre používateľov transparentná, pretože pred použitím siete VPN sa musia používatelia autentizovať. Všetky systémy koncových používateľov a servery, ktoré budú súčasťou sietí VPN, musia mať tiež nainštalovaný a/alebo nakonfigurovaný softvér VPN. **Architektúru typu host-host je však možné nasadiť automatizovanejším spôsobom**, ktorá na vytvorenie VPN nevyžaduje žiadnu interakciu koncového používateľa.

Špeciálnym prípadom sietí VPN typu host-host je **rozsiahle host-host nasadenie protokolu IPsec**. Zvyčajne sa to používa v prípade, keď je potrebné **zašifrovať všetky prepojenia v sieti, v cloude alebo v dátovom centre**. Vždy keď jeden host v takejto sieti potrebuje komunikovať s iným hostom v sieti, najskôr si vytvorí spojenie IPsec. Toto sa nazýva aj šifrovanie v mriežke. Zvyčajne sú tieto pripojenia IPsec spustené paketmi. Aplikácia v jednom hostovi odošle paket do druhého vzdialeného hosta. Paket z hosta odosiela kernel hosta. Kernel hosta, na ktorom je spustená aplikácia, prijme paket z aplikácie a zistí, či už nemá zriadené pripojenie IPsec k uvedenému vzdialenému hostovi, ak nie spustí zriadenie prepojenia IPsec. Po zriadení prepojenia IPsec sa paket zašifruje a odošle na vzdialeného hosta. Týmto spôsobom sa po sieti nikdy neprenáša žiadny nezašifrovaný paket. **Hosty sa navzájom autentizujú pomocou certifikátov X.509 alebo DNSSEC** (Domain Name System Security Extensions) [42]. Tieto typy autentizácie sú založené na zdieľanej dôvere: certifikačnej autorite (CA) X.509 alebo zónovom kľúči DNSSEC. Tento mechanizmus umožňuje pridanie hostov do siete bez potreby rekonfigurácie všetkých ostatných hostov, aby dostali informáciu o novo nasadenom hostovi. Jedna výhoda tohto typu architektúry IPsec je skutočnosť, že každý host je zodpovedný za svoju vlastnú ochranu. Nie sú potrebné žiadne veľké drahé brány IPsec, čo tiež znamená, že

do architektúry siete nie je pridaný jediný bod zlyhania SPF (Single Point of Failure). Hosty v sieti môžu byť nakonfigurovaní tak, aby trvali na IPsec alebo aby sa pokúsili o IPsec, ale ak zlyhajú, umožňujú komunikáciu v otvorenom texte. Túto architektúru je možné kombinovať s architektúrou typu brána-brána, kde hosty v jednej sieti môžu iniciovať protokol IPsec na hostoch v inej sieti, čím rozšíria šifrovanie sieťovej siete na obe siete. Tieto dve siete sú prepojené architektúrou typu brána-brána, takže na ich spojenie je možné naďalej používať Internet za cenu dvojnásobného šifrovania paketov, raz zavedením protokolu IPsec medzi hostmi a druhý raz nasadenie protokolu IPsec medzi bránami.

Typ prepojenia brána-brána. Na zaistenie bezpečnej sieťovej premávky **medzi dvoma intranetmi** sa často používajú virtuálne privátne siete VPN založené na protokole IPsec. Toto prepojenie sa zvyčajne realizuje **nasadením brán VPN do každej siete a vytvorením spojenia VPN medzi týmito dvoma bránami**. Premávka medzi intranetmi je bezpečná, premávka sa prenáša prostredníctvom nadviazaného spojenia VPN medzi týmito dvoma bránami VPN. Brána VPN môže byť dedikované zariadenie, ktoré vykonáva iba funkcie VPN, alebo môže byť súčasťou iného sieťového zariadenia, napríklad bezpečnostnej brány alebo smerovača. Obrázok 8.25 zobrazuje príklad sieťovej architektúry pomocou bezpečného protokolu IPsec, ktorá na zabezpečenie chráneného spojenia medzi týmito dvoma sieťami využíva model brána - brána.



Obr. 8.25: Príklad architektúry VPN typu brána-brána

Tomuto modelu je relatívne ľahko porozumieť. Na vytvorenie spojenia VPN požiada jedna brána VPN druhú bránu VPN, aby nadviazala spojenie protokolom IPsec. Tieto dve brány VPN si navzájom vymenia informácie a vytvoria spojenie IPsec. Smerovanie v každej sieti je nakonfigurované tak, že keď hosty z jednej sieti komunikujú s hostmi v druhej sieti je ich sieťová premávka automaticky smerovaná cez chránené prepojenie IPsec. Jedno prepojenie IPsec vytvára kryptograficky chránený tunel medzi bránami a podporuje všetku premávku medzi týmito dvoma sieťami, alebo viacero prepojení IPsec môže chrániť rôzne typy alebo triedy prenosov. **Brány sa navzájom prepájajú pomocou protokolu IPv4 alebo protokolu IPv6.** V prípade využitia tunelového režimu nemusí byť rodina adries IP vonkajších paketov ESP prenášaných medzi bránami rovnaká ako rodina adries IP šifrovaných paketov IP. Napríklad prepojenie IPsec medzi hostmi na adresách IPv6 1020:db8:1:2::45 a 1020:db8:1:2::23 môže použiť na prenos premávky protokol IPv4 z 192.0.2.0/24 na 198.51.100.0/24. **Tieto typy pripojení IPsec sa často nazývajú 6v4 alebo 4v6**, aby označili vnútorné a vonkajšie rodiny adries IP.

Obrázok 8.25 zobrazuje VPN typu brána-brána, ktoré **neposkytuje úplnú ochranu údajov počas celého prenosu**. V skutočnosti architektúra brána-brána chráni iba údaje medzi dvoma bránami, ktoré sú označené plnou čiarou. Prerušované čiary označujú, že premávka medzi klientmi VPN a ich lokálnou bránou a medzi vzdialenou bránou a cieľovými hostmi (napr. servermi) nie je chránená architektúrou typu brána-brána. Ostatné typy architektúr VPN poskytujú ochranu väčšej časti prenosovej cesty. Architektúra typu brána-brána sa najčastejšie používa pri prepájaní dvoch zabezpečených sietí, napríklad pri prepojení pobočky s centrálou organizácie prostredníctvom Internetu. **Z hľadiska správy používateľov a hostov je implementácia architektúry typu brána-brána najjednoduchšia**, pretože táto architektúra je pre používateľov zvyčajne transparentná a prepojenie VPN nie je pre nich viditeľné. Systémy používateľov a cieľové hosty (napr. servery) tiež nemusia mať nainštalovaný žiadny klientský softvér VPN, ani by nemali vyžadovať na používanie VPN žiadnu ďalšiu konfiguráciu.

Ak VPN typu brána-brána prepája dve rôzne organizácie, tak v prípade potreby je možné na adresáciu hostov v druhej organizácii využiť špeciálnu konfiguráciu DNS. Ak sú počítače adresované priamo adresou IP, nie je potrebné žiadne špeciálne spracovanie systémom DNS.

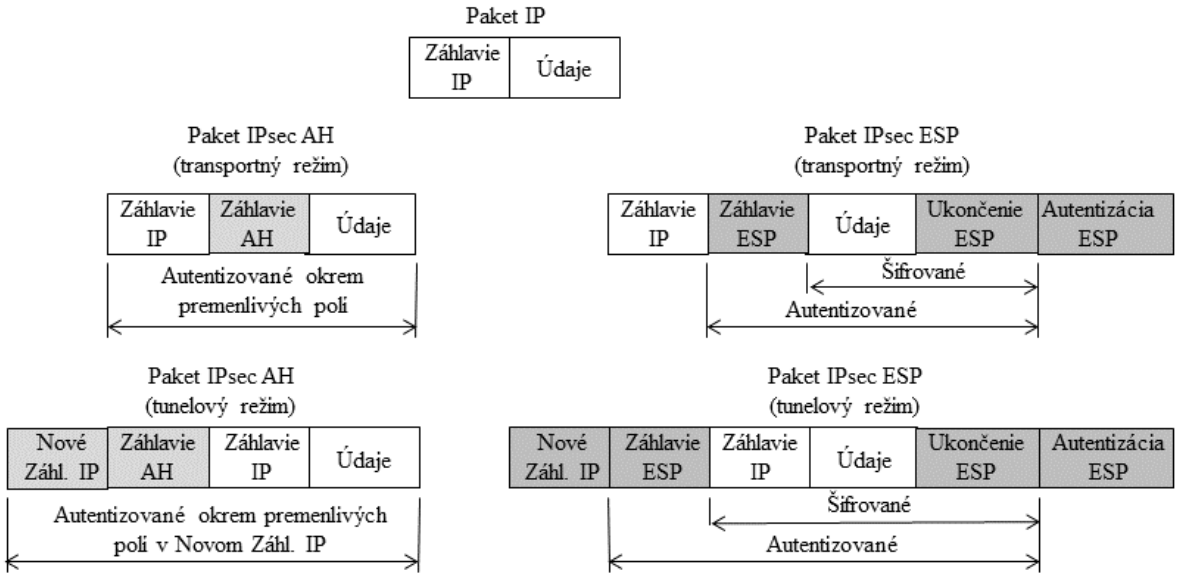
8.5.2 Protokol IPsec

Štandard IPsec, pôvodne špecifikovaný v [20, 26–28, 31–33, 38], poskytuje metódu autentizácie a ochrany údajov pri bezpečnom prenose správy. IPsec obsahuje protokol ISAKMP/Oakley (Internet Security Association a Key Management Protocol) a dva protokoly IPsec: IPsec ESP (Encapsulating Security Protocol) a IPsec AH (Authentication Header). IPsec používa na ochranu údajov symetrické šifrovacie algoritmy. Symetrické šifrovacie algoritmy sú časovo efektívnejšie a jednoduchšie sa implementujú v hardvéri. Tieto algoritmy potrebujú na zabezpečenie ochrany dát bezpečný spôsob zriadenia a výmeny šifrovacích kľúčov. Túto možnosť zabezpečujú protokoly IKE (Internet Key Exchange) ISAKMP/ Oakley. IPsec tiež obsahuje niekoľko spôsobov vytvorenia autentizačných kódov správ HMAC (Hashed Message Authentication Code), z ktorých si je možné vybrať, každý z nich poskytuje rôznu úroveň ochrany pred útokmi ako sú man-in-the-middle, znovuposlanie paketu (packet replay) a útoky na integritu údajov.

Bezpečnostné rozšírenie protokolu IP protokolom IPsec má dve možnosti: **protokoly IPsec ESP a IPsec AH**. Záhlavie **ESP** (protokol IP 50) tvorí jadro protokolu IPsec. Tento protokol, spolu s dohodnutým súborom bezpečnostných parametrov, zabezpečuje šifrovanie údajovej časti paketu (náklad paketu) a používa ďalšie ochrany (HMAC) na zaistenie integrity údajov, zaistenie proti útoku znovuposlatia paketu a útoku typu man-in-the-middle. Voliteľne môže IPsec ESP tiež zabezpečiť autentizáciu chránených údajov. Na Obrázku 8.26 je dokumentované zapúzdrenie paketu IP paketom IPsec ESP. **Protokol IPsec AH** (protokol IP 51) tvorí druhú časť IPsec. IPsec AH nezabezpečuje šifrovanie údajov bežným spôsobom, ale pridáva k údajom v pakete autentizačný kód, ktorý chráni paket pred neoprávnenou modifikáciou. Medzi chránené údaje paketu tiež možno zahrnúť nemeniteľné polia v záhlaví IP ako sú polia adresy IP. Protokol IPsec AH nezabezpečuje dôvernosť údajov, preto nemôže byť iba sám použitý v prípade, že je požiadavka na dôvernosť údajov. Na Obrázku 8.26 je dokumentované zapúzdrenie paketu IP paketom IPsec AH.

Protokol IPsec môže fungovať v dvoch režimoch vo vzťahu k prenášaniu údajov cez sieť a to v transportnom režime a v tunelovom režime. Jednotlivé režimy sa líšia v spôsobe používania

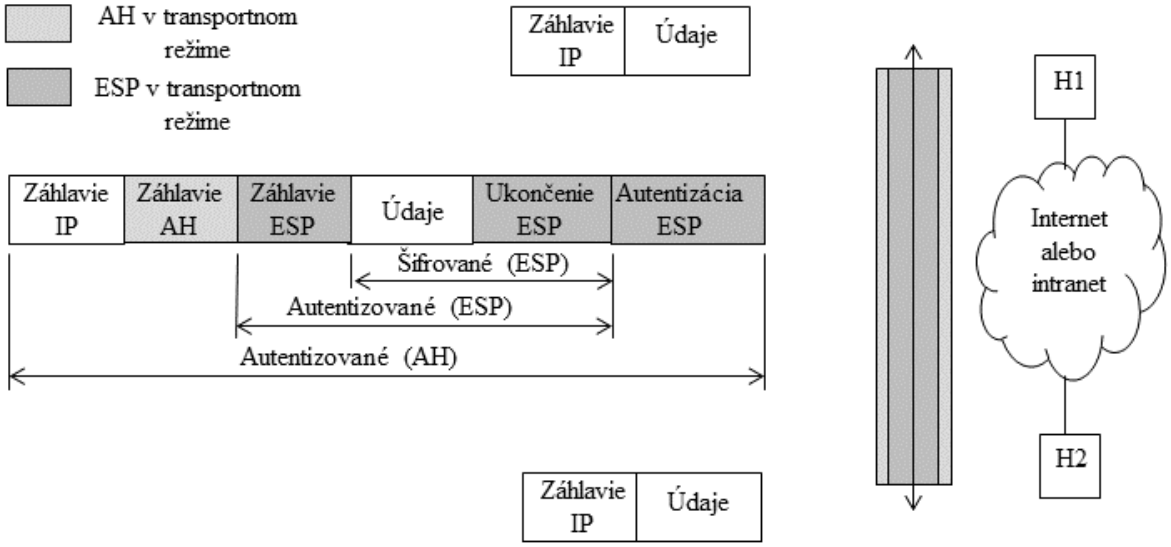
ako aj v množstve vyžadovanej réžie. **Tunelový režim** funguje tak, že celý paket IP je zapúzdrený a chránený. Pretože tunelový režim skryje aj záhlavie IP pôvodného paketu IP, pridáva sa nové záhlavie IP, aby mohol byť paket cez tunel úspešne prenesený. Šifrovacie zariadenie pozná adresy IP (začiatok a koniec tunela) v novom záhlaví a tieto adresy bývajú štandardne nastavené pri konfigurácii sieťovej brány (napríklad smerovača). Tunelový režim môže byť zriadený jedným alebo obidvomi protokolmi IPsec (ESP a AH). Výsledkom použitia tunelového režimu je rozšírenie pôvodného paketu IP asi o 20 bajtov z dôvodu zavedenia nového záhlavia IP. Tunelový režim je všeobecne považovaný za bezpečnejší a flexibilnejší než transportný režim. Tunelový režim IPsec šifruje zdrojovú a cieľovú adresu IP pôvodného paketu a teda skrýva tieto informácie na nechránenej sieti pred potecionálnym útočníkom. Na Obrázku 8.26 je dokumentované zapúzdrenie paketu IP paketom IPsec v tunelovom režime. **Transportný režim IPsec** sa zriadi tak, že do paketu IP sa za záhlavie IP vloží záhlavie ESP alebo AH. Obe adresy IP sieťových uzlov, medzi ktorými je premávka chránená IPsec, sú viditeľné v IP hlavičke aj po prípadnom šifrovaní paketu. Tento režim IPsec môže byť citlivý na útoky analýzy premávky. Pretože nie je pridané žiadne ďalšie záhlavie IP, z toho vyplýva menšie rozšírenie veľkosti paketu. Transportný režim môže byť zriadený jedným alebo oboma protokolmi IPsec ESP a AH. Na Obrázku 8.26 je dokumentované zapúzdrenie paketu IP paketom IPsec v transportnom režime.



Obr. 8.26: Formáty paketov protokolu IPsec a zabezpečenie jednotlivých častí formátu

Protokoly IPsec ESP a IPsec AH je možné použiť samostatne alebo v **kombinácii**. Vzhľadom k tomu, že každý protokol má dva režimy, existuje celý rad možných kombinácií. Aby to bolo ešte komplikovanejšie, bezpečnostné asociácie SA (Security Association - bezpečnostná asociácia je dohoda medzi dvoma entitami zapojenými do používania kryptografických prostriedkov) IPsec AH a IPsec ESP nemusia mať rovnaké koncové body. Prakticky používané sú však iba niektoré scénare. Kombinácie protokolov IPsec sú realizované s balíčkami SA a existujú dva prístupy na ich vytvorenie a to transportná priľahlosť (transport adjacency) a vnorené tunelovanie (nested tunneling). V prístupe **transportnej priľahlosti** sú oba bez-

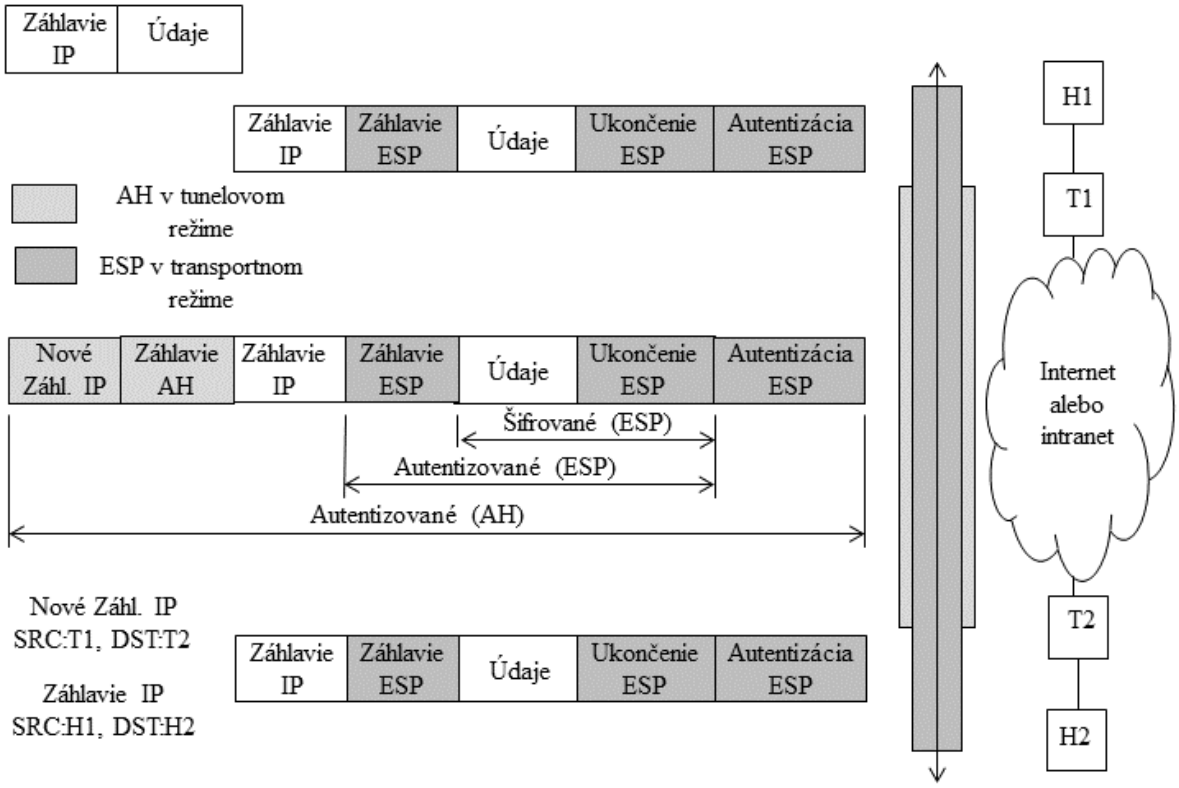
pečnostné protokoly použité v transportnom režime toho istého paketu IP. Táto metóda je praktická iba pre jednu úroveň kombinácie. Štandard IPsec stanovuje, že transportná priľahlosť susedov môže byť použitá iba spôsobom uvedeným na Obrázku č. 10.4.5 8.27. To znamená, že pre odchádzajúce pakety musí byť vykonané šifrovanie (vnútorná SA) pred autentizáciou (vonkajšia SA), zatiaľ čo pre prichádzajúce pakety sa musí autentizácia vykonať pred šifrovaním. Toto je logická následnosť a tiež šetrí zaťaženie systému dešifrovaním v prípade, keď skorej zlyhá autentizácia paketu (a teda dešifrovanie sa nemusí vykonať). V prístupe **vnoreného tunelovania** (nested tunneling) sú oba bezpečnostné protokoly aplikované za sebou. Po každom aplikovaní je vytvorený nový paket IP a na tento paket je aplikovaný ďalší protokol. Táto metóda nemá žiadne obmedzenia na počet vnorených úrovní. Ale viac ako tri úrovne vnorenia sú nepraktické. Na Obrázku č. 10.4.6 8.28 je príklad vnoreného tunelovania. Najprv sa na paket IP aplikuje protokol IPsec ESP v transportnom režime a následne protokol IPsec AH v tunelovom režime.



Obr. 8.27: Použitie protokolu IPsec na transportnú priľahlosť

Na implementáciu riešenia VPN so šifrovaním je nevyhnutná **pravidelná výmena relačných šifrovacích kľúčov**. Zanedbanie výmeny relačných kľúčov môže spôsobiť zraniteľnosť šifrovaných údajov prenášaných VPN na útok hrubou silou. IPsec rieši tento problém protokolom IKE [25], ktorý využíva ďalšie dva protokoly na autentizáciu entít využívajúce kryptografické prostriedky (krypto entity) a na generovanie kľúčov. IKE využíva matematický algoritmus Diffie-Hellmanovej výmeny kľúčov na generovanie symetrických relačných kľúčov, ktoré sú potom použité krypto entitami. IKE tiež riadi dojednanie ďalších bezpečnostných parametrov ako je výber chránených údajov, sila kľúčov, použité hešovacie funkcie a či pakety chrániť pred znovuposielaním. Protokol ISAKMP bežne používa port UDP 500 ako zdrojový a cieľový port.

Bezpečnostná asociácia SA (Security Association) je dohoda medzi dvomi krypto entitami. Táto dohoda zahrňuje typ a silu šifrovacieho algoritmu použitého na ochranu údajov. SA zahrňuje metódu a silu autentizácie údajov a metódu vytvárania nových kľúčov pre túto ochranu údajov. Krypto entity sú vytvorené podľa ďalej uvedeného opisu.



Obr. 8.28: Použitie protokolu IPsec na vnorené tunelovanie

Každá SA má stanovenú **dobu životnosti**, počas ktorej je SA považovaná za platnú. Životnosť je meraná v **jednotkách času existencie SA** (v sekundách) a v **jednotkách objemu prenesených údajov** (počet bajtov). Životnosť je dohodnutá pri vytvorení SA. Tieto dve životnosti sú kontrolované a vypršanie jednej z nich zneplatní aktuálnu SA. Za bežných okolností časová životnosť uplynie skorej ako objemová životnosť. V prípade, že sledovaný paket vyhovuje SA v záverečných 120 sekundách životnosti aktuálneho SA, je štandardne vyvolaný proces vytvorenia nových relačných kľúčov. Proces vytvorenia nových relačných kľúčov zriadi novú aktuálnu SA predtým než sa zruší stará SA. Výsledkom je plynulý prechod zo starej SA na novú SA s minimálnou stratou paketov v novej SA.

ISAKMP SA je jeden obojsmerný bezpečný dojednávací kanál používaný oboma krypto entitami na poslanie dôležitých bezpečnostných parametrov entity, ako sú bezpečnostné parametre pre IPsec SA (údajový tunel). Štandardné politiky ISAKMP SA majú predvolenú hodnotu životnosti 86 400 sekúnd (24 hodín) bez limitu na objem prenesených údajov.

IPsec SA je jednosmerný komunikačný kanál od jednej krypto entity do druhej krypto entity. Skutočné údaje zákazníka prechádzajú iba IPsec SA a nikdy nie cez ISAKMP SA. Každá strana IPsec tunela má pár IPsec SA na spojenie: jeden do vzdialenej krypto entity a druhý zo vzdialenej krypto entity. Tieto informácie o páre IPsec SA sú uložené lokálne v databáze SA. Štandardné politiky IPsec SA majú predvolenú životnosť 3 600 sekúnd (1 hodinu) a objemovú životnosť 4 608 000 kB.

Prvá fáza IKE predstavuje počiatočné dojednanie obojsmerného ISAKMP SA medzi dvoma krypto entitami. Táto fáza sa často nazýva **hlavný režim**. Prvá fáza IKE začína vzájomnou autentizáciou krypto entít. Po úspešnej autentizácii sa krypto entity dohodnú na šifrovacom algoritme, hešovacej funkcii a ďalších parametroch, potrebných na vytvorenie ISAKMP SA. Komunikácia medzi dvomi krypto entitami môžu byť predmetom odchytenia útočníkom, ale útočník má minimálnu šancu odhaliť šifrovací kľúč. ISAKMP SA je použitá procesom IKE na dojednanie bezpečnostných parametrov pre IPsec SA. Tieto informácie ISAKMP SA sú uložené lokálne v databáze SA každej krypto entity.

Prvá fáza IKE má tri možné autentizačné metódy:

- **Predvolený spoločný kľúč PSK** (Pre-Shared Key). Predvolený spoločný kľúč je správcom preddefinovaný reťazec kľúča vložený ručne do každej krypto entity a slúži na vzájomnú identifikáciu. Pomocou PSK sú schopné dve krypto entity dojednať a vytvoriť ISAKMP SA. PSK zvyčajne obsahuje adresu IP hosta alebo podsiete a masku, ktorá je platná pre daný PSK.
- **Infraštruktúra verejného kľúča PKI** (Public Key Infrastructure) pomocou digitálnych certifikátov X.509. Súčasťou certifikátu je názov, sériové číslo, doba platnosti a ďalšie informácie, ktoré môže zariadenie IPsec použiť na určenie platnosti certifikátu. Certifikáty môžu byť tiež zrušené, čo zariadenie IPsec odmietne na možnosť úspešnej autentizácie.
- **Náhodné čísla šifrované RSA.**

Na podporu premávky medzi krypto entitami cez NAT (Network Address Translator) alebo PAT (Port Address Translator) zariadenia sa v sieti zavádza uzol IPsec **NAT-T** (Network Address Translator - Transparency), ktorý zapúzdruje krypto pakety do obalu UDP a takto umožňuje paketom prejsť zariadeniami NAT alebo PAT. NAT-T je automaticky dojednané medzi dvoma krypto entitami počas dojednávania ISAKMP s cieľovým portom UDP 4500. Za zdrojový port sa používa nasledujúci vyšší dostupný port. Ak je použitý port UDP 4500, potom sa cieľový port posunie na port UDP 4501, 4502 a tak ďalej, až pokiaľ nie je zriadená relácia ISAKMP. NAT-T je definovaný v [29].

V druhej fáze IKE sú procesom IKE pomocou obojsmernej ISAKMP SA dojednané asociácie IPsec SA. Táto fáza sa často nazýva **rýchly režim**. Asociácie IPsec SA sú vo svojej podstate **jednosmerné**, čo spôsobuje, že je oddelená výmena kľúča pre tok údajov od krypto entity a pre tok údajov do krypto entity. Výhodou tejto stratégie je to, že **údaje prenášané jedným smerom sú šifrované iným kľúčom ako údaje prenášané opačným smerom**. To pre potenciálneho útočníka znamená dvojnásobnú námahu pri snahe dešifrovať odchytené zašifrované údaje. Počas procesu dojednania v rýchlom režime sa krypto entity dohodnú na kryptografickom súbore, hešovacích funkciách a ostatných parametroch.

8.5.3 VPN s protokolom SSL/TLS

VPN s protokolom SSL/TLS poskytuje bezpečný vzdialený prístup ku zdrojom organizácie [11]. VPN sa skladá z jedného alebo viacerých zariadení VPN, ku ktorým sa používatelia pripájajú pomocou svojich webových prehliadačov. **Komunikácia medzi webovým prehliadačom a**

zariadením VPN je šifrovaná protokolom SSL/TLS. VPN poskytujú vzdialeným používateľom prístup k webovým aplikáciám a aplikáciám klient/server a k pripojeniu k zdrojom intranetu organizácie. Ponúkajú všestrannosť a jednoduché použitie, pretože **používajú protokol SSL/TLS, ktorý je súčasťou všetkých štandardných webových prehliadačov**, takže klient zvyčajne nevyžaduje konfiguráciu hosta používateľa. Medzi typických používateľov VPN patria ľudia pracujúci z domu, mobilní používatelia, obchodní partneri a zákazníci. Medzi hardvérových klientov patria rôzne typy zariadení, napríklad verejné kiosky, domáce osobné počítače (PC), PDA alebo inteligentné telefóny. Pripojenie prostredníctvom VPN je možné používať všade tam, kde je internetová konektivita, a používateľ má webového klienta schopného používať konkrétne pripojenie VPN. **Celá premávka je šifrovaná**, pretože prechádza aj verejnými sieťami ako je napríklad Internet. **Brána VPN je koncovým bodom bezpečeného pripojenia** a poskytuje rôzne služby a funkcie (väčšina brán VPN s protokolom SSL/TLS je samostatným hardvérovým zariadením, aj keď na serveroch poskytujúcich služby používateľom sú nainštalované softvérové riešenia takejto brány). Poskytovanie bezpečného vzdialeného prístupu širokej škále používateľov a zariadení na mnohých miestach vyžaduje rozmanitú sadu služieb a funkcií VPN. Väčšina VPN má jednu alebo viacero z nasledujúcich troch základných funkcií a to proxovanie, aplikačný preklad a rozšírenie siete.

Proxovanie. Proxy je sprostredkovateľské zariadenie alebo program, ktoré **sprostredkuje komunikáciu a ďalšie služby medzi klientom a serverom**. Z pohľadu klienta vystupuje proxy ako server a z pohľadu servera vystupuje proxy ako klient. Serverová časť proxy môže interne obsluhovať požiadavky alebo prekladať informácie a prenášať ich prostredníctvom klientskej časti proxy na ďalšie servery. Proxovanie je hlavnou funkciou portálu VPN s protokolom SSL/TLS. Najjednoduchšia forma portálu VPN s protokolom SSL/TLS spočíva v bezpečnom proxovaní webových stránok. Portál VPN s protokolom SSL/TLS funguje ako brána sprostredkujúca premávku medzi používateľom a aplikáciou. Proxy prijme požiadavku od používateľa, pripojí sa k webovému serveru, stiahne informácie a prostredníctvom pripojenia SSL/TLS ich odosiela späť používateľovi. Proxy vykonáva šifrovanie alebo dešifrovanie a kontrolu obsahu každého paketu, čo spôsobuje mierne znížený výkon.

Aplikačný preklad. Aplikačný preklad konvertuje informácie z jedného protokolu do druhého. Často sa používa na konverziu starého alebo proprietárneho protokolu na používanejší alebo štandardný protokol. Používa sa tiež na uľahčenie integrácie systému a komunikácie medzi aplikáciami a zariadeniami. Aplikačný preklad využíva proxovanie na komunikáciu s oboma stranami spojenia pomocou príslušného protokolu. Portál VPN s protokolom SSL/TLS používajú aplikačný preklad pre aplikácie, ktoré nemajú webový prístup. Tento koncept umožňuje používateľom používať webový prehliadač na prístup k aplikáciám, ktoré nemajú vlastné webové rozhranie. Napríklad na zabezpečenie prístupu k súborovému serveru prostredníctvom portálu VPN by portál VPN komunikoval so súborovým serverom pomocou príslušného protokolu, ako je napríklad Common Internet File System (CIFS) alebo File Transfer Protocol (FTP), a preložil by informácie do webového formátu, aby používatelia mohli tieto informácie zobraziť pomocou webového prehliadača. Aplikačný preklad vyžaduje modul prekladača pre každý podporovaný protokol.

Rozšírenie siete. Rozšírenie siete je metóda poskytovania čiastočného alebo úplného **prístupu do siete vzdialeným používateľom**. Vzdialení používatelia sa môžu pripojiť k sieti a získať prístup k interným zdrojom siete rovnako akoby sa fyzicky nachádzali v lokálnej sieti organizácie. Tento koncept eliminuje potrebu vytvárania špecifických webových portá-

lov pre všetky aplikácie vyžadujúce vzdialený prístup. Sieťové rozšírenie prostredníctom VPN poskytuje bezpečné pripojenie zo systému používateľa do vnútornej siete organizácie. Tento tunel typu host-brána dokáže spracovať ľubovoľnú premávku rovnako ako to dokáže architektúra typu host-brána pre VPN s protokolom IPsec. Tento typ architektúry VPN je rovnaký ako je na Obrázku 8.23. Zariadenia pre tunel VPN s protokolom SSL/TLS môžu podporovať plné alebo rozdelené tunelovanie. **Plné tunelovanie** spôsobí, že všetka sieťová premávka bude prechádzať tunelom do organizácie. **Rozdelené tunelovanie** smeruje premávku špecificky určenú zdrojom lokálnej siete organizácie k týmto zdrojom, ale ostatnú premávku smeruje na predvolenú bránu vzdialeného používateľa. Takéto rozšírenie siete vyžaduje nainštalovanie klienta buď ako plug in do webového prehliadača používateľa alebo ako program do systému používateľa, čo vyžaduje administratívny prístup k systému používateľa. Klient je zvyčajne agent s aktívnym obsahom (vykonateľný kód), takže systém musí mať schopnosť načítať agenta a musí mať tiež potrebné privilégiá na jeho spustenie. Táto skutočnosť môže spôsobiť problémy vo verejných systémoch, v ktorých používatelia nemusia mať tieto oprávnenia, a v spravovaných systémoch, v ktorých bezpečnostná politika bráni inštalácii takýchto appletov a opatreniam. Obmedzenejšou formou rozšírenia siete sa niekedy nazýva presmerovanie portov.

Tieto tri základné funkcie umožňujú VPN s protokolom SSL/TLS vytvoriť bezpečený vzdialený prístup k rôznym aplikáciám. Produkty VPN sa líšia v kvalite a efektívnosti na základe spôsobu akým produkty implementujú tieto tri základné funkcie. Produkty VPN môžu napríklad ponúkať prostredníctvom proxy a aplikačného prekladu podporu pre rôzne protokoly. Iné produkty môžu ponúkať väčšiu alebo menšiu kontrolu sieťového prístupu pre rozšírenie siete. Pri hodnotení produktov VPN je dôležité identifikovať potreby vzdialeného prístupu a obsluhované aplikácie. Je zaujímavé klasifikovať funkcie VPN s protokolom SSL/TLS podľa typov prepojenia VPN s protokolom IPsec. Funkciu VPN s protokolom SSL/TLS proxovanie je možné podľa VPN s protokolom IPsec klasifikovať ako typ prepojenia host-brána alebo host-host, v závislosti kde končí tunel SSL/TLS. Funkciu aplikačný preklad je možné klasifikovať ako typ host-brána. Funkciu rozšírenie siete je možné klasifikovať ako typ host-brána alebo host-host v prípade, že medzi dvomi intranetmi je vytvorený prostredníctvom brán tunel s protokolom SSL/TLS.

8.5.4 Protokol SSL/TLS

Protokol SSL vyvinula spoločnosť Netscape. Jeho verzia 3 bola publikovaná ako predbežný internetový dokument. (Ako historický dokument bol tento protokol opísaný v [18]). Následne vznikla v rámci IETF (Internet Engineering Task Force, iniciatívna skupina špecialistov navrhujúca štandardy pre Internet) pracovná skupina TLS (Transport Layer Security) a navrhla spoločný štandard. Prvú publikovanú verziu TLS možno chápať v podstate ako SSL v3.1, ktorá je spätne kompatibilná s SSL v3. V tejto časti bude opísaná základná charakteristika protokolu SSL v3 a na záver hlavné rozdiely medzi SSL v3 a TLS [6–8].

Protokol TCP nezabezpečuje spoľahlivú bezpečnostnú službu medzi komunikujúcimi koncovými entitami (bezpečnosť end-end). Preto bolo nevyhnutné nad protokolom TCP v transportnej vrstve navrhnúť ďalší protokol SSL tak, aby protokol TCP bol schopný zabezpečovať spoľahlivú bezpečnú komunikáciu dvoch koncových entít. Samotný protokol SSL nie je jediný protokol, ale predstavuje dve vrstvy protokolov. Na nižšej vrstve je protokol SSL Record Protocol (poskytuje základné bezpečnostné služby rôznym protokolom na vyššej úrovni, ako je napríklad protokol HTTP) a na vyššej vrstve sú protokoly SSL Alert Protocol, SSL Change

Cipher Spec Protocol a SSL Handshake Protocol (špecifické protokoly SSL a sú využité pri manažmente SSL výmen).

Koncepcia protokolu SSL predpokladá reláciu SSL a spojenie SSL, ktoré sú definované takto:

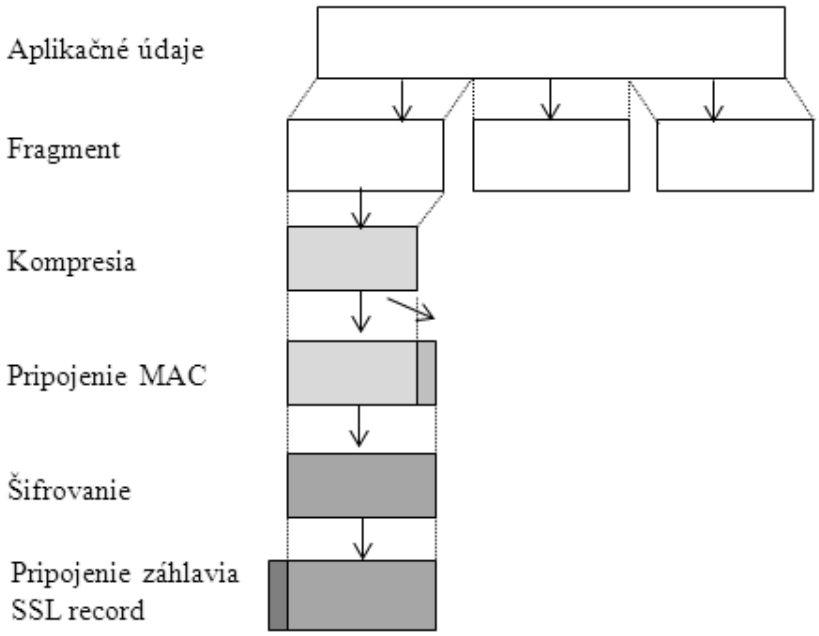
- **Spojenie SSL** je transport (podľa definície vrstvového modelu OSI), ktoré zabezpečuje vhodný typ služieb. Pre SSL toto spojenie zodpovedá spojeniu odpovedajúcich si entít (správy medzi koncovými uzlami SSL). Spojenia sú dočasné. Každé spojenie je asociované s jednou reláciou.
- **Relácia SSL** je asociácia medzi klientom a serverom. Relácie sú vytvárané prostredníctvom protokolu SSL Handshake Protocol. Relácie definujú množinu kryptografických bezpečnostných parametrov, ktoré môžu byť spoločné medzi viacerými spojeniami. Relácie sa využívajú na to, aby sa zamedzilo náročnému dohadovaniu nových bezpečnostných parametrov pre každé spojenie.

SSL Record Protocol je protokol, ktorý zabezpečuje dve služby pre spojenia SSL a to **dôvernosť a integritu správy**. **SSL Handshake Protocol definuje spoločné tajné kľúče**, ktoré sú využité pri symetrickom šifrovaní údajov nákladu SSL a pri tvobe autentizačného kódu správy MAC (Message Authentication Code). Na Obrázku 8.29 je zobrazená celková funkcionalita protokolu SSL Record Protocol. Tento protokol pri vysielaní v začiatočnom uzle SSL zabezpečuje prevzatie aplikačnej správy, vykoná fragmentáciu správy do zvládnuteľných blokov, voliteľne vykoná kompresiu údajov bloku, určí autentizačný kód bloku MAC, blok s pripojeným autentizačným kódom zašifruje, pridá záhlavie SSL a vyšle ho v TCP segmente. Prijatý TCP segment v koncovom uzle SSL je potom podľa protokolu SSL Record Protocol spätne dešifrovaný, je verifikovaný MAC bloku, voliteľne je blok dekompresovaný a fragmenty sú zložené do správy pre aplikáciu.

Change Cipher Spec Protocol je najjednoduchší zo špecifických protokolov SSL a používa ho protokol SSL Record Protocol. **Pozostáva z jedinej správy** a z jediného bajtu s hodnotou 1. Účelom tejto správy je spôsobiť preklopenie pripravenej množina šifrovacích nástrojov (predtým dohodnutej protokolom SSL Handshake Protocol) do aktuálneho stavu a začať používať novú množinu šifrovacích nástrojov v danom spojení.

Alert Protocol je využitý pri prenose **výstražných správ SSL do odpovedajúcej entity**. Podobne ako pri aplikačnej správe aj výstražné správy sú komprimované a šifrované podľa nastaveného aktívneho stavu. Každá správa v tomto protokole sa skladá z dvoch bajtov. Prvý bajt vyjadruje závažnosť správy a má hodnotu varovanie (warning) alebo fatálne (fatal). Ak je závažnosť správy fatálne, potom SSL okamžite ukončí spojenie, v ktorom vznikla situácia fatálne. Ostatné spojenia relácie, v ktorom je spojenie so situáciou fatálne, môžu pokračovať, ale v tejto relácii nemôže byť zriadené žiadne nové spojenie.

Najkomplexnejšou časťou SSL je protokol **SSL Handshake Protocol**. Tento protokol **umožňuje vzájomnú autentizáciu klienta a servera, umožňuje dojednanie šifrovacieho algoritmu, algoritmu na výpočet autentizačného kódu správy a kryptografických kľúčov použitých na ochranu údajov v SSL protokole**. Protokol SSL Handshake Protocol sa vykoná pred prenosom aplikačných údajov. SSL Handshake Protocol pozostáva z výmeny správ medzi klientom a serverom. Správy sú zoskupené do štyroch fáz. Na Obrázku



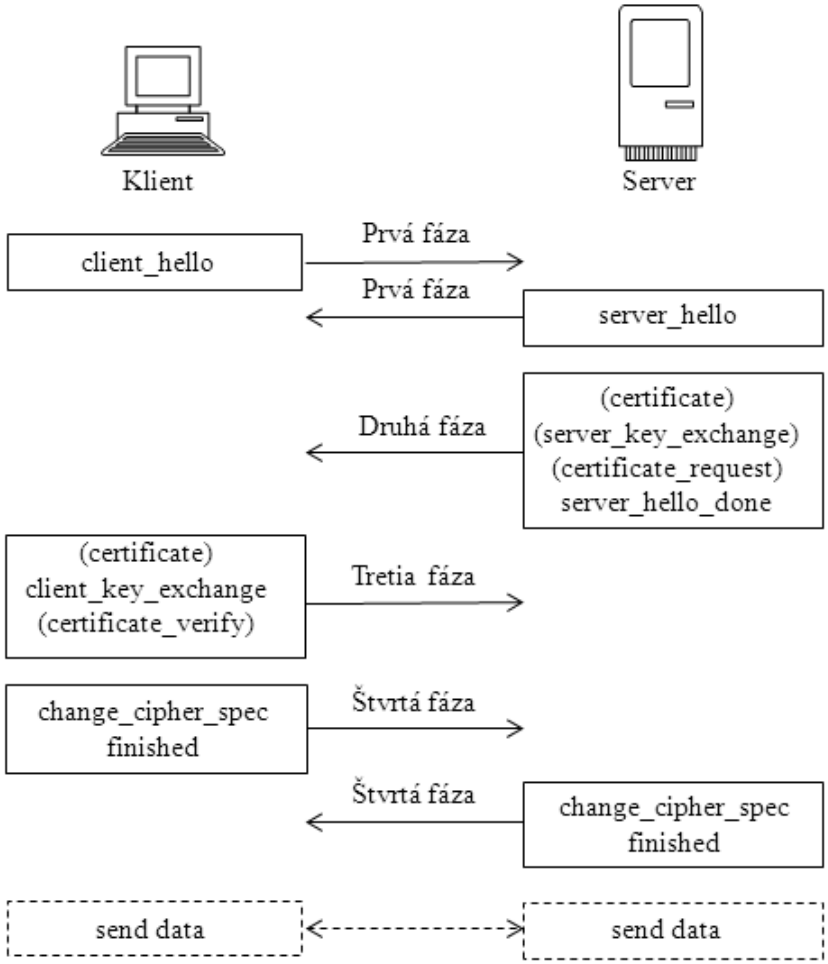
Obr. 8.29: Prenos údajov protokolom SSL Record Protocol

8.30 je zobrazená postupnosť výmeny správ. Správy v zátvorkách sa vymieňajú voliteľne alebo závisia na konkrétnej situácii a správy nie sú vždy poslané.

Prvá fáza – Zriadenie bezpečnostných funkcií. Táto fáza slúži na nadviazanie logického spojenia a na zriadenie bezpečnostných funkcií, ktoré budú s ním spojené. Túto fázu inicializuje klient, ktorý posiela správu **client_hello** s parametrami verzia (najvyššia verzia SSL podporovaná klientom) a náhodné číslo (klientom vytvorené náhodné číslo pozostávajúce z 32 bitovej hodnoty času a dátumu a 28 bajtov vytvorených náhodným generátorom, využíva sa pri výmene kľúčov proti útokom typu znovuprehratie). Na správu client_hello odpovedá server správou **server_hello**, ktorá obsahuje rovnaké parametre ako správa client_hello. Interpretácia parametrov správy server_hello je takáto. Pole verzia obsahuje nižšiu verziu z verzií navrhnutej klientom a najvyššou verziou podporovanou serverom, náhodné číslo je vytvorené serverom rovnakým spôsobom nezávisle na náhodnom čísle klientovej správe. Ak pole ID relácie (SessionID) klienta bolo nenulové, potom takú istú hodnotu použije aj server, v opačnom prípade pole ID relácie servera obsahuje hodnotu pre novú reláciu. Pole šifrovacia suita (CipherSuite) obsahuje jednu serverom vybratú šifrovaciu suitu zo šifrovacej suity navrhnutej klientom. Pole kompresie (Compression) obsahuje kompresnú metódu zvolenú serverom z metód navrhnutých klientom.

Prvým elementom v parametroch šifrovacej suity je **metóda výmeny kľúčov** (spôsob, ktorým sa dojedná výmena kryptografických kľúčov pre symetrické šifrovanie a MAC). Sú podporované tieto výmeny kľúčov:

- **RSA** – tajný kľúč je zašifrovaný verejným RSA kľúčom príjemcu. Musí byť k dispozícii certifikát verejného kľúča príjemcu.



Obr. 8.30: Výmena správ v SSL Handshake Protocol

- Pevný Diffie-Hellman (D-H) – táto D-H výmena kľúča predpokladá, že server má certifikát verejného kľúča, ktorý obsahuje verejné D-H parametre (prvočíslo a primitívny koreň) a verejný **D-H kľúč.** Klient poskytne svoje parametre verejného D-H kľúča v certifikáte, ak sa požaduje autentizácia klienta, alebo v správe výmeny kľúča. Táto metóda poskytuje pevný tajný kľúč medzi komunikujúcimi entitami, nakoľko je tajný kľúč vypočítaný z pevných verejných D-H kľúčov entít.

- **Dočasný D-H** – táto D-H výmena kľúča poskytuje vytvorenie dočasného (jednorázového) tajného kľúča. V tomto prípade sú verejné D-H parametre a verejné D-H kľúče vymenené a podpísané odosielateľovým privátnym kľúčom RSA alebo DSS. Príjemca môže verifikovať podpis pomocou odpovedajúceho verejného kľúča z certifikátu. Táto výmena kľúča je najbezpečnejšia, pretože poskytuje dočasný (jednorázový) autentizovaný tajný kľúč.

- **Anonymný D-H** – používa D-H algoritmus výmeny kľúča bez autentizácie komunikujúcich entít. To znamená, že každá entita posiela svoje D-H parametre bez autentizácie. Tento spôsob výmeny kľúča je zraniteľný na útok man-in-the-middle, pri ktorej útočník

realizuje anonymnú výmenu kľúča s obidvomi entitami (sprostredkováva komunikáciu entít).

- **Fortezza** – technika definovaná v schéme Fortezza.

Druhá fáza – Autentizácia servera a výmena kľúča. Túto fázu začne server poslaním svojho certifikátu, ak je potreba jeho autentizácie. Správa **certificate** je vyžadovaná pre každú metódu výmeny kľúčov s výnimkou anonymného D-H. Ako ďalšia správa môže byť poslaná správa **server_key_exchange**, pokiaľ sa to požaduje. Nie je to požadované v prípade, keď server poslal certifikát s pevnými D-H parametrami alebo bude použitá výmena kľúčov RSA. Správa server_key_exchange je potrebná v týchto prípadoch:

- **Anonymný D-H.** Správa obsahuje dva verejné D-H parametre (prvočíslo a primitívne koreň tohto čísla) a verejný D-H kľúč servera.
- **Dočasný D-H.** Správa obsahuje dva verejné D-H parametre (prvočíslo a primitívny koreň tohto čísla), verejný D-H kľúč servera spolu s podpisom týchto troch parametrov.
- Výmena kľúča RSA (server používa RSA, ale má iba podpisovací kľúč RSA). To znamená, že klient nemôže jednoducho poslať tajný kľúč zašifrovaný verejným kľúčom servera. Namiesto toho musí server vytvoriť dočasný kľúčový pár (verejný a privátny kľúč) RSA a použiť správu server_key_exchange na odoslanie verejného kľúča. Správa obsahuje dva parametre dočasného verejného kľúča RSA (exponent a modul) a podpis týchto parametrov.
- **Fortezza.**

Neanonymný server (server nepoužíva anonymný D-H) môže klienta požiadať o certifikát. Správa **certificate_request** obsahuje dva parametre, a to typ certifikátu a certifikačné autority. Typ certifikát udáva algoritmus verejného kľúča a jeho použitie. Napríklad RSA (algoritmus)/iba na podpis (použitie), RSA/pre pevný D-H (v tomto prípade je podpis použitý iba na autentizáciu), RSA/dočasný D-H. Druhý parameter v správe certificate_request je zoznam názvov akceptovateľných certifikačných autorít. Záverečná správa v druhej fáze, ktorá sa vždy vyžaduje, je správa servera **server_done**. Po odoslaní tejto správy bude server čakať na klientovu odpoveď. Táto správa neobsahuje žiadne parametre.

Tretia fáza – Autentizácia klienta a výmena kľúča. Po prijatí správy **server_done** by klient mal overiť, či server predložil platný certifikát (ak sa požaduje) a skontrolovať, či sú akceptovateľné parametre správy **server_hello**. Ak je všetko akceptovateľné, klient pošle späť serveru jednu alebo viacero správ. Ak server požadoval certifikát, klient začne túto fázu zaslaním správy **certificate**. Ak klient nemá k dispozícii vhodný certifikát, pošle serveru namiesto certifikátu varovanie **no_certificate**.

Ďalej nasleduje správa **client_key_exchange**, ktorá musí byť poslaná v tejto fáze. Obsah správy závisí od typu výmeny kľúča takto:

- **RSA.** Klient vygeneruje 48 bajtové pre-master tajomstvo, ktoré následne zašifruje pomocou verejného kľúča zo serverovho certifikátu alebo dočasného kľúča RSA zo správy server_key_exchange.

- **Dočasný alebo anonymný D-H.** Sú poslané klientove verejné parametre D-H.
- **Pevný D-H.** Verejné parametre D-H klienta boli poslané v správe certificate, takže obsah tejto správa je prázdny.
- **Fortezza.** Pošlú sa klientove parametre Fortezza.

Nakoniec v tejto fáze môže klient poslať správu **certificate_verify** na potvrdenie explicitnej verifikácie klientovho certifikátu. Táto správa je poslaná iba ako následná po akomkoľvek klientskom certifikáte, ktorý má funkciu podpisovania (t.j. všetky certifikáty s výnimkou tých, ktoré obsahujú pevné D-H parametre). Táto správa obsahuje podpis zreťazených predchádzajúcich správ. Ak privátny kľúč klienta je pre algoritmus DSS, potom sa používa algoritmus SHA-1 na vypočítanie hešovacej hodnoty zreťazených predchádzajúcich správ. Ak privátny kľúč klienta je pre algoritmus RSA, potom sa za hešovaciu hodnotu zoberie zreťazenie hešovacích hodnôt vypočítaných zo zreťazených predchádzajúcich správ algoritmom MD5 a SHA-1. V každom prípade je účelom overiť, že klient vlastní súkromný kľúč pre verejný kľúč z certifikátu klienta. Aj keby niekto zneužíval certifikát klienta, nie je schopný zabezpečiť podpis, pretože nemá súkromný kľúč klienta.

Štvrtá fáza – Ukončenie. Táto fáza ukončí vytvorenie bezpečeného spojenia. Klient pošle správu **change_cipher_spec** a skopíruje pripravenú šifrovaciu suitu (CipherSpec) do aktuálnej šifrovacej suity. Stojí za zmienku, že táto správa nie je súčasťou protokolu SSL Handshake Protocol, ale je poslaná pomocou protokolu Change Cipher Spec Protocol. Po tejto správe klient bezprostredne pošle správu **finished** podľa novej šifrovacej suity. Táto správa potvrdzuje, že výmena kľúča a autentizačné procesy boli úspešné. Ako odpoveď na tieto dve správy klienta pošle server vlastnú správu **change_cipher_spec**, skopíruje pripravenú šifrovaciu suitu (CipherSpec) do aktuálnej šifrovacej suity, a pošle správu **finished**. V tomto bode je dohodnutie šifrovacej suity ukončené a klient a server môžu začať výmenu údajov na aplikačnej vrstve.

Protokol TLS je štandardizačná iniciatíva IETF, ktorej cieľom je vytvorenie verzii internetového štandardu protokolu SSL. Verzia TLS 1.2 je definovaná v internetovom štandarde [8], ktorý je veľmi podobný SSL v3. Ďalej sa poukáže na **niektoré ich rozdiely**. Formát správy protokolu SSL Record Protokol je v TLS rovnaký. Jediný **rozdiel je v hodnotách verzií**, pre aktuálnu verziu TLS je hodnota vyššej verzie 3 a hodnota nižšej verzie je tiež 3. **Pri výpočte autentizačného kódu správy MAC existujú** medzi SSL v3 a TLS **dva rozdiely, a to v používanom algoritme a rozsahu údajov, z ktorých sa počíta autentizačný kód**. TLS používa algoritmus HMAC definovaný v [30]. **TLS podporuje všetky výstražné kódy protokolu Alert Protocol definované vo SSL v3 s výnimkou varovania no_certificate. V TLS sú definované ďalšie výstražné kódy najmä typu fatálne.** V šifrovacích suitách existuje niekoľko malých rozdielov medzi SSL v3 a TLS. Pri výmene kľúča **TLS podporuje všetky výmeny kľúča** definované v SSL v3 **s výnimkou Fortezza**. Pri symetrických šifrovacích algoritmoch **TLS obsahuje všetky symetrické šifrovacie algoritmy** definované v SSLv3 **s výnimkou Fortezza**. V klientskych typoch certifikátu **TLS definuje len tieto typy certifikátu, o ktoré je možno požiadať v správe certificate_request**: rsa_sign, dss_sign, rsa_fixed_dh a dss_fixed_dh. TLS nepodporuje systém Fortezza. V správach certificate_verify a finished **TLS zahrňuje do výpočtu hešovacej hodnoty menší počet položiek**.

8.6 Systémy na detekciu/prevenciu prienikov IDPS

Pri písaní tejto časti autor čerpal najmä z publikácie [48].

Detekcia prienikov je proces monitorovania udalostí v počítačovom systéme alebo v sieti a ich analyzovania na príznaky možných incidentov, ktoré sú porušením alebo bezprostrednou hrozbou porušenia politík počítačovej bezpečnosti, politík akceptovateľného použitia alebo štandardných bezpečnostných praktík.

Systém detekcie prienikov (IDS – Intrusion Detection Systém) je softvér, ktorý automatizuje proces detekcie prienikov. Novšou verziou IDS je **systém prevencie prienikov** (IPS – Intrusion Prevention System), čo je softvér, ktorý má všetky schopnosti systému detekcie prienikov a je schopný pokúsiť sa zastaviť možné incidenty. Súhrnne tieto technológie nazývame IDPS (Intrusion Detection/Prevention System)

Technológie IDPS sú primárne určené na identifikáciu možných incidentov. IDPS môže detegovať úspešnú kompromitáciu systému útočníkom, ktorý využil slabinu systému. IDPS potom môže oznámiť incident bezpečnostnému manažérovi, ktorý okamžite začne aktivity reakcie na incident, aby sa minimalizovala škoda spôsobená incidentom. IDPS ďalej môže vytvoriť **informačný záznam**, ktorý je využitý na riešenie incidentu. Veľa IDPS môže byť konfigurovaných tak, že **rozpozná porušenie bezpečnostnej politiky**. Napríklad niektoré IDPS môžu byť konfigurované nastaveniami podobnými ako bezpečnostná brána, ktoré IDPS umožnia identifikovať sieťovú premávku porušujúcu politiku bezpečnosti organizácie alebo politiku akceptovateľného použitia. Niektoré IDPS môžu **monitorovať prenos súborov a identifikovať možné podozrivé prenosy**, napríklad kopírovanie rozsiahlej databázy na používateľský laptop. Veľa IDPS môžu identifikovať prieskumné aktivity útočníka, ktoré môžu indikovať bezprostredný útok. Príkladom takýchto prieskumných aktivít je skenovanie portov na webovom serveri. IDPS môže blokovať takýto prieskum a upovedomiť bezpečnostného administrátora.

Technológie IPS sa líšia od technológií IDS jednou zásadnou vlastnosťou, technológie IPS **sú schopné reagovať na detegovanú hrozbu** tak, že sa pokúšajú zabrániť, aby bola hrozba úspešná. IPS používajú viaceré techniky reakcie, ktoré je možné rozdeliť do týchto skupín:

- **IPS zastavuje samotný útok.** Napríklad ukončí sieťové spojenie alebo reláciu používateľa, ktorá je použitá na útok, alebo blokuje prístup na cieľ (alebo možné ďalšie pravdepodobné ciele) z útočiaceho účtu používateľa, adresy IP alebo iných atribútov útočníka, alebo blokuje všetky prístupy na cielený uzol, službu, aplikáciu alebo ďalší zdroj.

- **IPS mení bezpečnostné prostredie.** IPS na prerušenie útoku by mohol zmeniť konfiguráciu iných bezpečnostných opatrení. Bežným príkladom je rekonfigurácia sieťového zariadenia (napríklad bezpečnostná brána, smerovač, prepínač) na blokovanie prístupu od útočníka alebo na cieľ a zmenenie hostovej bezpečnostnej brány na cieľ, aby bezpečnostná brána blokovala prichádzajúci útok. Niektoré IPS môžu dokonca spôsobiť aplikáciu záplat na hosta v prípade, že IPS deteguje, že host má slabiny.

- **IPS mení útočníkov obsah.** Niektoré IPS technológie môžu odstrániť alebo zmeniť škodlivú časť útoku a tak útok spravia neškodný. Klasickým príkladom je IPS, ktoré odstráni prílohu s infikovaným súborom v správe elektronickej pošty a až potom umožní,

aby „očistený“ email dostal príjemca. Ďalším príkladom je „normalizácia“ prichádzajúcich žiadostí. To znamená, že proxy „prebalí“ obsah žiadosti zničením informácii hlavičky.

Technológie IDPS **nie sú schopné zabezpečiť úplnú a presnú detekciu prieniku**. Môže nastať prípad, keď IDPS nesprávne identifikuje neškodné aktivity ako škodlivé. Tento prípad označujeme ako **false positive**. Ďalším prípadom je, keď IDPS zlyhá pri identifikácii škodlivých aktivít. Tento prípad označujeme ako **false negative**. Nie je možné eliminovať všetky prípady false positive a false negative. V mnohých prípadoch pri zmene konfigurácie IDPS na potlačenie false negative sa zvyšuje výskyt false positive. Menenie konfigurácie IDPS s cieľom zlepšenia presnosti detekcie sa nazýva **ladenie** (tuning) technológie IDPS.

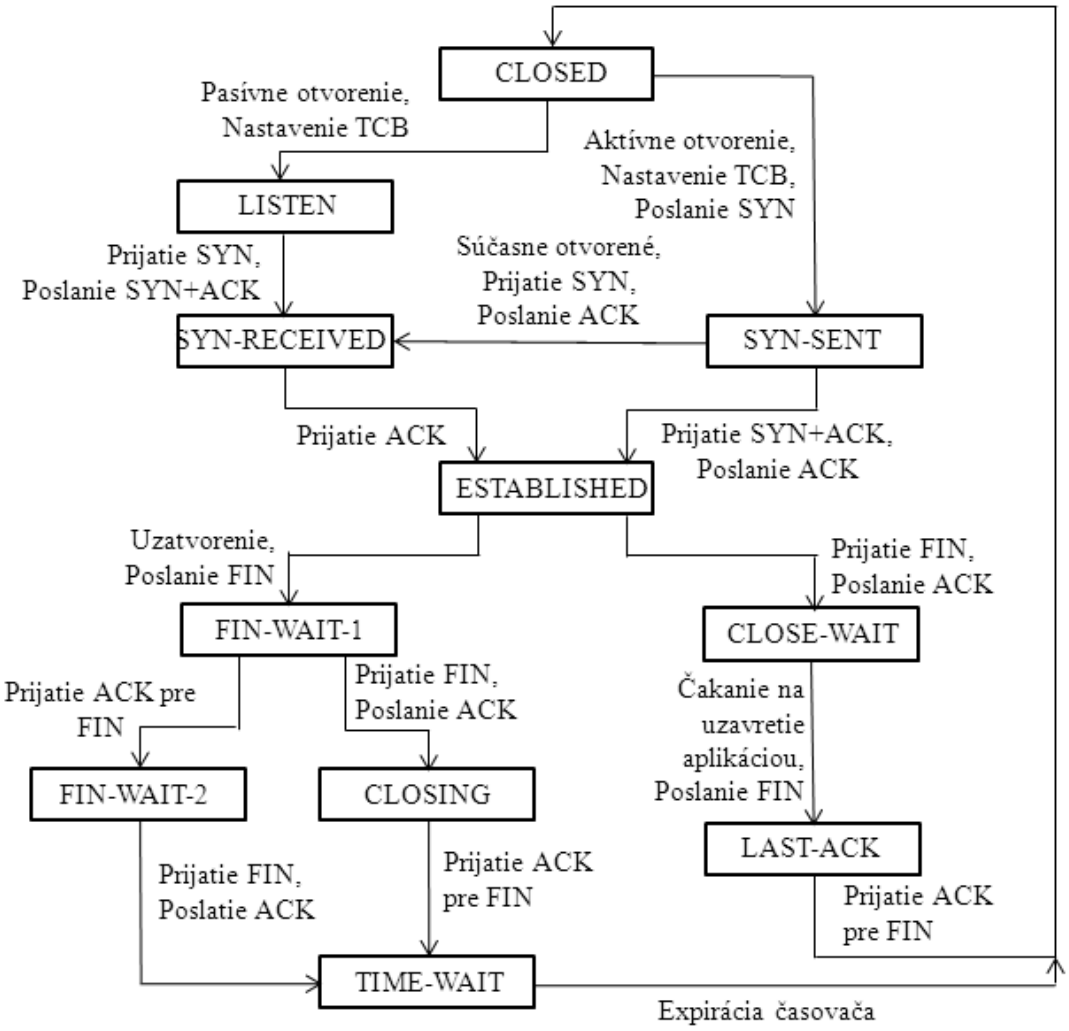
8.6.1 Štandardné detekčné mechanizmy

Technológie IDPS používajú veľa mechanizmov na detegovanie incidentov. Základné triedy detekčných mechanizmov sú založené na príznakoch (signature based), anomáliách (anomaly based) a analýze stavových protokolov (stateful protocol analysis).

Detekčný mechanizmus založený na príznakoch vychádza zo znalosti príznaku (tzv. vzorky), ktorá odpovedá známej hrozbe. Spočíva v podstate na procese porovnávania príznakov oproti pozorovaným udalostiam s cieľom identifikovať možné incidenty. Príklady príznakov je napríklad pokus o spustenie telnetu s loginom „root“, čo je porušenie bezpečnostnej politiky spoločnosti alebo správa elektronickej pošty s predmetom „New games“ a s prílohou „newgames.exe“, čo sú charakteristiky známej formy škodlivého kódu. Tento mechanizmus je veľmi účinný pri detekcii známych hrozieb, ale neefektívny pri detekcii doteraz neznámych hrozieb. Je to najjednoduchšia metóda, pretože iba porovnáva súčasné jednotky aktivity (paket alebo položku v logu) so zoznamom príznakov použitím operácie porovnania reťazcov.

Detekčný mechanizmus založený na anomáliách je proces porovnania definovanej normálnej aktivity oproti pozorovaným udalostiam s cieľom identifikovať významné odchýlky. IDPS využívajúce tento mechanizmus detekcie majú uložené profily, ktoré reprezentujú normálne správanie takých objektov ako je používateľ, uzly, sieťové spojenia alebo aplikácie. Profily sú vytvorené monitorovaním charakteristík typickej aktivity za istý čas. IDPS potom používa štatistické metódy na porovnanie súčasných aktivít oproti prahom súvisiacich s profilom. Napríklad detekcia zvýšeného počtu emailových správ oproti očakávanému počtu správ zaznamenanom v profile. Profily môžu byť vytvorené pre mnoho atribútov správania sa ako sú napríklad počty navštívených webových stránok používateľom, počet neúspešných prihlásení sa na uzol, úroveň využitia procesora uzla v danom časovom intervale. Tento mechanizmus môže byť veľmi účinný pri detekcii predtým neznámych hrozieb. Napríklad počítač bol infikovaný neznámym škodlivým kódom, ktorý spotrebováva počítačové zdroje, posiela veľké množstvo emailových správ, inicializuje veľké množstvo sieťových spojení a vykonáva iné aktivity, ktoré sú významne odlišné od zavedeného profilu pre tento počítač. Iniciálny profil je vytvorený v tréningovom intervale v trvaní typicky dní alebo týždňov. Neúmyselné zahrnutie škodlivých aktivít ako súčasti profilu je spoločným problémom detekčného mechanizmu anomálií (administrátori ručne modifikujú vytvorený profil tak, že z neho vyhadzujú známe škodlivé aktivity). Pri snahe vytvoriť „presné“ profily, častokrát nastáva situácia, kedy IDPS vytvára veľké množstvo false positive alertov. Je to z toho dôvodu, že zriedka vykonávané neškodlivé aktivity nie sú zahrnuté do profilu, a teda generujú alerty.

Detekčný mechanizmus založený na analýze stavových protokolov je proces porovnania dopredu určených profilov všeobecne akceptovaných definícií neškodnej aktivity protokolu pre každý stav protokolu oproti sledovaným udalostiam s cieľom identifikovať odchýlky (potenciálne škodlivé stavy). Definícia protokolu je prevzatá zo štandardizačných dokumentov RFC alebo ich najrozšírenejších implementácií. Slovo „stavový“ v analýze stavového protokolu znamená, že IDPS je schopný porozumieť a sledovať stav sieťového, transportného alebo aplikačného protokolu, ktoré obsahujú koncept stavu. Tento mechanizmus môže identifikovať neočakávané postupnosti príkazov ako je opakované zadanie toho istého príkazu alebo zadanie príkazu bez predchádzajúceho zadanie príkazu, na ktorom je závislý. Primárnou nevýhodou tohto mechanizmu je jeho náročnosť na výpočtové zdroje, pretože pre každý protokol musí vytvoriť novú inštanciu „stavového stroja“ a teda pri viacerých súčasne monitorovaných spojeniach musí pre každé spojenie (a každý použitý stavový protokol) vytvoriť novú inštanciu stavového stroja. Na Obrázku 8.31 je príklad stavového stroja pre transportný protokol TCP.



Obr. 8.31: Stavový stroj pre transportný protokol TCP

8.6.2 Technológie IDPS

Typické komponenty riešení technológií IDPS sú senzor alebo agent, server manažmentu, databázový server a konzola manažmentu.

Senzor alebo agent je prostriedok, ktorý monitoruje alebo analyzuje aktivity. Označenie senzor sa typicky používa pre IDPS, ktoré monitorujú siete. Označenie agent sa typicky používa pre hostové IDPS.

Server manažmentu je centralizované zariadenie, ktoré prijíma informácie od senzorov a agentov a spravuje ich. Niektoré servery manažmentu vykonávajú analýzu informácií o udalosti, ktorú poskytli senzory alebo agenti, a sú schopní identifikovať udalosti, ktoré individuálne senzory a agenti schopné nie sú. Párovanie informácií o udalosti z viacerých senzorov alebo agentov (napríklad udalostí spustených z tej istej adresy IP) sa nazýva **korelácia**. Niektoré malé nasadenia technológií IDPS nepoužívajú server manažmentu, ale väčšina nasadení IDPS servery manažmentu používa.

Databázový server je úložisko na uloženie informácií, ktoré zaznamenali senzory, agenti a/alebo server manažmentu. Veľa IDPS poskytuje podporu pre databázové servery.

Konzola manažmentu je program, ktorý zabezpečuje interfejs medzi IDPS a jeho administrátormi a používateľmi. Typicky je tento program inštalovaný na štandardnom desktope alebo laptope. Niektoré konzoly sú používané iba na administráciu IDPS ako je konfigurácia senzorov alebo agentov, aktualizácia programového vybavenia. Iné konzoly sú používané výlučne iba na monitorovanie a analýzu.

Vyššie uvedené komponenty IDPS môžu byť prepojené medzi sebou prostredníctvom **štandardnej sieti organizácie** (in-band). V takomto prípade je vhodné vytvoriť oddelenie siete manažmentu od produkčnej sieti aspoň na úrovni virtuálnej LAN (VLAN). Použitie VLAN zabezpečuje ochranu IDPS komunikácie (ale nie na takej úrovni ako fyzicky oddelenej siete manažmentu), ale ochrana môže zlyhať pri chybnej konfigurácii VLAN alebo pri útoku DoS na produkčnú sieť. Druhým riešením je prepojiť komponenty IDPS prostredníctvom **oddelenej sieti** (out of band), ktorá je výlučne určená pre manažment bezpečnostného softvéru. Tejto oddelenej sieti sa tiež hovorí sieť manažmentu. V takomto prípade musí mať senzor alebo agent **ďalší sieťový interfejs** (interfejs manažmentu), ktorým je pripojený do siete manažmentu. Toto riešenie sieti efektívne izoluje sieť manažmentu od produkčnej sieti a skrýva existenciu a identitu IDPS pred útočníkmi. Ďalej chráni IDPS pred útokmi a zabezpečuje, že IDPS má k dispozícii dostatočnú sieťovú priepustnosť aj v prípade útoku DoS na produkčnú sieť. Nevýhodou riešenia sú dodatočné náklady na vytvorenie siete manažmentu a nepohodlie pre administrátorov IDPS a používateľov IDPS, pretože musia pre svoje činnosti s IDPS používať oddelené počítače.

Detekčné schopnosti technológií IDPS sú typicky rozsiahle a široké. Väčšina produktov používa kombináciu detekčných techník, ktoré vo všeobecnosti zabezpečujú presnejšiu detekciu a väčšiu flexibilitu pri ladení a prispôsobovaní (customizácii). Príklady ladiacich a prispôsobovacích možností IDPS technológií:

- **Prahy** (Thresholds) – sú hodnoty, ktoré nastavujú limity medzi normálnym a abnormálnym správaním. Prahy sú najviac používané v detekčných mechanizmoch založených na anomáliách a analýze stavových protokolov.

- **Čierne a biele zoznamy** (Blacklists and Whitelists). Čierny zoznam je zoznam diskrétnych entít ako sú hosty, čísla TCP alebo UDP portov, typy a kódy ICMP, aplikácií, mien používateľov, URL, mien súborov alebo súborových rozšírení, ktoré boli v minulosti identifikované ako súčasť škodlivých aktivít. Biely zoznam je zoznam diskrétnych entít, ktoré sú známe ako neškodné. Zvyčajne sa používajú na báze granularity ako po protokoloch, na redukovanie alebo ignorovanie false positive zahrňujúce známe neškodné aktivity z dôveryhodných hostov. Čierne a biele zoznamy sú najčastejšie používané pri detekčných mechanizmoch na báze príznakov a analýzy stavového protokolu.

8.6.3 Sieťové IDPS

Senzory sieťových IDPS sú dostupné v dvoch prevedeniach:

- **Zariadenie.** V tomto prevedení senzor pozostáva zo špecializovaného hardvéru a softvéru. Hardvér je optimalizovaný na použitie senzora vrátane špecializovanej karty NIC a jej ovládača na efektívne odchytávanie paketov a špecializovaných procesorov alebo ďalších hardvérových komponentov podporujúcich analýzu. Časť alebo celý softvér môže byť z dôvodu zvýšenia efektívnosti umiestnený vo firmvéri. Tieto zariadenia často obsahujú prispôsobený, utesnený operačný systém, ku ktorému sa nepredpokladá prístup administrátorov. Príklady: rad CISCO IDS 4200, IBM Real Secure Network.
- **Iba softvér.** Niektorí predajcovia predávajú senzorový softvér bez zariadenia. Administrátori inštalujú tento softvér na počítače, ktoré splňujú určité špecifikácie. Senzorový softvér môže obsahovať prispôsobený (customized) operačný systém alebo senzorový softvér môže byť inštalovaný štandardnom operačnom systéme ako iná aplikácia. Príklady: Snort, Bro.

Senzory môžu byť nasadené v dvoch režimoch:

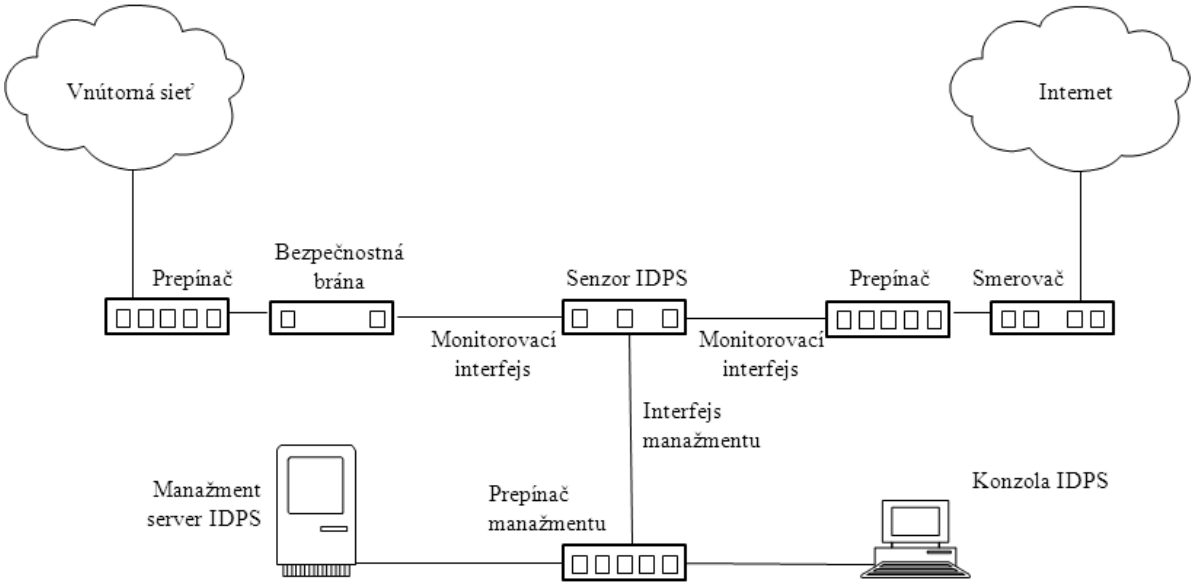
- **Prechodový senzor** (Inline). Všetka monitorovaná premávka prechádza senzorom (podobne ako všetka premávka prechádza bezpečnostnou bránou). **Má dva sieťové interfejsy** na monitorovanie premávky siete (cez tieto interfejsy prechádza sieťová premávka) a **jeden interfejs manažmentu** na pripojenie do siete manažmentu.
- **Pasívny senzor.** Monitoruje kópiu skutočnej sieťovej premávky. Žiadna premávka neprechádza senzorom.

V skutočnosti sú niektoré prechodové senzory **hybridy bezpečnostná brána / IDPS zariadenie**. Primárnym dôvodom pre nasadenie prechodových senzorov IDPS je skutočnosť, aby boli schopné **zastaviť útok blokovaním sieťovej premávky**. Prechodové senzory sú typicky umiestnené na tie miesta v sieti, kde sú umiestňované bezpečnostné brány a iné sieťové bezpečnostné zariadenia a to na hranici medzi sieťami, na pripojení do externých sietí a hranicami medzi rozdielnymi vnútornými sieťami, ktoré by mali byť oddelené. Prechodové senzory, ktoré nie sú hybridy bezpečnostná brána / IDPS zariadenie sú často **umiestňované na bezpečnejšiu stranu siete** (z tej strany hranice, kde je sieť bezpečnejšia), aby spracovávali menší objem premávky. Senzory môžu byť tiež umiestnené na menej bezpečnej strane sieti, aby zabezpečovali ochranu redukovaním záťaže oddeľovacieho zariadenia ako je bezpečnostná brána. Na Obrázku 8.32 je príklad takejto architektúry.

Pasívne senzory sú typicky nasadzované tak, aby monitorovali kľúčové sieťové miesta ako sú hranice medzi sieťami, kľúčové sieťové segmenty ako sú aktivity v demilitarizovanej zóne (DMZ). Pasívne senzory môžu monitorovať premávku prostredníctvom rôznych metód, ako napríklad:

- **Pokrývajúci port** (spanning port) - je port prepínača, ktorý je schopný vidieť **všetku sieťovú premávku prechádzajúcu cez prepínač**. Pripojením senzora na pokrývajúci port môže senzor monitorovať premávku na / z veľa uzlov. Táto metóda monitorovania je relatívne ľahká a lacná.
- **Sieťová prípojka** (network tap) – je priame prepojenie medzi senzorom a samotným fyzickým médiom ako je napríklad optické vlákno. Prípojka dodáva senzoru kópiu celej sieťovej premávky, ktorá sa prenáša cez médium.
- **Vyvažovač záťaže IDS** (load balancer IDS) – je zariadenie, ktoré **dáva dokopy a smeruje premávku siete** do monitorovacích systémov vrátane IDPS senzorov. Vyvažovač dostane kópiu sieťovej premávky z jedného alebo viacerých pokrývajúcich portov alebo sieťových prípojok a dáva dokopy premávku z rôznych sietí (napríklad znovu skladá reláciu, ktorá bola rozdelená medzi dve siete).

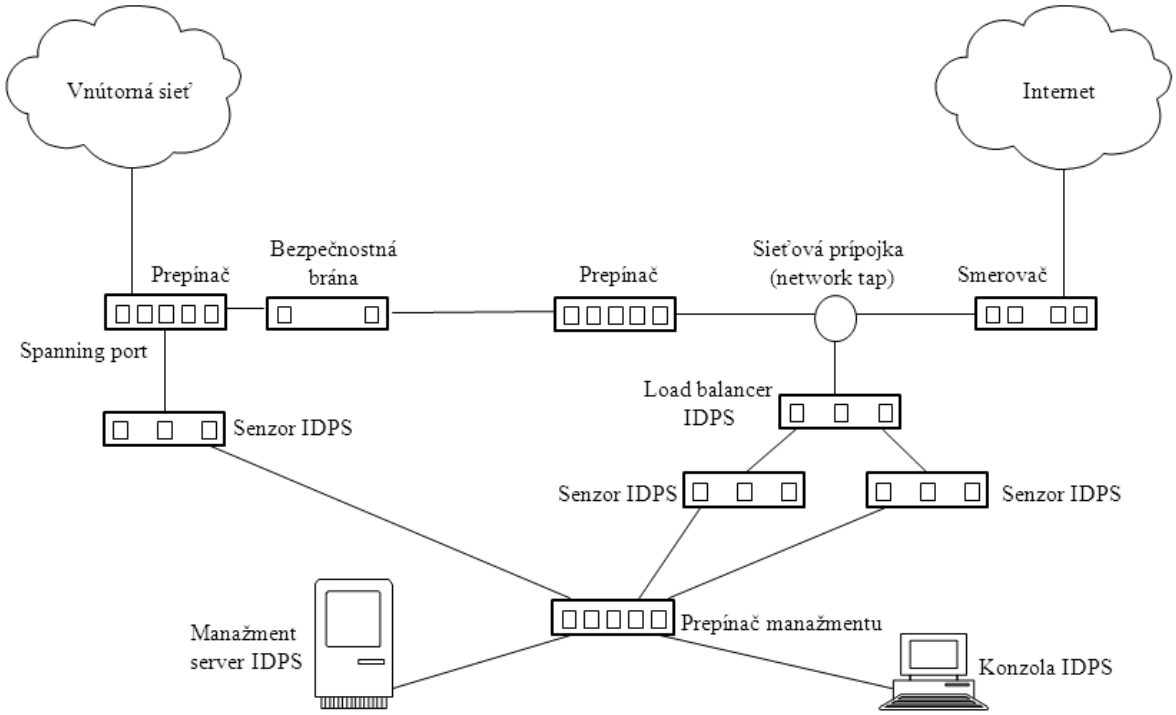
Príklad architektúry IDS s pasívnym senzorom je na Obrázku 8.33.



Obr. 8.32: Príklad architektúry IDPS s prechodovým senzorom

Sieťové IDPS poskytujú široké možnosti bezpečnostných funkcií, ktoré môžu byť štruktúrované do štyroch kategórií: zhromaždenie informácií, zaznamenanie, detekcia a prevencia.

Funkcia zhromaždenia informácií. Niektoré sieťové IDPS ponúkajú obmedzené schopnosti zhromažďovania informácií, čo znamená, že zbierajú informácie o uzloch a sieťových aktivitách zahrňujúcich tieto uzly. Príklady možností zhromažďovania informácií sú: **identifikácia uzla** (vytvorenie zoznamu uzlov pripojených do siete organizácie podľa adries IP alebo



Obr. 8.33: Príklad architektúry IDPS s pasívnym senzorom

adries MAC), **identifikácia operačných systémov** (identifikácia operačných systémov a ich verzií, ktoré sa používajú v organizácii), **identifikácia aplikácií** (identifikácia používanej verzie aplikácie tak, že sleduje, ktoré porty sú používané a monitoruje určité charakteristiky komunikácie aplikácie).

Funkcia zaznamenania. Sieťové IDPS typicky vykonávajú rozsiahle zaznamenanie údajov majúcich vzťah k detegovanej udalosti. Tieto údaje môžu byť použité na potvrdenie platnosti alertu, na vyšetrenie incidentov a na koreláciu udalostí medzi IDPS a ostatnými logovacími zdrojmi. Väčšina sieťových IDPS je schopná vykonať zachytenie paketov. Štandardne sa to vykonáva vtedy, keď sa generuje alert. Zachytávajú sa alebo následné aktivity v spojení po alerte alebo sa zanamená celé spojenia (ak IDPS dočasne uchovával predchádzajúce pakety). **Záznam sieťového IDPS môže vo všeobecnosti obsahovať tieto údajové polia** (položky): časová pečiatka (dátum a čas), ID spojenia alebo relácie (typicky postupné alebo jedinečné číslo priradené každému TCP spojeniu alebo podobným skupinám paketov pre protokoly bez spojenia), typ udalosti alebo alertu, rating (napríklad priorita, dôležitosť, dopad, dôvernosť), protokol sieťovej, transportnej a aplikačnej vrstvy, zdrojová a cieľová adresa IP, zdrojový a cieľový port TCP alebo UDP, alebo typy ICMP a kódy, počet slabík prenesených týmto spojením, dekódované údaje užitočného nákladu (payload), ako sú žiadosti a odpovede aplikácie, informácie viažúce sa na stav (napríklad autentizované meno používateľa), vykonané preventívne akcie (ak treba).

Funkcia detekcie. Sieťové IDPS typicky ponúkajú široké a všeobecné detekčné schopnosti. Väčšina produktov využíva kombináciu mechanizmov detekcie pomocou príznakov, anomálií a analýzy stavových protokolov (in-depth analysis bežných protokolov). Detekčné mechanizmy

sú zvyčajne pevne previazané, napríklad stroj na detekciu mechanizmu analýzy stavových protokolov môže rozobrať aktivity do žiadostí a odpovedí, pričom každá z nich je preverovaná na anomálie a porovnaná s príznakom známych škodlivých aktivít. Detekčné schopnosti možno analyzovať z týchto pohľadov: typy detegovaných udalostí, presnosť detekcie, ladenie a prispôsobenie, obmedzenia technológie. **Najbežnejšie typy detegovaných udalostí** senzormi sieťových IDPS sú: **prieskum a útoky na aplikačnej vrstve** (napríklad odchytenie bannera, pretečenie vyrovnávacej pamäti, útoky na formátové reťazce, hádanie hesla, prenášanie škodlivého kódu), **prieskum a útoky na transportnej vrstve** (Napríklad skenovanie portov, nezvyčajná fragmentácia paketov, záplava SYN. Najfrekventovanejšie analyzované protokoly transportnej vrstvy sú TCP a UDP.), **prieskum a útoky na sieťovej vrstve** (napríklad falošná - spoofed adresa IP, nedovolená hodnota hlavičky IP), **neočakávané aplikačné služby** (napríklad tunelované protokoly, zadné vrátka, uzly vykonávajúce neautorizované aplikačné služby) a **porušenuie politiky** (napríklad použitie nevhodných webových sídiel, použitie zakázaných aplikačných protokolov).

Funkcia prevencie (prechodové senzory a niektoré pasívne sieťových IDPS): **ukončenie aktuálneho TCP spojenia** (pasívny senzor IDPS môže skúsiť ukončiť existujúcu reláciu TCP tak, že pošle pakety TCP reset obidvom komunikujúcim koncom, táto technika nie je v súčasnosti široko používaná, pretože iné prevenčné schopnosti sú efektívnejšie), **vykonanie prechodového firewallingu** (väčšina senzorov IDPS ponúka funkcie bezpečnostnej brány, ktoré môžu byť použité na zastavenie alebo odmietnutie podozrivej sieťovej aktivity), **obmedzenie na použitie prenosového pásma** (v prípade, že určitý protokol sa používa nevhodne, ako napríklad na útok DoS, distribúciu škodlivého kódu alebo peer-to-peer zdieľanie súborov, niektoré prechodové senzory IDPS môžu obmedziť percento sieťového prenosového pásma), a **zmena škodlivého obsahu** (niektoré prechodové senzory IDPS môžu sanovať časť paketu, čo znamená, že je nahradený škodlivý obsah za neškodný obsah a sanovaný paket je odoslaný do svojho cieľa).

Funkcie prevencie (aj pasívne aj prechodové senzory sieťových IDPS): **rekonfigurácia iných sieťových bezpečnostných zariadení** (veľa senzorov IDPS môže dať pokyn sieťovým bezpečnostným zariadeniam ako sú bezpečnostné brány, smerovače a prepínače na ich rekonfiguráciu s cieľom blokovania určitého typu aktivity alebo ich smerovania inam), **vykonávanie programov tretích strán alebo skriptov** (niektoré senzory IDPS sú schopné, v prípade detekcie určitej škodlivej aktivity, vykonať administrátorom určený skript alebo program). Väčšina senzorov IDPS dovoľuje administrátorom **špecifikovať prevencie schopné konfigurácie pre každý typ alertu**. Toto zvyčajne zahrňuje povolenie alebo zakázanie prevencie, rovnako ako špecifikovanie ktoré prevenčné možnosti by mali byť použité. Niektoré senzory IDPS majú režim učenia alebo simulácie, ktorý potláča všetky preventívne akcie a namiesto toho indikuje kedy by bola preventívna akcia vykonaná. Tento režim umožňuje administrátorom monitorovať a jemne ladiť preventívne schopnosti konfigurácie predtým než sa povolia, čo redukuje riziko náhleho blokovania neškodnej aktivity.

8.6.4 Bezdrôtové IDPS

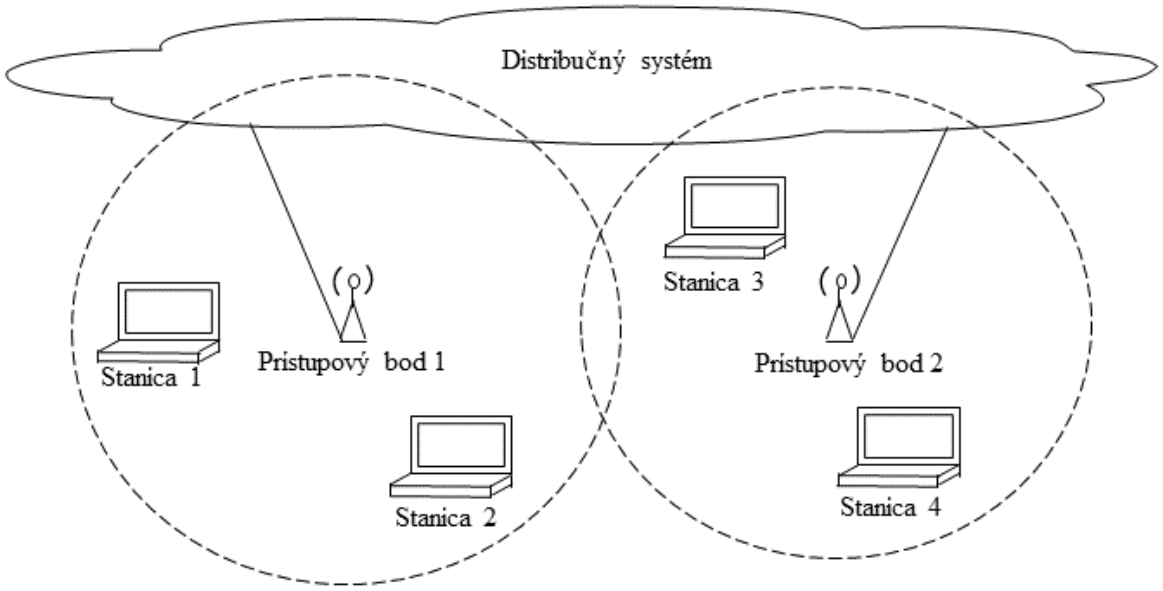
Bezdrôtové IDPS monitorujú bezdrôtovú sieťovú premávku a analyzujú jej bezdrôtové sieťové protokoly s cieľom **identifikovať podozrivé aktivity zahrňujúce samotné protokoly**.

WLAN (bezdrôtové LAN) podľa štandardu IEEE 802.11 majú dva základné architektonické komponenty a to stanicu a prístupový bod. **Stanica** (STA) je bezdrôtové koncové zariadenie. Typickým príkladom STA je notebook, laptop, smartfón, tablet a ďalšie zariadenia spotrebnej elektroniky s vybavením podľa IEEE 802.11. **Prístupový bod** (AP – Access Point) logicky pripája STA k distribučnému systému, ktorým je typicky pevná (drôtovaná) infraštruktúra organizácie. Distribučný systém je prostriedok, prostredníctvom ktorého môžu STA komunikovať s pevnou LAN spoločnosti a externou sieťou ako je Internet. Príklad architektúry bezdrôtovej LAN je na Obrázku 8.34.

Niektoré WLAN používajú tiež **bezdrôtové prepínače** (wireless switch). Je to zariadenie, ktoré funguje ako prostredník medzi STA a AP (a distribučným systémom).

Štandard IEEE 802.11 tiež definuje tieto dve WLAN architektúry a to ad hoc režim a infraštruktúrny režim. **Ad hoc režim** nevyužíva AP. Ad hoc režim, tiež známy ako peer-to-peer režim, zahrňuje dve alebo viac STA komunikujúcich priamo jeden s druhým. Známym prípadom tohto režimu sú siete MANET (Mobile Ad-hoc NETwork). V **infraštruktúrnom režime** prístupový bod logicky pripája STA k distribučnému systému, ktorý je typicky pevné (drôtovaná) sieť. Takmer všetky WLAN sa využívajú v infraštruktúrnom režime.

Každý modul AP v sieti WLAN má priradené meno, ktoré sa nazýva identifikátor množiny služieb **SSID** (Service Set IDentifier). SSID umožňuje STA odlíšiť jednu WLAN od druhej WLAN. AP vysiela SSID vo **formáte obyčajného textu**, takže každé prijímajúce bezdrôtové zariadenie sa môže ľahko dozvedieť SSID každej WLAN, ktorá je v dosahu zariadenia.



Obr. 8.34: Príklad architektúry bezdrôtovej LAN

Bezdrôtová aj pevná (drôtovaná) sieť čelia **rovnakým všeobecným typom hrozieb**, relatívne riziko niektorých hrozieb sa však výrazne líši. Napríklad bezdrôtové útoky zvyčajne vyžadujú, aby útočník alebo útočníkove zariadenie bolo v tesnej fyzickej blízkosti k bezdrôtovej sieti, na druhej strane, mnoho útokov na pevnej siete možno vykonávať na diaľku z ľubovoľného

miesta. Navyše, mnoho WLAN je nastavených tak, že nevyžadujú autentizáciu alebo vyžadujú len slabé formy autentizácie, čo značne uľahčuje útočníkom vykonávať niekoľko typov útokov, napríklad útok Man In The Middle. Väčšina hrozieb proti WLAN zahrňujú útočníka s prístupom k rádiovému spojeniu medzi STA a AP (alebo medzi dvoma STA v režime ad hoc). Mnoho útokov sa spolieha na možnosť útočníka zachytiť sieťovú komunikácie alebo vložiť do komunikácie ďalšie správy. To dokumentuje najvýznamnejší rozdiel medzi ochranou bezdrôtovej a pevnej siete LAN: relatívna jednoduchosť prístupu a zmena sieťovej komunikácie.

Typické komponenty bezdrôtových IDPS sú rovnaké ako v sieťových IDPS: konzola, databázové servery (voliteľne), servery manažmentu a senzory. Všetky komponenty okrem senzorov majú v podstate rovnaké funkcie pre oba typy IDPS. Bezdrôtové senzory majú rovnakú základnú úlohu ako sieťové senzory IDPS, ale **fungujú veľmi odlišne** z dôvodu zložitosti monitorovania bezdrôtovej komunikácie. Na rozdiel od sieťových IDPS, ktoré môžu vidieť všetky pakety siete, bezdrôtové IDPS pracujú na princípe **vzorkovania premávky**. Existujú dve frekvenčné pásma na monitorovanie (2,4 GHz a 5 GHz) a každé pásmo je rozdelená do kanálov. **Senzor nemôže monitorovať všetku premávku v pásme naraz, v danom čase môže monitorovať iba jeden kanál.** Aby sa potlačil tento handicap, senzory často prepínajú medzi monitorovanými kanálmi. Tomuto mechanizmu sa hovorí **skenovanie kanálov** (senzor monitoruje každý kanál niekoľkokrát za sekundu).

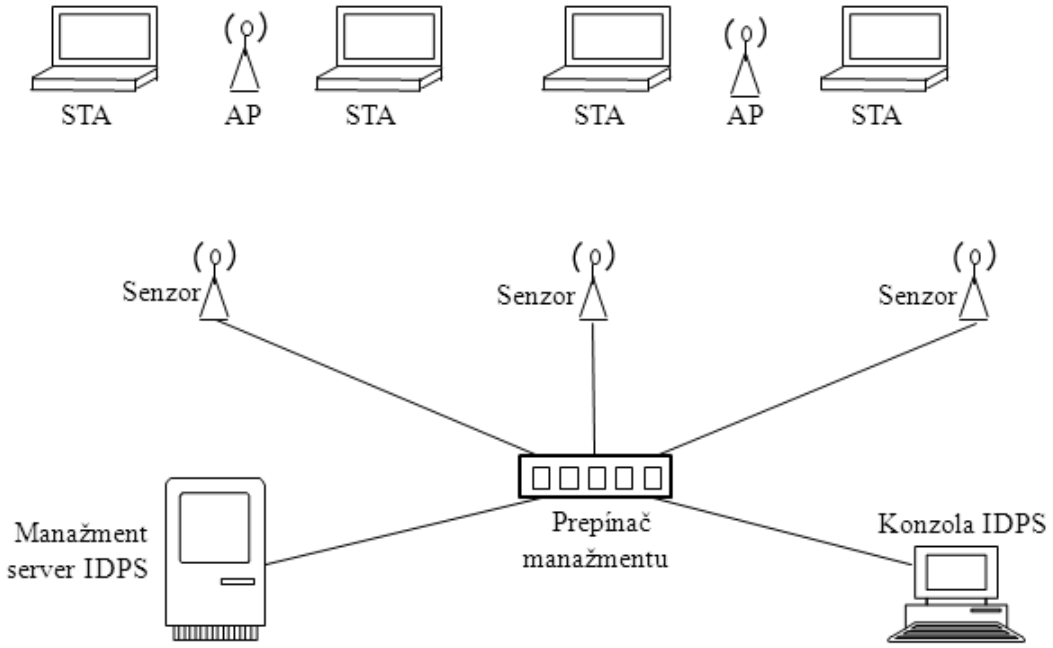
Bezdrôtové senzory sú dostupné vo viacerých formách:

- **Venované.** Venovaný senzor je zariadenie, ktoré vykonáva funkcie bezdrôtového IDPS, ale neprenáša sieťovú premávku od zdroja k cieľu. Venované senzory sú často úplne pasívne a iba odchytávajú sieťovú premávku, ktorú majú v danom kanále v dosahu. Niektoré špecializované senzory **vykonávajú analýzu premávky samy**, zatiaľ čo ostatné senzory iba **preposielajú sieťovú premávku na analýzu na server manažmentu**. Senzor je typicky pripojený k pevnej sieti. Venované senzory sú zvyčajne navrhnuté ako pevný senzor (Je nasadený na určitom mieste a je typicky závislý od infraštruktúry organizácie, napr. energie, pevná sieť. Pevné senzory sú obvykle zariadenia.) alebo ako mobilný senzor (Je určený na použitie v pohybe. Napríklad bezpečnostný správca môže používať mobilný senzor pri prechádzkach po budove spoločnosti a hľadať škodlivé AP.)

- **V spojení s AP.** Niekoľkí výrobcovia **pridali funkcie IDPS do AP**. Takýto AP zvyčajne zabezpečuje menšie možnosti detekcie ako venovaný senzor, pretože AP sa musí rozdeliť s existujúcim výpočtovým výkonom na zabezpečenie prístupu do siete a monitorovanie viacerých kanálov alebo pásiem na škodlivé aktivity.

- **V spojení s bezdrôtovým prepínačom.** Niektoré bezdrôtové prepínače tiež ponúkajú niektoré funkcie **bezdrôtových IDPS ako sekundárne funkcie**. Bezdrôtové prepínače obvykle neposkytujú také detekčné schopnosti ako v spojení s AP alebo venované senzory.

Komponenty bezdrôtových IDPS sú typicky vzájomne prepojené prostredníctvom pevnej siete (viď Obrázok 8.35). Podobne ako pri sieťových IDPS, môže byť na komunikáciu medzi komponentmi IDPS využitá štandardná (produkčná) sieť spoločnosti alebo oddelená sieť manažmentu. Niektoré bezdrôtové senzory IDPS (mobilné senzory) sú používané samostatne a nepotrebujú pevnú sieťovú konektivitu.



Obr. 8.35: Príklad architektúry bezdrôtových IDPS

Bezdrôtové IDPS poskytujú niekoľko typov bezpečnostných funkcií. Pretože bezdrôtové IDPS je relatívne nová forma IDPS, ich možnosti sa medzi výrobcami v súčasnej dobe veľmi líšia.

Funkcia zbierania informácií. Väčšina bezdrôtových IDPS môže zbierať informácie o bezdrôtových zariadeniach. Príklady možností zbierania týchto informácií sú: **identifikácia zariadení WLAN** (väčšina senzorov IDPS dokáže vytvoriť a udržiavať - na základe SSID a adries MAC), **zoznam spozorovaných zariadení WLAN, vrátane AP, bezdrôtových klientov a ad hoc** (peer-to-peer) klientov), **identifikácia WLAN** (väčšina senzorov IDPS sleduje pozorované siete WLAN identifikujúc ich podľa SSID).

Funkcia zaznamenania. Bezdrôtové IDPS zvyčajne vykonávajú rozsiahle zaznamenanie údajov týkajúcich sa detegovaných udalostí. Tieto údaje možno použiť na **potvrdenie platnosti alertov, vyšetrovanie incidentov a na koreláciu udalostí medzi IDPS a ďalších záznamových zdrojov**. Údajové polia, zvyčajne zaznamenané pomocou bezdrôtových IDPS, obsahujú časová pečiatka (zvyčajne dátum a čas), typ udalosti alebo alertu, priradenie priority a závažnosti, zdrojová adresa MAC (výrobca je často identifikovaný podľa adresy), číslo kanála, ID senzoru, ktorý spozoroval udalosť, vykonané preventívne akcie (ak nejaké boli).

Funkcia detekcie. Bezdrôtové IDPS **dokáže detegovať útoky, chybné konfigurácie a porušovania politiky na úrovni protokolu WLAN, a to predovšetkým skúmanie komunikačného protokolu IEEE 802.11**. Bezdrôtové IDPS neskúmajú komunikáciu na vyšších úrovniach (napr. adresy IP, aplikačný náklad). Niektoré produkty vykonávajú iba jednoduchú detekciu príznakov, zatiaľ čo iné používajú kombináciu mechanizmu príznakov, mechanizmu anomálií a mechanizmu analýzy stavových protokolov. **Typy udalostí**, ktoré sú najčastejšie **detegované bezdrôtovými senzormi IDPS**, pokrývajú: **neoprávnené WLAN**

a zariadenia WLAN (prostredníctvom svojich možností zbierania informácií, väčšina bezdrôtových senzorov IDPS sú schopní detegovať škodlivé AP, neoprávnené STA a neoprávnené WLAN), **slabo zabezpečené zariadenia WLAN** (Väčšina bezdrôtových senzorov IDPS je schopná identifikovať AP a STA, ktoré nepoužívajú náležité bezpečnostné opatrenia. To zahŕňa detegovanie chybných konfigurácií a použitie slabých protokolov WLAN a implementácií protokolu.), **nezvyčajné vzory použitia** (niektoré senzory používajú mechanizmus anomálií na detekciu nezvyčajných vzorov použitia WLAN), **používanie bezdrôtových sieťových skenerov** (môžu detegovať iba používanie aktívnych skenerov), **podmienky a útoky Denial of Service (DoS)** (napríklad logické útoky ako sú záplavy (flooding), ktorá predstavuje súčasné posielanie veľkého množstva správ na AP a fyzické útoky ako je rušenie (jamming), ktorá predstavuje vyžarovanie elektromagnetickej energie na frekvenciách siete WLAN tak, aby sa frekvencia stala pre WLAN nepoužiteľná) a **impersonifikácia a útoky Man In The Middle** (Niektoré bezdrôtové senzory IDPS môžu detegovať prípad, keď zariadenie sa snaží sfalšovať identitu iného zariadenia. Tento prípad môže byť zistený tak, že senzor identifikuje rozdiely v charakteristikách aktivity ako sú napríklad určité hodnoty v rámcoch.)

Funkcia prevencie. Senzory bezdrôtových IDPS ponúkajú dva typy možností prevencie pred prienikmi a to bezdrôtové a drôtové. V prípade **bezdrôtovej prevencie** niektoré senzory sú schopné vzduchom ukončiť spojenia medzi škodlivým alebo chybne konfigurovaným STA a autorizovaným AP alebo medzi oprávneným STA a škodlivým alebo chybne konfigurovaným AP. Senzory túto aktivitu zabezpečia zaslaním správy koncovým bodom komunikácie, aby de-asociovali aktuálnu reláciu. Senzor potom odmieta, aby bolo povolené nadviazanie nového spojenia. V prípade **drôtovej prevencie** niektoré senzory môžu dať pokyn prepínaču na pevnej sieti, aby zablokoval sieťovú aktivitu zahŕňajúce konkrétne STA alebo AP a to podľa adresy MAC zariadenia alebo portu prepínača. Ak STA napríklad posiela útoky na server v pevnej sieti, senzor môže dať pokyn pevnému prepínaču, aby blokoval všetku aktivitu na a z tohto STA. Táto technika je účinná iba pre blokovanie škodlivého STA alebo AP v komunikácii pevnej sieti. Technika nezastaví STA alebo AP od ďalšieho vykonávania škodlivých aktivít prostredníctvom bezdrôtových protokolov.

Táto časť bola spracovaná z uvedených zdrojov, najma však sa opiera o prácu [48]. Pre záujemcov o funkcie a nasadenie voľne šíriteľného nástroja sieťového IDS Snort sa odporúčajú publikácie [3, 19, 36].

Literatúra

[1] E. Barker, Q. Dang, S. Frankel, K. Scarfone a P. Wouters. *Guide to IPsec VPNs*. NIST SP 800-77, Revision 1. National Institute of Standards and Technology (NIST), jún 2020. URL: https://doi.org/10.6028/NIST.SP.800-77r1 (citované na strane 200).

[2] A. Barth. *HTTP State Management Mechanism*. ISSN: 2070-1721. Internet Engineering Task Force (IETF), apr. 2011. URL: https://tools.ietf.org/html/rfc6265 (citované na strane 199).

[3] J. Beale a Caswell. *Snort 2.1 Intrusion Detection, Second Edition*. ISBN-10: 9781931836043. Syngress, máj 2004 (citované na strane 228).

[4] R. Bush, D. Karrenberg, M. Kosters a R. Plzak. *Root Name Server Operational Requirements*. Internet Engineering Task Force (IETF), jún 2000. URL: https://tools.ietf.org/html/rfc2870 (citované na strane 167).

[5] D. H. Crocker. *Standard for the format of ARPA Internet text messages*. Internet Engineering Task Force (IETF), aug. 1982. URL: https://tools.ietf.org/html/rfc822 (citované na stranách: 178, 188, 190).

[6] T. Dierks a C. Allen. *The TLS Protocol Version 1.0*. Internet Engineering Task Force (IETF), jan. 1999. URL: https://tools.ietf.org/html/rfc2246 (citované na strane 211).

[7] T. Dierks a E. Rescorla. *The Transport Layer Security (TLS) Protocol Version 1.1*. Internet Engineering Task Force (IETF), apr. 2006. URL: https://tools.ietf.org/html/rfc4346 (citované na strane 211).

[8] T. Dierks a E. Rescorla. *The Transport Layer Security (TLS) Protocol Version 1.2*. Internet Engineering Task Force (IETF), aug. 2008. URL: https://tools.ietf.org/html/rfc5246 (citované na stranách: 211, 216).

[9] C. Everhart, L. Mamakos, R. Ullmann a P. Mockapetris. *New DNS RR Definitions*. Internet Engineering Task Force (IETF), dec. 1990. URL: https://tools.ietf.org/html/rfc1183 (citované na strane 171).

[10] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach a T. Berners-Lee. *Hypertext Transfer Protocol – HTTP/1.1*. Internet Engineering Task Force (IETF), jún 1999. URL: https://tools.ietf.org/html/rfc2616 (citované na stranách: 188, 195).

[11] S. Frankel, P. Hoffman, A. Orebaugh a R. Park. *Guide to SSL VPNs*. NIST SP 800-113. National Institute of Standards and Technology (NIST), júl 2008. URL: https://doi.org/10.6028/NIST.SP.800-113 (citované na strane 209).

[12] J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen a L. Stewart. *Hypertext Transfer Protocol – HTTP/1.1*. Internet Engineering Task Force (IETF), jún 1999. URL: https://tools.ietf.org/html/rfc2617 (citované na stranách: 188, 198).

[13] N. Freed a N. Borenstein. *Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples*. Internet Engineering Task Force (IETF), nov. 1996. URL: https://tools.ietf.org/html/rfc2049 (citované na stranách: 179, 188, 190, 193, 196).

[14] N. Freed a N. Borenstein. *Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies*. Internet Engineering Task Force (IETF), nov. 1996. URL: https://tools.ietf.org/html/rfc2045 (citované na stranách: 179, 180, 188, 190, 193, 196).

[15] N. Freed a N. Borenstein. *Multipurpose Internet Mail Extensions (MIME) Part Three: Message Header Extensions for Non-ASCII Text*. Internet Engineering Task Force (IETF), nov. 1996. URL: https://tools.ietf.org/html/rfc2047 (citované na stranách: 179, 188, 190, 193, 196).

[16] N. Freed a N. Borenstein. *Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types*. Internet Engineering Task Force (IETF), nov. 1996. URL: https://tools.ietf.org/html/rfc2046 (citované na stranách: 179, 180, 188, 190, 193, 196).

[17] N. Freed, J. Klensin a J. Postel. *Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures*. Internet Engineering Task Force (IETF), nov. 1996. URL: https://tools.ietf.org/html/rfc2048 (citované na stranách: 179, 188, 190, 193, 196).

[18] A. Freier, P. Karlton a P. Kocher. *The Secure Sockets Layer (SSL) Protocol Version 3.0*. ISSN: 2070-1721. Internet Engineering Task Force (IETF), aug. 2011. URL: https://tools.ietf.org/html/rfc6101 (citované na strane 211).

[19] C. Gerg a K. J. Cox. *Managing Security with Snort and IDS Tools*. ISBN-10 : 0596006616. O'Reilly Media, aug. 2004 (citované na strane 228).

[20] D. Harkins a D. Carrel. *The Internet Key Exchange (IKE)*. Internet Engineering Task Force (IETF), nov. 1998. URL: https://tools.ietf.org/html/rfc2409 (citované na strane 205).

[21] R. Hously. *Cryptographic Message Syntax (CMS)*. Internet Engineering Task Force (IETF), júl 2004. URL: https://tools.ietf.org/html/rfc3852 (citované na strane 178).

[22] R. Hously. *Cryptographic Message Syntax (CMS) Algorithms*. Internet Engineering Task Force (IETF), aug. 2002. URL: https://tools.ietf.org/html/rfc3370 (citované na strane 178).

[23] *ISO 3166 Country Codes*. ISO (citované na strane 167).

[24] *ISO/IEC 8859 Information technology – 8-bit single-byte coded graphic character sets*. ISO a IEC (citované na strane 180).

[25] C. Kaufman, P. Hoffman, Y. Nir a P. Eronen. *Internet Key Exchange Protocol Version 2 (IKEv2)*. ISSN: 2070-1721. Internet Engineering Task Force (IETF), sept. 2010. URL: https://tools.ietf.org/html/rfc5996 (citované na strane 207).

[26] S. Kent a R. Atkinson. *IP Authentication Header*. Internet Engineering Task Force (IETF), nov. 1998. URL: https://tools.ietf.org/html/rfc2402 (citované na strane 205).

[27] S. Kent a R. Atkinson. *IP Encapsulating Security Payload (ESP)*. Internet Engineering Task Force (IETF), nov. 1998. URL: https://tools.ietf.org/html/rfc2406 (citované na strane 205).

[28] S. Kent a R. Atkinson. *Security Architecture for the Internet Protocol*. Internet Engineering Task Force (IETF), nov. 1998. URL: https://tools.ietf.org/html/rfc2401 (citované na strane 205).

[29] T. Kivinen, B. Swander, A. Huttunen a V. Volpe. *Negotiation of NAT-Traversal in the IKE*. Internet Engineering Task Force (IETF), jan. 2005. URL: https://tools.ietf.org/html/rfc3947 (citované na strane 209).

[30] H. Krawczyk, M. Bellare a R. Canetti. *HMAC: Keyed-Hashing for Message Authentication*. Internet Engineering Task Force (IETF), feb. 1997. URL: https://tools.ietf.org/html/rfc2104 (citované na strane 216).

[31] C. Madson a R. Glenn. *The Use of HMAC-MD5-96 within ESP and AH*. Internet Engineering Task Force (IETF), nov. 1998. URL: https://tools.ietf.org/html/rfc2403 (citované na strane 205).

[32] C. Madson a R. Glenn. *The Use of HMAC-SHA-1-96 within ESP and AH*. Internet Engineering Task Force (IETF), nov. 1998. URL: https://tools.ietf.org/html/rfc2404 (citované na strane 205).

[33] D. Maughan, M. Schertler, M. Schneider a J. Turner. *Internet Security Association and Key Management Protocol (ISAKMP)*. Internet Engineering Task Force (IETF), nov. 1998. URL: https://tools.ietf.org/html/rfc2408 (citované na strane 205).

[34] P. V. Mockapetris. *Domain Names – Concepts and Facilities*. Internet Engineering Task Force (IETF), nov. 1987. URL: https://tools.ietf.org/html/rfc1034 (citované na strane 166).

[35] P. V. Mockapetris. *Domain Names – Implementation and Specification*. Internet Engineering Task Force (IETF), nov. 1987. URL: https://tools.ietf.org/html/rfc1035 (citované na stranách: 166, 171).

[36] S. Northcutt a J. Novak. *Network Intrusion Detection: An Analyst's Handbook, Third Edition*. ISBN-10 : 0735712654. Sams Publishing, aug. 2002 (citované na strane 228).

[37] M. Ohta. *Incremental Zone Transfer in DNS*. Internet Engineering Task Force (IETF), aug. 1996. URL: https://tools.ietf.org/html/rfc1995 (citované na strane 168).

[38] H. Orman. *The OAKLEY Key Determination Protocol*. Internet Engineering Task Force (IETF), nov. 1998. URL: https://tools.ietf.org/html/rfc2412 (citované na strane 205).

[39] J. Postel. *Domain Name System Structure and Delegation*. Internet Engineering Task Force (IETF), mar. 1994. URL: https://tools.ietf.org/html/rfc1591 (citované na strane 168).

[40] J. Postel. *Simple Mail Transfer Protocol*. Internet Engineering Task Force (IETF), aug. 1982. URL: https://tools.ietf.org/html/rfc821 (citované na strane 179).

[41] F. I. P. S. Publication. *Security Requirements for Cryptographic Modules*. FIPS PUB 140-2, Change Notice 2 December 03, 2002. National Institute of Standards and Technology (NIST), máj 2001. URL: https://doi.org/10.6028/NIST.FIPS.140-2 (citované na strane 203).

[42] F. I. P. S. Publication. *Security Requirements for Cryptographic Modules*. FIPS PUB 140-3. National Institute of Standards and Technology (NIST), mar. 2019. URL: https://doi.org/10.6028/NIST.FIPS.140-3 (citované na strane 203).

[43] B. Ramsdell. *Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Certificate Handling*. Internet Engineering Task Force (IETF), júl 2004. URL: https://tools.ietf.org/html/rfc3850 (citované na strane 178).

[44] B. Ramsdell. *Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification*. Internet Engineering Task Force (IETF), júl 2004. URL: https://tools.ietf.org/html/rfc3851 (citované na strane 178).

[45] P. Resnick. *Internet Message Format*. Internet Engineering Task Force (IETF), okt. 2008. URL: https://tools.ietf.org/html/rfc5322 (citované na stranách: 178–180, 182, 185).

[46] P. Resnick a A. Walker. *The text/enriched MIME Content-type*. Internet Engineering Task Force (IETF), feb. 1996. URL: https://tools.ietf.org/html/rfc1896 (citované na strane 180).

[47] S. A. I. Sainstitute.org. *Attacking the DNS Protocol*. Jan. 2003. URL: http://www.rootsecure.net/content/downloads/pdf/sans_attacking_dns_protocol.pdf (citované na strane 173).

[48] K. Scarfone a P. Mell. *Guide to Intrusion Detection and Prevention Systems*. NIST SP 800-94. National Institute of Standards and Technology (NIST), feb. 2007. URL: https://doi.org/10.6028/NIST.SP.800-94 (citované na stranách: 217, 228).

[49] R. Troost, S. Dorner a K. Moore. *Communicating Presentation Information in Internet Messages: The Content-Disposition Header Field*. Internet Engineering Task Force (IETF), aug. 1997. URL: https://tools.ietf.org/html/rfc2183 (citované na strane 180).

[50] P. Vixie, S. Thomson, Y. Rekhter a J. Bound. *Dynamic Updates in the Domain Name System (DNS UPDATE)*. Internet Engineering Task Force (IETF), apr. 1997. URL: https://tools.ietf.org/html/rfc2136 (citované na strane 168).

It takes 20 years to build
a reputation and few minutes of
cyber-incident to ruin it.

Stephane Nappo

Kapitola 9

Verejné obstarávanie

Richard Ostertág

Na kybernetickú bezpečnosť by sa malo myslieť od začiatku verejného obstarávania, keďže samotné obstarávanie ju môže netriviálnym spôsobom ovplyvniť a poskytnúť jej dobré (alebo zlé) základy. Cieľom tejto kapitoly je poukázať na niektoré základné formulácie využiteľné pri verejnom obstarávaní s cieľom pomôcť obstarávateľovi naplniť svoje bezpečnostné ciele. Vychádzame pritom najmä z materiálov publikovaných Ministerstvom financií SR (Sekcia informatizácie spoločnosti) v spolupráci s Úradom pre verejné obstarávanie [7, 8], Európskou agentúrou pre kybernetickú bezpečnosť (ENISA – The European Union Agency for Cybersecurity[1]) [3, 4] a Ministerstvom vnútornej bezpečnosti Spojených štátov (United States Department of Homeland Security) [2].

Podla zákona 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov[2] je verejným obstarávateľom (a teda verejné obstarávanie povinne používa):

- Slovenská republika zastúpená svojimi orgánmi,
- obec,
- vyšší územný celok,
- niektoré právnické osoby, ktoré sú založené alebo zriadené na osobitný účel plnenia potrieb všeobecného záujmu (bližšie pozri § 7 odsek 2 zákona 343/2015 Z. z.),
- združenie právnických osôb, ktorého členmi sú výlučne verejní obstarávatelia.

Z uvedeného vyplýva, že existujú rôzne sektory využívajúce verejné obstarávanie, ako napríklad štátna správa, zdravotníctvo, energetika, . . . , ako aj rôzne druhy verejného obstarávania, ktoré všetky majú svoje špecifiká. Navyše sa obstarávajú rôzne druhy tovaru, ako napríklad:

- hardvér (notebooky, stolové počítače, servery, sieťové komponenty, . . .),
- softvér (operačné systémy, kancelárske aplikácie, . . .)

alebo služieb (vývoj nového softvéru na zákazku, outsourcing niektorých činností, cloudové služby, školenia, testovanie, bezpečnostné analýzy, . . .). Z týchto dôvodov je táto kapitola len všeobecným úvodom do tejto problematiky a nemôže obsahovať informácie „šité na mieru“ konkrétnemu obstarávaniu.

[1] Skratka ENISA pochádza z pôvodného názvu: European Network and Information Security Agency.
[2] Zákon je prístupný aj online na adrese: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2015/343/.

9.1 Úvod

Obstarávateľ by mal najprv posúdiť riziká spojené s novým obstarávaním a špecifikovať požiadavky kybernetickej bezpečnosti pre obstarávaný tovar alebo službu. Následne je vhodné tieto požiadavky premietnuť do technickej špecifikácie a bezpečnostných funkcií obstarávaného produktu/služby. V súťažných podkladoch sa odporúča uviesť požiadavku zodpovednosti dodávateľa za bezpečnostné aspekty dodaného produktu/služby. S víťazným dodávateľom je potrebné uzatvoriť zmluvu, ktorá tieto podmienky obsahuje.

Po obstaraní produktu/služby by sa mala neustále monitorovať jeho kybernetická bezpečnosť (napríklad bezpečnostné incidenty a nové zraniteľnosti). V prípade identifikovania nedostatkov by sa mali vykonať nápravné opatrenia (napríklad zaplátanie, aktualizácia produktu) tak, aby sa trvalo udržala vysoká úroveň jeho bezpečnosti. Ako spomenieme neskôr v tejto kapitole, niektoré z týchto činností je možné požadovať od dodávateľa v rámci podpory. Na konci životného cyklu produktu je zas potrebné myslieť na jeho bezpečnú likvidáciu (napríklad z dôvodu ochrany osobných údajov, ktoré mohli byť v zariadení uložené).

V [3] sa spomína, že najväčšou výzvou sú bezpečnostné hrozby spojené s obstarávaniami, ktorých sa IT oddelenie obvykle nezúčastňuje. Keďže ide o štúdiu z oblasti nemocníc, mali na mysli obstarávanie špecifických medicínskych zariadení, ktoré na prvý pohľad nesúviseli s infomačnými technológiami a preto IT oddelenie nebolo k obstarávaniu prizvané. Dnes sa však mnohé moderné zariadenia často pripájajú do siete, priamo v sebe obsahujú softvér, prípadne treba ovládací softvér nainštalovať na počítač zamestnanca obsluhujúceho zariadenie. Moderné zariadenia často umožňujú vzdialenú správu, čím znižujú náklady na údržbu. Ak sú takéto zariadenia obstarané, nainštalované a nakonfigurované bez vedomia IT oddelenia, tak je väčšia pravdepodobnosť, že môžu pre útočníkov predstavovať zadné dvierka do organizácie. Takéto zariadenia však môžu existovať aj v iných odvetviach (napríklad elektronické zabezpečovacie systémy (EZS), kamerový dohľad, automatizácia a inteligentné riadenie budov, ...) a preto by malo byť dobrou praxou aspoň konzultovať obstarávanie akýchkoľvek zariadení, ktoré sa pripájajú do siete alebo sa k nim inštaluje nejaký softvér, s IT oddelením.

Je zvykom, že špecifikácia obstarávaného produktu sa vytvára na základe jeho prípadov použitia (use cases). Nesmie sa však zabúdať aj na prípady zneužitia (abuse cases). Obstarávateľ najneskôr po nasadení produktu zistí, ak nejaký prípad použitia nebol pokrytý alebo bol nesprávne špecifikovaný/implementovaný. Menej často sa však obstarávateľ, či dodávateľ, zamýšľa nad správaním produktu v neštandardnej situácii[3]. Takéto opomenutie môže viesť k rôznym zraniteľnostiam[4] vo výslednom produkte, ktoré môžu byť útočníkom zneužité (aj na diaľku). Preto je dôležité, aby obstarávateľ v špecifikácii myslel aj na tieto prípady a zahrnul do akceptačného testovania napríklad aj penetračné testovanie. Pokiaľ nemá obstarávateľ interné kapacity na vykonanie penetračného testovania, tak ho môže obstarať od tretej strany. V každom prípade je potrebné pôvodného dodávateľa zmluvne zaviazať k spolupráci pri penetračnom testovaní a uložiť mu povinnosť odstrániť zistené nedostatky.

[3] Napríklad pri neočakávaných vstupoch (neobvykle dlhý vstup, neočakávané znaky alebo hodnoty na vstupe, napr. záporná dĺžka, či počet kusov, ...), pri zaplnení úložného priestoru, pri strate sieťového pripojenia, pri neočakávanej postupnosti alebo súčasnej aktivácii ovládacích prvkov, ...

[4] Napríklad pretečenie vyrovnávacej pamäte (buffer overflow), vkladanie kódu (code injection), vyčerpanie zdrojov (resource exhaustion), ...

9.2 Legislatívny rámec

Pri definovaní bezpečnostných požiadaviek je dôležité zohľadňovať existujúcu legislatívu a štandardy. Tieto požiadavky by mali byť súčasťou technickej špecifikácie pre verejné obstarávanie. Nižšie uvádzame niektoré relevantné časti zákonov, vyhlášok, výnosov, ...:

- Zákon 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov[5].

  § 15, bod (2), písmeno d) Vo fáze prípravy a obstarania projektu je správca[6] *povinný akceptovať* také zmluvné podmienky, podľa ktorých:

  1. *zdrojový kód* vytvorený počas projektu *bude otvorený* v súlade s licenčnými podmienkami verejnej softvérovej licencie Európskej únie podľa osobitného predpisu[7], a to v rozsahu, v akom zverejnenie tohto kódu nemôže byť zneužité na činnosť smerujúcu k narušeniu alebo k zničeniu *informačného systému verejnej správy* (ďalej ISVS),
  2. *je jediným a výhradným disponentom so všetkými informáciami* zhromaždenými alebo získanými počas projektu a prevádzky projektom vytvoreného riešenia vrátane jeho zmien a servisu a
  3. *pri zmene dodávateľa pôvodný dodávateľ poskytne správcovi úplnú súčinnosť pri prechode na nového dodávateľa*, najmä v oblasti architektúry a integrácie informačných systémov.

  § 20 Bezpečnosť informačných technológií verejnej správy v oblasti obstarávania a implementácie

  (1) Správca pri vytváraní alebo nadobúdaní informačného systému verejnej správy

  a) určí bezpečnostné požiadavky na ISVS vrátane podmienok jeho vývoja, testovania a dodania v podmienkach vytvorenia alebo dodania ISVS,

  b) poskytne dodávateľovi ISVS pseudonymizované kópie údajov alebo fiktívne údaje na testovanie ISVS a jeho vývoj, ak poskytnutie údajov neznamená pre správcu neprimeranú záťaž s ohľadom na prínos poskytnutia pre testovanie a vývoj,

  c) zabezpečí pre tento systém vypracovanie bezpečnostného projektu podľa § 23 ods. 1 a 2.

  (2) Dodávateľ informačného systému verejnej správy pre vývoj tohto systému

  a) zabezpečí

[5] Zákon je prístupný aj online na adrese: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2019/95.

[6] Správcom na účely tohto zákona je ten orgán riadenia, ktorého za správcu informačnej technológie verejnej správy ustanoví zákon alebo je ustanovený na základe tohto zákona. Ak zákon vo vzťahu k informačnej technológii verejnej správy správcu neustanovuje, je správcom na účely tohto zákona ten orgán riadenia, ktorý informačnú technológiu verejnej správy používa na účely poskytovania služby verejnej správy, služby vo verejnom záujme alebo verejnej služby; ak je takýchto orgánov riadenia viac a jedným z nich je aj ústredný orgán štátnej správy, správcom je tento ústredný orgán štátnej správy.

[7] Vykonávacie rozhodnutie Komisie (EÚ) 2017/863 z 18. mája 2017, ktorým sa aktualizuje verejná **open source softvérová licencia Európskej únie** (EUPL) v záujme ďalšej podpory zdieľania a opätovného používania softvéru vyvinutého verejnými správami (Ú. v. EÚ L 128, 19. 5. 2017). Aktuálna verzia EUPL-1.2 je k dispozícii na adrese: https://joinup.ec.europa.eu/collection/eupl/eupl-text-eupl-12.

1. *bezpečné vývojové prostredie*,
2. *dokumentáciu vývoja vrátane používateľskej dokumentácie a administrátorskej dokumentácie.*

b) je oprávnený zabezpečiť *vytvorenie časti ISVS treťou osobou len po predchádzajúcom písomnom informovaní správcu*,

c) je povinný

1. dodržiavať mlčanlivosť o dodávanom ISVS aj po ukončení dodania a zaviazať rovnakou povinnosťou všetky osoby, ktoré sa na dodaní podieľali,
2. dodržiavať vhodné bezpečnostné mechanizmy a preukázať, že ich rozsah a úroveň zodpovedajú bezpečnostným požiadavkám podľa odseku 1 písmeno a),
3. identifikovať bezpečnostné požiadavky na ISVS podľa odseku 1 písm. a), ktoré nie sú pokryté týmto systémom, a predložiť správcovi návrh bezpečnostných opatrení na naplnenie týchto bezpečnostných požiadaviek pre prostredie, v ktorom bude ISVS prevádzkovaný,
4. upozorniť správcu na kritické časti alebo na rizikové časti ISVS, ktoré odhalí pri jeho dodaní, a navrhnúť opatrenia na ich riešenie,
5. *preukázateľne odstrániť alebo znemožniť používanie funkcie ISVS ktoré by jemu alebo tretej strane umožňovali získať neoprávnený prístup* do tohto systému a k údajom, ktoré obsahuje.

- Vyhláška 179/2020 Z. z. Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu, ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy[8].

§ 2 Bezpečnostné opatrenia

(1) Bezpečnostné opatrenia informačných technológií verejnej správy tvoria minimálne bezpečnostné opatrenia troch kategórií[9] pre jednotlivé oblasti podľa prílohy č. 2. Uvádzame vybrané časti zo všetkých kategórií informačných technológií verejnej správy:

D. Pri riadení prístupov sa hovorí podľa kategórie napríklad o zavedení pravidiel na zmenu používateľských hesiel s frekvenciou najmenej jeden rok, o presadzovaní určenej štruktúry hesla, o automatickom zaznamenávaní každého prístupu administrátora do informačných technológií verejnej správy, ako aj o automatickom zaznamenávaní prístupu používateľa, prípadne o implementácii centrálnej správy identít (IDM). Ďalej sa hovorí o *zamedzení možnosti zmeny log záznamov o prístupoch, o zamedzení možnosti vymazania týchto záznamov a o uchovávaní týchto záznamov šesť mesiacov*. Spomína sa aj používanie silných autentizačných metód na overenie identity

[8] Zákon je prístupný aj online na adrese: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2020/179.

[9] Pre podrobnejší popis rozdelenia do kategórií pozri § 3 tohto zákona. Kategórie sú tri: Kategória I, Kategória II a Kategória III (od najslabšej po najsilnejšiu). Napríklad minimálne bezpečnostné opatrenia Kategórie I jednotlivých oblastí kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahu k informačným technológiám verejnej správy sa vzťahujú na obec do 6 000 obyvateľov – § 3 ods. 2 písm. a). Kategória I a II sa vzťahuje na obec nad 6 000 obyvateľov – § 3 ods. 3 písm. a). Kategórie I, Kategórie II a Kategórie III sa vzťahujú na obec, ktorá je aj krajským mestom – § 3 ods. 4 písm. a).

používateľov, ako je viacfaktorová autentizácia pri informačných technológiách verejnej správy, ktoré obsahujú prísne chránené informačné aktíva v zmysle klasifikácie informačných aktív.

E. V časti s názvom „Riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami“ sa už v I. kategórii hovorí, že v zmluve s dodávateľmi musí byť určená požiadavka na dodržiavanie všetkých interných riadiacich dokumentov a všeobecne záväzných predpisov týkajúcich sa kybernetickej bezpečnosti a informačnej bezpečnosti.
Vo vyšších kategóriách majú zmluvné požiadavky na kybernetickú bezpečnosť a informačnú bezpečnosť obsahovať najmenej záväzok: riadenia a monitorovania prístupov do informačných technológií verejnej správy (vrátane spôsobu a mechanizmu), možnosti vykonávania kontrolných činností a auditu (vrátane rozsahu a spôsobu), *oznámenia všetkých bezpečnostných rizík, nedostatkov alebo zraniteľností* v rámci plnenia predmetu zmluvy (*ako aj povinnosť a proces ich ošetrenia*), *spolupráce pri riešení kybernetických bezpečnostných incidentov* a záväzok zachovania úrovne kybernetickej bezpečnosti a informačnej bezpečnosti pri významných zmenách *vrátane spôsobu a formy prechodu k inému dodávateľovi*.
Pri vývoji aplikácií a systémov realizovaných treťou stranou sa v zmluve majú jasne určiť podmienky týkajúce sa najmä autorských práv, práv duševného vlastníctva, bezpečnostných parametrov, bezpečnostného a funkčného testovania, legislatívnych a regulačných požiadaviek.

I. V časti „Sieťová a komunikačná bezpečnosť“ sa hovorí podľa kategórie napríklad o tom, že všetky koncové stanice majú byť chránené prostredníctvom softvérového personálneho firewallu. Na sieťových zariadeniach sa má pravidelne aktualizovať firmvér, je potrebné zmeniť továrensky nastavené autentifikačné údaje, . . . , má sa vypnúť možnosť správy zariadenia na diaľku alebo prijať iné opatrenia zabraňujúce zneužitiu vzdialeného prístupu. V kategórii III sa majú nasadiť aj systémy na detekciu a prevenciu prieniku a webové aplikačné firewally.

J. „Akvizícia, vývoj a údržba informačných technológií verejnej správy“ spomína napríklad, že informácie prenášané prostredníctvom verejných sietí sa šifrujú alebo iným adekvátnym opatrením chránia najmä pred neoprávneným prístupom, modifikáciou alebo nedostupnosťou. Tiež že, súčasťou akceptačného testovania informačných technológií verejnej správy je aj testovanie implementovaných bezpečnostných opatrení najmä bezpečnostne dôležitých prvkov aplikácií, alebo systémov, ako sú autentizačné, autorizačné mechanizmy, prístupové roly a ďalšie opatrenia zaisťujúce požadovanú dôvernosť, dostupnosť a integritu.

K. V časti „Zaznamenávanie udalostí a monitorovanie“ sa požaduje minimálne zaznamenávanie úspešných a neúspešných autentifikačných udalostí. Podrobnejšie sa téme vytvárania záznamov venuje časť 9.3.4 tejto kapitoly.

- Výnos 525/2011 Z. z. Ministerstva vnútra Slovenskej republiky o štandardoch pre elektronické informačné systémy na správu registratúry[10].

[10]Zákon je prístupný aj online na adrese: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2011/525.

- Vyhláška 248/2015 Z. z. Národného bezpečnostného úradu, ktorou sa mení a dopĺňa vyhláška Národného bezpečnostného úradu č. 136/2009 Z. z. o spôsobe a postupe používania elektronického podpisu v obchodnom styku a administratívnom styku[11].

- Zákon 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov[12].

  § 19 Povinnosti prevádzkovateľa základnej služby

  (2) Prevádzkovateľ základnej služby je povinný pri uzatvorení zmluvy s dodávateľom na výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre prevádzkovateľa základnej služby (ďalej len „tretia strana“) *uzatvoriť zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností* podľa tohto zákona počas celej doby platnosti zmluvy.

  (6) Prevádzkovateľ základnej služby je ďalej povinný

  a) riešiť kybernetický bezpečnostný incident,

  b) bezodkladne hlásiť závažný kybernetický bezpečnostný incident,

  c) spolupracovať s úradom a ústredným orgánom pri riešení hláseného kybernetického bezpečnostného incidentu a na tento účel im poskytnúť potrebnú súčinnosť, ako aj informácie získané z vlastnej činnosti dôležité pre riešenie kybernetického bezpečnostného incidentu,

  d) v čase kybernetického bezpečnostného incidentu zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní,

  e) oznámiť orgánu činnému v trestnom konaní alebo Policajnému zboru skutočnosti, že bol spáchaný trestný čin, ktorého sa kybernetický bezpečnostný incident týka, ak sa o ňom hodnoverným spôsobom dozvie.

  Obstarávateľ by mal myslieť na tieto vyššie (ako aj obdobné nižšie) uvedené povinnosti už pri špecifikácii predmetu obstarávania a napríklad požadovať vytváranie záznamov napomáhajúcich riešeniu incidentu a napríklad aj spoluprácu dodávateľa pri jeho riešení (ak už tieto požiadavky nie sú zahrnuté z iných vyššie spomínaných dôvodov).

- Zákon 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov[13].

  § 11 Zásada integrity a dôvernosti – Osobné údaje musia byť spracúvané spôsobom, ktorý prostredníctvom primeraných technických a organizačných opatrení zaručuje primeranú bezpečnosť osobných údajov vrátane ochrany pred neoprávneným spracúvaním osobných údajov, nezákonným spracúvaním osobných údajov, náhodnou stratou osobných údajov, výmazom osobných údajov alebo poškodením osobných údajov.

- Nariadenie Európskeho parlamentu a rady Európskej únie 2016/679[14] z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (General Data Protection Regulation – GDPR)

[11] Zákon je prístupný aj online na adrese: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2015/248.
[12] Zákon je prístupný aj online na adrese: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/69.
[13] Zákon je prístupný aj online na adrese: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/18.
[14] Nariadenie je prístupné aj online na adrese: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

  - Oddiel 2 (Bezpečnosť osobných údajov), článok 33 (Oznámenie porušenia ochrany osobných údajov dozornému orgánu) bod 1. v prípade porušenia ochrany osobných údajov ukladá prevádzkovateľovi bez zbytočného odkladu a podľa možnosti najneskôr do 72 hodín po tom, čo sa o tejto skutočnosti dozvedel, oznámiť porušenie ochrany osobných údajov dozornému orgánu príslušnému podľa článku 55 s výnimkou prípadov, keď nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva a slobody fyzických osôb.

- Smernica Európskeho parlamentu a rady Európskej únie 2016/1148[15] zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (The Network and Information Security directive – NISD[16]).

  - V článku 4 bod 4 a prílohe II definuje prevádzkovateľov základných služieb. Na najvyššej úrovni ide o odvetvia: energetika, doprava, bankovníctvo, infraštruktúry finančných trhov, zdravotníctvo, dodávka a distribúcia pitnej vody, digitálna infraštruktúra (internetové prepojovacie uzly, poskytovatelia služieb DNS, registre domén najvyššej úrovne).
  - Článok 14 (Bezpečnostné požiadavky a oznamovanie incidentov) stanovuje prevádzkovateľom základných služieb povinnosť bez zbytočného odkladu oznamovať príslušnému orgánu alebo jednotke CSIRT incidenty, ktoré majú závažný vplyv na kontinuitu základných služieb, ktoré poskytujú.

  V niektorých prípadoch by sa oznamovanie malo šíriť po reťazci dodávateľov až smerom k obstarávateľovi. Obstarávateľ by mal zaviazať dodávateľov k tejto povinnosti už pri špecifikácii verejného obstarávania.

- Nariadenie Európskeho parlamentu a rady Európskej únie 2017/745[17] z 5. apríla 2017 o zdravotníckych pomôckach, zmene smernice 2001/83/ES, nariadenia (ES) č. 178/2002 a nariadenia (ES) č. 1223/2009 a o zrušení smerníc Rady 90/385/EHS a 93/42/EHS (Medical Devices Regulation (EU) 2017/745 – MDR). V prílohe I (Všeobecné požiadavky na bezpečnosť a výkon) sa okrem iného požaduje:

  - V prípade pomôcok so zabudovaným softvérom alebo v prípade softvéru, ktorý je sám osebe pomôckou, sa takýto softvér musí naprogramovať a vyrobiť v súlade s najnovšími poznatkami vedy a techniky v odvetví s prihliadnutím na zásady *životného cyklu daného vývoja*, riadenia rizík vrátane *bezpečnosti informácií*, overovania a validácie[18].
  - MDCG (Medical Device Coordination Group) vydal v decembri 2019 „Guidance on Cybersecurity for medical devices“ [6], aby poskytol výrobcom pomoc s naplnením požiadaviek MDR.

  Dodržanie správneho životného cyklu vývoja a ostatných požiadaviek MDR je potrebné zachytiť už v špecifikácii pre verejné obstarávanie.

[15] Smernica je prístupná aj online na adrese: https://eur-lex.europa.eu/eli/dir/2016/1148/oj.
[16] NISD je prístupné aj online na adrese: https://www.enisa.europa.eu/topics/nis-directive.
[17] Nariadenie je prístupné aj online na adrese: https://eur-lex.europa.eu/eli/reg/2017/745/oj.
[18] The software shall be developed and manufactured in accordance with the state of the art taking into account the principles of development life cycle, risk management, including information security, verification and validation.

9.3 Vybrané formulácie

V tejto časti uvedieme príklady formulácií pre niektoré vybrané oblasti týkajúce sa verejného obstarávania. Upozorňujeme čitateľa, že existujú aj ďalšie oblasti, napríklad ďalšie sieťové komponenty (smerovače, load balancery, proxy, gateways rôzneho druhu, ...), alebo systémy elektronickej pošty, databázy, bezpečnostné riešenia (AV, SIEM, VPN, PKI, ...), ktoré všetky tiež majú svoje vlastné špecifiká.

9.3.1 Odstránenie nepotrebných služieb a programov

Počítače, notebooky, mobilné telefóny a iné zariadenia sa často dodávajú s rôznymi predinštalovanými programami a povolenými službami. Môže ísť od nástrojov pre diagnostiku systému, programy pre informovanie zákazníka o nových produktoch dodávateľa/výrobcu, četovacie programy, ..., až po rôzne hry. Tieto nepotrebné programy a služby zbytočne zväčšujú priestor pre útoky (attack surface). Niektoré z nich majú známe bezpečnostné zraniteľnosti a existujú rôzne útoky/nástroje na využitie týchto zraniteľností k ohrozeniu systému. Navyše nepoužívané služby/programy často nie sú ani monitorované, či aktualizované.

Formulácie

Pred dodaním a akceptačným testovaním musí dodávateľ deaktivovať a/alebo odstrániť všetky softvérové komponenty, ktoré nie sú potrebné na prevádzku a údržbu dodávaného zariadenia. Dodávateľ poskytne dokumentáciu o tom, čo je deaktivované a/alebo odstránené. Softvér, ktorý sa má odstrániť alebo aspoň deaktivovať, musí okrem iného zahŕňať:

- Hry, četovacie programy, reklamné programy, ...
- Servre a klientov pre nepoužívané internetové služby.
- Nepotrebné kompilátory a interpretre programovacích jazykov (C, Python, Perl, ...).
- Nepoužívané sieťové a komunikačné protokoly.
- Nepotrebné administratívne a diagnostické nástroje.
- Nepotrebné súbory. Napríklad zdrojové kódy, databázy a programy použité iba počas vývoja aplikácie. Rovnako dodávateľ odstráni aj všetky nepoužívané dáta a konfiguračné súbory, ukážkové programy a skripty.
- Nepotrebné aplikácie na spracovanie dokumentov (napr. Microsoft Office, OpenOffice, Adode Acrobat, ...[19]).
- Nepoužívané prehliadače a ich rozšírenia.

Kontroly

Dodávateľ poskytne dokumentáciu o deaktivovaných a/alebo odstránených softvérových komponentoch. Pri akceptačnom testovaní sa overí, že sú v dokumentácii uvedené všetky relevantné komponenty a že sú v dodávanom systéme naozaj deaktivované alebo odstránené.

[19] Uvedené produkty sú len príkladom produktov z danej kategórie, ktorý nepredstavuje odporúčanie alebo neodporúčanie daného produktu, rodiny produktov alebo výrobcu.

Údržba

Kedykoľvek je produkt aktualizovaný, odporúča sa vykonať pred jeho nasadením u obstarávateľa vhodnú podmnožina akceptačných testov za účelom overenia, že nie je opätovne aktivovaný niektorý z deaktivovaných alebo odstránených softvérových komponentov.

Referencie

[2, bod 2.1], [1, body 2.1.1 a 2.1.3]

9.3.2 Aktualizácia softvéru a firmvéru

V produktoch sa neustále objavujú nové zraniteľnosti[20]. Zodpovední dodávatelia preto pravidelne vydávajú aktualizácie pre svoje produkty, v ktorých sa snažia odstrániť zistené bezpečnostné nedostatky. Pred ich nasadením na produkčnom systéme je dobrým zvykom aktualizácie najprv otestovať a overiť si, či neprinášajú do systému nejaké nové regresie.

Formulácie

1. Dodávateľ zabezpečí, že všetky dodané softvérové komponenty (firmvér, operačný systém, aplikácie) sú aktualizované na aktuálny stav v čase ich inštalácie u obstarávateľa, o čom poskytne aj dokumentáciu.

2. Dodávateľ zabezpečí (v rámci vopred dohodnutého obdobia) aktualizácie dodaných softvérových komponentov odstraňujúce všetky zraniteľnosti[21] v dodanom produkte pri zachovaní bezpečnostnej úrovne stanovenej v špecifikácii obstaraného produktu. Tieto aktualizácie poskytne obstarávateľovi do zmluvne stanoveného času od ich objavenia. Aktualizácie odstraňujúce kritické zraniteľnosti budú poskytnuté v dohodnutom kratšom čase (oproti aktualizáciám pre ostatné menej závažné zraniteľnosti).

3. Pokiaľ dodávateľ nemôže poskytnúť aktualizácie v stanovenom čase, tak poskytne v dohodnutom čase aspoň iné dočasné riešenie (workaround), ktoré zamedzí zneužitiu zraniteľnosti do vytvorenia aktualizácie.

4. Povinnosť dodávateľa zabezpečiť aktualizácie (ak výrobca komponentu takú aktualizáciu vydal) alebo iné dočasné riešenie sa vzťahuje aj na komponenty tretích strán, ktoré dodávateľ zahrnul do dodaného riešenia.

5. Dodávateľ zabezpečí distribúciu nových aktualizácií tak, aby bola overiteľná ich integrita a autentickosť. Systém musí byť navrhnutý tak, aby neumožnil nainštalovať aktualizáciu bez overenia jej integrity a autentickosti.

[20] Pozri napríklad: https://cve.mitre.org/cve/search_cve_list.html.

[21] Ak niektoré komponenty dodávateľ nevyvíjal (napr. ide o produkty tretej strany, ktoré len integroval do riešenia), musí si dodávateľ ich aktualizácie zmluvne zabezpečiť od výrobcu (pokiaľ sa dodávateľ s obstarávateľom nedohodli na inom režime aktualizácií pre tento komponent).

Kontroly

1. Dodávateľ poskytne dokumentáciu o aktualizácii softvérových komponentov (na akom zariadení, aký komponent, na akú verziu, kedy bol aktualizovaný).
2. Dodávateľ poskytne dokumentáciu k svojmu procesu správy aktualizácií (patch management). Táto dokumentácia by mala najmä:
   - obsahovať popis zdrojov a technických schopností dodávateľa potrebných na udržanie tohto procesu,
   - dokladovať schopnosť dodávateľa opraviť nové zraniteľnosti minumálne v ním vyvynutých komponentoch,
   - dokladovať schopnosť dodávateľa zabezpečiť aktualizácie pre integrované komponenty tretích strán (pokiaľ ich výrobca vydal),
   - dokladovať schopnosť dodávateľa vyvinúť iné dočasné riešnie na preklenutie obdobia kým výrobca takú aktualizáciu vydá.

Údržba

Kedykoľvek je produkt aktualizovaný, odporúča sa vykonať pred jeho nasadením u obstarávateľa vhodnú podmnožinu akceptačných testov potvrdzujúcu, že systém stále vyhovuje špecifikácii a že nenastala regresia (napríklad zníženie výkonu oproti predošlej verzii).

Referencie

[2, bod 2.1], [1, bod 3.4]

9.3.3 Spoľahlivosť

Obstarávateľ nemusí prevádzkovať všetky svoje informačné systémy na svojich vlastných serveroch. Niektoré informačné systémy môžu byť obstarávateľom prevádzkované na outsourcovanej infraštruktúre (IaaS, prípadne PaaS) alebo celý informačný systém môže byť outsourcovaný (SaaS)[22]. Obstarávateľ sa týmto stáva závislý na outsourcovaných službách (napríklad na cloudových službách). Rovnako výpadok internetového pripojenia, zlyhanie samotnej lokálnej siete (či už jej aktívnych alebo pasívnych prvkov) alebo výpadok dodávky elektrickej energie môže mať za následok nedostupnosť týchto informačných systémov, čo podľa ich povahy a dĺžky trvania výpadku môže mať až zničujúce následky.

Formulácie

Na zmiernenie takejto hrozby je možné aplikovať opatrenia ako redundanciu, správny návrh topológie siete, záložné riešenia, garantovanú úroveň služieb a schopnosť systému pracovať aj offline. To podľa typu obstarávanej služby môže viesť napríklad k nasledovným formuláciám:

1. Dodávateľ bude poskytovať službu podľa parametrov definovaných v technickej špecifikácii. V prípade ich nedodržania sa zaväzuje uhradiť obstarávateľovi zmluvnú pokutu.

[22] Pre vysvetlenie pojmov IaaS, PaaS, SaaS pozri časť 4.4 „Virtualizácia, cloud“ na strane 78.

Takýmito parametrami môžu byť podľa druhu služby napríklad: úroveň dostupnosti, čas odozvy, priepustnosť[23], stredná doba medzi poruchami (Mean Time Between Failures – MTBF[24]), priemerná doba opravy (Mean Time To Repair – MTTR), ...

V špecifikácii dostupnosti môžu byť naplánované servisné okná (s vopred stanovenou periódou a v určenom časovom intervale), ktoré sa nezarátavajú do merania dostupnosti. Napríklad: „Priebežná servisná údržba systému sa vykonáva raz za polroka v noci zo soboty na nedeľu v čase od 01:00 do 02:00 hodiny. Presný dátum vykonanie aktualizácie oznámi dodávateľ minimálne sedem dní vopred."

Pokiaľ ide o garanciu dostupnosti, zvykne sa uvádzať v percentách z času poskytovania služby. V tabuľke 9.1 je znázornené, čo to v praxi znamená[25].

Tabuľka 9.1: Maximálne celkové povolené trvanie výpadku (h:mm:ss,ss) pre jednotlivé úrovne dostupnosti.

Dostupnosť	Denne	Týždenne	Mesačne	Ročne
90 %	2:24:00,00	16:48:00,00	3 dni 1:02:54,38	36 dní 12:34:52,60
99 %	14:24,00	1:40:48,00	7:18:17,44	3 dni 15:39:29,26
99,9 %	1:26,40	10:04,80	43:49,74	8:45:56,93
99,99 %	8,64	1:00,48	4:22,97	52:35,69
99,999 %	0,86	6,05	26,30	5:15,57

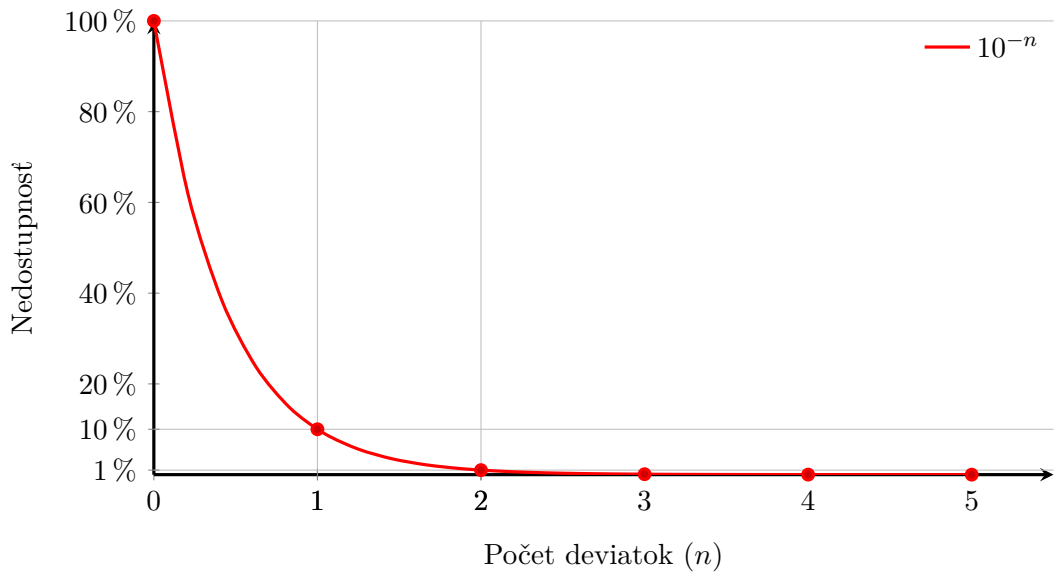
Napríklad 99,9 % dostupnosť môže v skutočnosti znamenať výpadok až na vyše osem hodín ročne. Pokiaľ by sa celý tento čas sústredil do jedného výpadku, tak je to jeden celý pracovný deň (alebo jedna pracovná zmena). Takýto výpadok môže spôsobiť organizácii oveľa vážnejšie škody ako napríklad výpadok na cca minútu a pol denne. Pritom za rok ide celkovo zhruba o rovnaký čas nedostupnosti služby a teda stále o rovnakú 99,9 % dostupnosť. Preto pri špecifikovaní dostupnosti je nutné myslieť aj na ďalšie parametre, ako napríklad maximálnu súvislú dobu trvania výpadku, minimálny čas dostupnosti, po ktorom sa považuje služba za obnovenú, granularitu dostupnosti (teda či daná dostupnosť má byť dodržaná na dennej, týždennej, mesačnej alebo ročnej báze).

Na obrázku 9.1 je znázornený exponenciálny pokles nedostupnosti (os Y) s rastom počtu deviatok (os X) v požadovanej úrovni dostupnosti (jedna deviatka – 90 %, ..., tri deviatky – 99,9 %, ...). Treba si uvedomiť, že pridaním jednej deviatky sa zmenší nedostupnosť desaťnásobne. Tomu môže následne zodpovedať exponenciálny nárast nákladov na zabezpečenie vyššej úrovne dostupnosti. Preto je dôležité správne vyvážiť úroveň požadovanej dostupnosti s nákladmi na jej udržanie.

Výška zmluvne stanovenej pokuty za nedodržanie parametrov služby by mala zodpovedať vzniknutej škode (ušlý zisk, strata dobrého mena, ...). Môže sa teda odvíjať od závažnosti porušeného parametra, miery jeho porušenia a doby trvania tohto porušenia.

2. Dodávateľ implementuje aplikáciu tak, aby mohla dočasne pracovať aj bez sieťového pripojenia. (Napríklad zber údajov môže prebiehať aj bez sieťového spojenia. Údaje sa

[23] Pre podrobnejšiu diskusiu o odozve a priepustnosti pozri časť 9.3.7 „Výkon" na strane 252.
[24] Obvykle sa udáva v hodinách. Napríklad pre disky býva zvyčajne v rozpätí 300 000 až 2 500 000 hodín.
[25] Hodnoty pre inú úroveň dostupnosti je možné ľahko vypočítať napríklad na stránke: https://uptime.is.



Obr. 9.1: Exponenciálny pokles nedostupnosti s rastom počtu deviatok.

budú ukladať lokálne. Po obnovení spojenia sa zozbierané a lokálne uložené údaje zapíšu na server.) Je možné požadovať aj odolnosť systému voči výpadku niektorých jeho častí, či služieb z ktorých pozostáva (obvykle riešiteľné pomocou redundancie).

3. Dodávateľ navrhne topológiu siete a jej aktívne komponenty tak, aby odolala výpadku ľubovoľného spojenia alebo aktívneho komponentu a/alebo bude v pohotovosti (v pracovné dni, prípadne aj cez víkendy a sviatky) a výpadok odstráni (t.j. identifikuje problém a následne vykoná potrebnú opravu alebo výmenu) v dohodnutom čase od nahlásenia výpadku dodávateľovi. Výpadok sa považuje za odstránený, až keď je bezchybná prevádzka obnovená aspoň na stanovenú minimálnu dobu.

Kontroly

1. Uzavretie zmluvy o poskytovaní služby, ktorej časťou je aj dohoda o garantovanej úrovni poskytovanej služby (Service-Level Agreement – SLA). Obstarávateľ by mal priebežne monitorovať parametre poskytovanej služby.

2. Pri akceptačnom testovaní sa overí, že aplikácia dokáže dočasne pracovať aj bez sieťového pripojenia a že po jeho obnovení sa údaje so serverom zosynchronizujú.

3. Pri akceptačnom testovaní sa minimálne experimentálne overí, že sieť odolá odpojeniu ľubovoľného spojenia alebo aktívneho prvku a/alebo sa uzavrie zmluva o servise s požadovaným časom na odstránenie poruchy.

Údržba

1. V prípade, že sa pre organizáciu zmení dôležitosť poskytovanej služby, tak je vhodné[26] túto skutočnosť prerokovať s dodávateľom a po vzájomnej dohode adekvátne upraviť SLA (môže ísť o sprísnenie podmienok, ak sa stala služba dôležitejšou alebo aj o ich uvoľnenie, ak je menej dôležitá – cieľom je potom ušetriť na jej prevádzke).
2. Pri rozširovaní alebo iných úpravách siete je potrebné požadovať a zachovať stanovenú mieru jej odolnosť voči výpadkom.

Referencie

[3, bod 3.1.2], [8, bod 3.3]

9.3.4 Vytváranie záznamov (audit logs)

> There are only two types of companies: those that have been hacked and those that will be.
>
> Robert Mueller, 2012

Ak predpokladáme, že každý systém bude skôr či neskôr napadnutý, tak vytváranie záznamov (protokolov, logov) je jedným z najužitočnejších nástrojov, pomocou ktorých môžeme spätne zistiť, ako útočníci získali prístup do napadnutého systému. Rovnako nám umožnia vyhodnotiť, o ktoré časti systému mali záujem, aké informácie boli zmenené alebo unikli a v neposlednom rade pomáhajú identifikovať útočníkov. Protokolovanie (vytváranie záznamov o činnosti) je teda dôležité pre forenznú analýzu a zisťovanie anomálií.

Pokročilejší útočníci sa snažia upraviť na napadnutom systéme záznamy tak, aby zahladili stopy svojej činnosti. Aby ich útočník nemohol modifikovať, tak musia byť samotné protokoly uložené bezpečným spôsobom (napríklad na oddelenom serveri, na ktorý sa záznamy o činnosti odosielajú po sieti alebo sa záznamy zapíšu na WORM médium). V niektorých aplikáciách môže byť implementácia protokolovania dokonca zákonnou požiadavkou pre prevádzku systému.

Záznamy by okrem popisu samotnej udalosti mali obsahovať aspoň dátum a presný čas jej vzniku, identifikáciu zariadenia (na ktorom vznikla), identifikáciu používateľa a procesu, ktorý ju inicioval, indikáciu úspešnosti alebo zlyhania operácie a pri sieťových službách aj protokol, zdrojovú a cieľovú IP adresu a port.

Podľa kategórie systému by mali byť protokolované napríklad nasledovné udalosti[27]:

- úspešný a neúspešný pokus o prihlásenie
- požiadavka na autentizačné služby (vrátane označenia požadujúcej entity)
- vytváranie, úprava (napríklad zmena hesla) a mazanie používateľských účtov alebo skupín
- dôležité transakcie (napríklad presun finančných prostriedkov)

[26] Pokiaľ je z legislatívneho hľadiska možné meniť podmienky zmluvy (priebežne, k výročiu, pri predlžovaní, nové obstarávanie).

[27] Pozri napríklad vyhlášku č. 179/2020 Z. z. na strane 236, príloha č. 2, časť K.

- spustenie, vypnutie alebo reštartovanie služby, či procesu
- chybové stavy systému, výnimky
- dôležité zmeny v konfigurácii systému
  - obzvlášť zmeny bezpečnostných nastavení a politík
- aktivácia a deaktivácia bezpečnostných mechanizmov
- zmeny v prístupových oprávneniach
- požiadavky a odpovede klienta pokúšajúce sa o známe útoky
- úspešné a neúspešné
  - privilegované operácie
  - prístupy k záznamom o činnosti
  - prístupy k systémovým zdrojom
- významné aktivity v sieťovej komunikácii
- IP adresy pridelené prostredníctvom služby DHCP (aby bolo možné dynamicky prideľované adresy jednoznačne spojiť s konkrétnym používateľom pre daný čas)

Pri protokolovaní je potrebné pamätať na rezervovanie dostatočnej kapacity pre vytvárané záznamy. Keďže protokolovanie bez následného vyhodocovania záznamov je málo užitočné, tak treba pamätať aj na to, kto, kedy, akým spôsobom bude záznamy vyhodnocovať a čo sa má stať, ak sa v záznamoch identifikuje niečo podozrivé.

Formulácie

1. Dodávateľ implementuje protokolovanie, pomocou ktorého sa zaznamená všetka relevantná aktivita v systéme v súlade s obstarávateľovými bezpečnostnými požiadavkami. Systém musí aj so zapnutým a dlhodobo prevádzkovaným protokolovaním spĺňať v špecifikácii stanovené výkonové požiadavky.

2. Dodávateľ v dodávanom systéme implementuje synchronizáciu času (napríklad pomocou NTP – Network Time Protocol) s autoritatívnym zdrojom času (napríklad s GPS – Global Positioning System, s DCF77 alebo s dôveryhodným internetovým časovým serverom).

3. Dodávateľ realizuje uloženie protokolov bezpečným spôsobom tak, aby ich útočník nemohol modifikovať ani v prípade napadnutia protokolovaného počítača.

4. Dodávateľ v dokumentácii k produktu popíše všetky možnosti protokolovania, jeho formát, správu a preddefinované nastavenia.

Kontroly

1. Obstarávateľ overí, že implementované protokolovanie pokrýva všetky požiadavky.

2. Vykoná sa meranie výkonu systému, za účelom overenia, či systém aj s aktívnym protokolovaním všetkých požadovaných činností spĺňa výkonové požiadavky.

Údržba

1. Archivácia záznamov z protokolovania.
2. Pravidelná kontrola protokolov spojená s analýzov podozrivých záznamov.
3. V prípade zmeny alebo rozšírení systému sa musí adekvátne zmeniť alebo rozšíriť aj protokolovanie jeho činnosti.

Referencie

[3, bod 3.1.3], [2, bod 4.4], [1, body 2.6.1, 2.6.2 a 2.6.7], vyhláška 179/2020 Z. z. príloha 2. bod K.

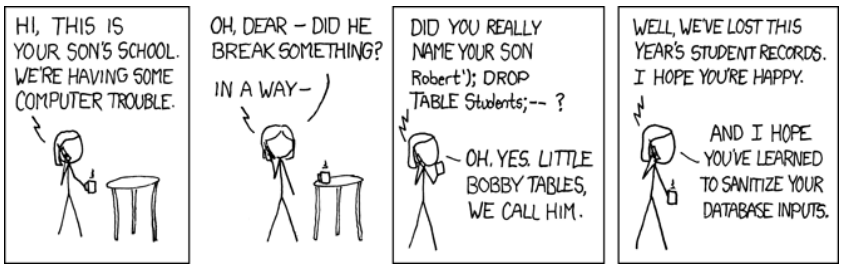
9.3.5 Postupy bezpečného vývoja

Pri vývoji softvéru sa neskúsení programátori zameriavajú iba na samotnú požadovanú funkcionalitu (spracovanie údajov). Niekedy aj kvôli časovému stresu alebo finančným obmedzeniam nie je dostatočný priestor pre zamyslenie sa nad neštandardnými situáciami (ktoré potenciálne môžu nastať) a nad ich bezpečnostnými dôsledkami. Tieto okolnosti sú potom príčinou vytvorenia programov, ktoré síce za bežných okolností robia to, čo sa od nich požaduje, ale v špeciálnych situáciách sa správajú nekorektne (napríklad vôbec nedajú výsledok, dajú zlý výsledok alebo vykonajú činnosti nad rámec ich špecifikácie).

Softvérové chyby sú primárnou cestou k získaniu prístupu do systému. Mnohé bezpečnostné zraniteľnosti sú priamym dôsledkom nedostatočnej pozornosti venovanej ochrane pred cielene zostavenými škodlivými vstupmi. Medzi najznámejšie takéto útoky patria:

- **Pretečenie vyrovnávacej pamäte (buffer overflow)** — Ako vstupné dáta sú použité dlhé postupnosti znakov/bajtov, ktoré spôsobia zaplnenie pamäte rezervovanej pre vstup a prepísanie pamäte nachádzajúcej sa za touto oblasťou[28]. Toto útočník obvykle využije k prepísaniu časti programu vhodne zvoleným vlastným programom. Po jeho vykonaní môže v niektorých prípadoch získať až vzdialený prístup k príkazovému riadku na serveri, kde beží napadnutá aplikácia.
- **Vkladanie kódu (code injection)** — Ide o širokú škálu útokov. Ich základná myšlienka je jednoduchá. Aplikácia často potrebuje na základe vstupu od používateľa vytvoriť reťazec – postupnosť znakov – predstavujúcu príkaz, ktorý sa dá vykonať nejakej inej časti systému (napríklad databáze). Označme takýmto spôsobom *dáta* a takýmto **príkazy**.
  - Nech databáza podporuje príkazy v podobe reťazcov:
    - pre vloženie nového používateľa v tvare: **Vlož:"***Meno***"**,
    - pre zmazanie používateľa v tvare: **Zmaž:"***Meno***"**.
  - Viacero príkazov je možné spojiť do jedného „zloženého“ príkazu oddelením samostatných príkazov znakom bodkočiarky. Napríklad: **Vlož:"***Meno***";Zmaž:"***Meno***"**.

[28] Dajme tomu, že programátor s veľkou rezervou vyhradil pre meno používateľa dvesto znakov. Ak však útočník zadá meno dĺžky povedzme tristo znakov a programátor neoveruje dĺžku vstupu, ale rovno ho zapíše do vyhradeného priestoru, tak sto znakov za vyhradeným priestorom bude prepísaných.



Obr. 9.2: Známy vtip o SQL injection. Zdroj: https://xkcd.com/327.

– Programátor môže implementovať vytvorenie vlož-príkazu jednoduchým spojením reťazcov `Vlož:"`, *`Meno`* a `"`, pričom reťazec `Meno` je zadaný používateľom.

  Ak útočník ako svoje meno zadá reťazec `MenoA";Zmaž:"MenoB`, tak uvedeným spojením reťazcov vznikne jeden reťazec `Vlož:"MenoA";Zmaž:"MenoB"`. My by sme ho chceli chápať ako príkaz: `Vlož:"`*`MenoA";Zmaž:"MenoB`*`"`, ktorý vytvorí záznam pre nového používateľa s divným menom `MenoA";Zmaž:"MenoB`. Databáza ho však interpretuje ako dva príkazy: `Vlož:"`*`MenoA`*`";Zmaž:"`*`MenoB`*`"`, a tak vytvorí záznam pre nového používateľa s menom `MenoA` a zároveň zmaže záznam pre používateľa s menom `MenoB`. Podobný prípad je základom vtipu na obrázku 9.2.

Postupy bezpečného vývoja produktu (secure product development practices) sú súborom procesov integrovaných do životného cyklu vývoja systému (System Development Life Cycle – SDLC), ktoré znižujú bezpečnostné riziká výsledného produktu. Tieto postupy pomáhajú vyvíjať robustnejší hardvér, softvér a firmvér s menšími počtom zraniteľností. Postupy bezpečného vývoja zaisťujú, že bezpečnosť je integrovaná do všetkých fáz životného cyklu vývoja systému a považuje sa za ich kľúčovú súčasť.

Formulácie

1. Dodávateľ predloží súhrnnú dokumentáciu popisujúcu zohľadnenie bezpečnosti v jednotlivých fázach vývoja/úpravy dodávaného systému a to vrátane použitých štandardov a odporúčaných postupov (vrátane procesu neustáleho zlepšovania[29] a postupov bezpečného vývoja/programovania).

   Dodávateľ zdokumentuje (ak to bude potrebné), ako predchádza najzávažnejším zraniteľnostiam (vrátane OWASP Top 10[30] alebo SANS Top 25[31] najnebezpečnejších softvérových chýb) počas všetkých fáz životného cyklu vývoja systému.

2. Dodávateľ zdokumentuje svoj program zabezpečenia kvality a potvrdí, že obstarávaný produkt prešiel testom kontroly kvality s cieľom identifikovať a opraviť potenciálne bezpečnostné zraniteľnosti. Toto testovanie[32] musí zahŕňať minimálne fuzzy testovanie, sta-

[29] Napríklad podľa ISO/IEC TR 33014:2013 Information technology – Process assessment – Guide for process improvement (https://www.iso.org/standard/54186.html).

[30] Zoznam OWASP Top 10 je prístupný na stránke: https://owasp.org/www-project-top-ten/.

[31] Zoznam SANS Top 25 je prístupný na stránke: https://www.sans.org/top25-software-errors.

[32] Úlohou tohto testovania nie je nahradiť napríklad penetračné testovanie vykonané obstarávateľom alebo treťou stranou počas akceptačného testovania, ale zdokladovať kvalitu bezpečného vývoja u dodávateľa.

tické testovanie, dynamické testovanie a penetračné testovanie. Rovnako je dodávateľ povinný pomocou vhodných testov overiť, že obstaraný produkt funguje v súlade s požiadavkami a bez ďalších funkcií navyše, ako aj monitorovať neočakávané alebo nežiaduce správanie počas testov.

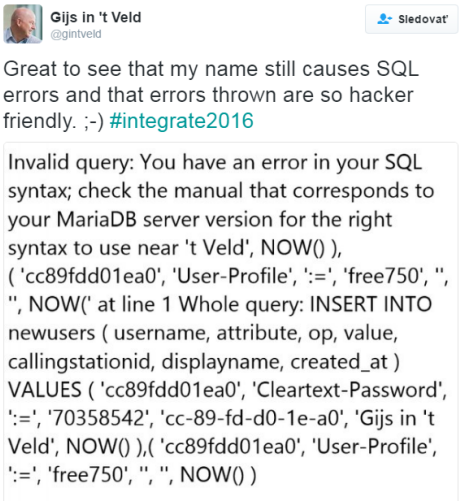
Testovanie môže vykonať dodávateľ sám alebo ním môže poveriť nezávislú tretiu stranu. Dodávateľ poskytne súhrnnú dokumentáciu o výsledkoch testovania.

3. Dodávateľ poskytne plán na udržanie bezpečnosti obstarávaného produktu aj v prípade, že by ukončil podnikanie. Napríklad niektoré interné bezpečnostne relevantné informácie, postupy, či produkty môžu byť umiestnené v notárskej úschove a odovzdané obstarávateľovi v prípade zániku dodávateľa.

Kontroly

1. Obstarávateľ má právo požadovať od dodávateľa dokumentáciu popisujúcu dodávateľov prístup ku kybernetickej bezpečnosti, vrátane výsledkov jeho posledného bezpečnostného auditu. Alternatívne môže mať obstarávateľ právo vykonávať pravidelný audit kybernetickej bezpečnosti v priestoroch dodávateľa (v dohodnutej frekvencii a rozsahu). Obstarávateľ môže poveriť vykonaním tohto bezpečnostného auditu aj nezávislú tretiu stranu.

2. Dodávateľ poskytne dokumentáciu o všetkých testoch kontroly vstupných údajov, ako napríklad opatrení na prevenciu vkladania kódu (napríklad: SQL injection (pozri obrázok 9.2), XSS, ...), pretečenia vyrovnávacej pamäte (buffer overflow), ...



Obr. 9.3: Reálny príklad zlého ošetrenia vstupu.

Nesprávne spracovanie vstupov môže byť nielen vstupnou bránou pre útočníkov, ale môže viesť k negatívnej používateľskej skúsenosti (pozri napríklad obrázok 9.3, zdroj https://twitter.com/gintveld/status/730317679886794752).

Údržba

1. Dodávateľ bezodkladne oznámi kontaktnej osobe obstarávateľa technické problémy týkajúce sa bezpečnosti obstaraného produktu. Následne pozri časť 9.3.2 „Aktualizácia softvéru a firmvéru“ na strane 241.

2. Dodávateľ musí aj pri vývoji aktualizácií zachovať úroveň bezpečnosti vývoja a riadenia kvality ako bola požadovaná pri obstaraní produktu, k čomu by mal byť pri podpise zmluvy zaviazaný (vrátane možných kontrol).

Referencie

[1, bod 3.1], [2, bod 5.1]

9.3.6 Firewall

Minimálne od roku 1666 sa pod slovom firewall rozumie stena vyrobená z nehorľavých materiálov, ktorej úlohou je v prípade vzniku požiaru zabrániť jeho ďalšiemu šíreniu. Takáto stena obvykle úplne oddeľuje dve časti budovy[33]. V IT oblasti dnes firewall (alebo brána firewall[34]) predstavuje samostatné zariadenie, ktoré úplne oddeľuje dve siete (network-based firewall), kontroluje všetku komunikáciu medzi nimi a blokuje prípadnú neoprávnenú komunikáciu z jednej siete do druhej. Nemusí však ísť nutne o samostatné hardvérové zariadenie, ale firewall môže byť napríklad softvérovo implementovaný na inom zariadení, ktoré spája viacero počítačových sietí (napríklad môže byť jednou z rozširujúcich funkcií smerovača). Softvérový firewall je často aj súčasťou operačného systému samotných koncových zariadení pripájajúcich sa do počítačovej siete (host-based firewall). Existuje niekoľko generácií firewallov, pričom každá využíva iný spôsob filtrovania sieťových prenosov:

1. **generácia** – paketový filter (pracuje na sieťovej vrstve OSI modelu). Používa iba základné informácie ako sú zdroj a cieľ paketu, použitý port alebo protokol. Na základe zoznamu pravidiel pre kontrolu prístupu potom vyhodnocuje pre každý paket samostatne, či ho má prepustiť alebo zahodiť.

2. **generácia** – stavový firewall (pracuje na transportnej vrstve OSI modelu). Takýto firewall má všetky vlastnosti paketového filtra, ale navyše si v internej tabuľke pamätá stavy všetkých aktívnych sieťových spojení. Vďaka tomu vie každý paket zaradiť do kategórie:

   - nadväzujúci nové spojenie,
   - súvisiaci s existujúcim spojením,
   - nepriraditeľný ku žiadnemu spojeniu.

   Vo filtrovacích pravidlách je potom možné využiť aj informáciu o kategórii paketu.

3. **generácia** – aplikačná brána (pracuje na aplikačnej vrstve OSI modelu). Hlavnou výhodou tejto generácie je, že „vidí“ do vnútra podporovaných protokolov (napríklad FTP, DNS,

[33] Zdroj: https://www.merriam-webster.com/words-at-play/word-origins-computer-terms/firewall.
[34] Zdroj: napríklad https://support.microsoft.com/sk-sk/help/4028544 a iné.

HTTP, ...) a tak sa môže filtrovanie okrem všetkých informácií z predošlých generácií riadiť aj obsahom samotnej komunikácie[35].

Nepoužívanie firewallov, používanie starých verzií firewallov alebo ich prehnane benevolentné nastavenie zľahčuje útočníkom využitie zraniteľností v systéme, čo môže potenciálne viesť až k neoprávnenému prístupu k systému. Firewally môžu vytvárať aj záznamy o sieťovej komunikácii (ako prichádzajúcej, tak aj odchádzajúcej), ktoré sú veľmi dôležité pre monitorovanie počítačovej siete a na prípadné forenzné účely (pre podrobnejšiu diskusiu pozri časť 9.3.4 „Vytváranie záznamov (audit logs)“ na strane 245).

Formulácie

1. Dodávaný produkt[36] musí obsahovať medzi jednotlivými sieťovými zónami dodávateľom nakonfigurované firewally.

2. Dodávateľ predloží zoznam pravidiel pre jednotlivé firewally alebo inú ekvivalentnú dokumentáciu. Základným nastavením musí byť odmietnutie všetkej komunikácie okrem dodávateľom výslovne uvedených výnimiek.

3. Dodávateľ poskytne podrobnú písomnú informáciu o všetkej prichádzajúcej aj odchádzajúcej komunikácii cez jednotlivé firewally. V dokumentácii identifikuje každé sieťové zariadenie, ktoré iniciuje komunikáciu a popíše použitý protokol.

Kontroly

1. Akceptačné testovanie musí prebiehať s nasadenými a plne nakonfigurovanými firewallmi podľa dodanej dokumentácie.

2. Počas akceptačného testovania je potrebné overiť aj činnosť firewallov a ich súlad so špecifikáciou, t.j. korektné blokovanie, ale aj prepúšťanie komunikácie, vrátane vytvárania požadovaných záznamov o komunikácii.

Údržba

1. Priebežná aktualizácia firewallov a ich pravidiel.

Referencie

[2, bod 3.1], NIST Special Publication 800-41 Rev. 1, “Guidelines on Firewalls and Firewall Policy (Draft).”

[35] Vďaka kontrole obsahu komunikácie môžu takéto firewally rozpoznať a zastaviť požadovaný typ komunikácie aj keď sa ich útočník snaží zmiasť použitím neštandardného portu (alebo iného štandardného portu).

[36] Produktom sa v tomto kontexte myslí napríklad celý informačný systém aj so sieťovou infraštruktúrov, ktorej súčasťou majú byť aj správne nasadené firewally.

9.3.7 Výkon

Pri špecifikácii predmetu obstarávania by sa okrem popisu funkcií nemalo zabúdať aj na špecifikovanie výkonových parametrov týchto funkcií. Stáva sa, že obstarávateľ sa sústredí najmä na popis toho, čo potrebuje dosiahnuť a ticho predpokladá, že riešenie bude nielen správne implementované ale aj dostatočne výkonné. Potom sa môže stať, že obstarávateľ po nejakom čase prevádzky zistí (v lepšom prípade už pri akceptačnom testovaní), že je systém pomalý. Napríklad, že niektoré úlohy je potrebné spustiť ešte pred odchodom z práce, aby mohli „bežať“ celú noc, pričom sa dúfa, že ráno, keď prídu zamestnanci do práce, tak už budú vykonané. Rovnako treba myslieť aj na to, že systém má dosahovať požadované parametre nielen na začiatku, keď je ešte možno prázdny a málo používaný, ale aj po jeho naplnení množstvom údajov, súčasnom využívaní väčším počtom používateľov, ako aj pri aktivovanom vytváraní protokolov, pri zapnutom antivírusovom programe, a tak podobne.

S narastajúcim výkonom hardvéru rastie (najviac priamo úmerne) aj výkon na ňom nasadeného softvéru. Preto, pokiaľ predmetom obstarávania nie je aj hardvér pre prevádzku systému, tak je nutné pri špecifikácii výkonu uviesť, na ako výkonnom hardvéri sa očakáva dosiahnutie požadovaného výkonu.

Testovanie výkonu systému by malo byť neoddeliteľnou súčasťou životného cyklu jeho vývoja. Minimálne, pred prevzatím predmetu obstarávania, by malo okrem testovania modulov a funkcií systému prebehnúť aj testovanie jeho výkonu. Pri špecifikácii výkonových požiadaviek je dôležité, aby boli špecifikované:

- **s výhľadom do budúcnosti (plan for future),**
  Aby systém spĺňal výkonové požiadavky aj povedzme po dvoch rokoch prevádzky. V prípade, že okruh používateľov nie je viac-menej pevne daný[37], tak treba odhadnúť ich nárast po úspešnom sprevádzkovaní systému. Aj pri stálom počte používateľov môže záťaž časom narastať vplyvom zväčšujúceho sa množstva uložených dát.

- ako aj **s prihliadnutím na záťažové špičky (plan for peak).**
  Predstavme si napríklad akademický informačný systém, ktorý poskytuje služby študentom a zamestnancom veľkej univerzity. Jeho vyťaženie je po väčšinu školského roka mierne a cez prázdniny minimálne. Ale v určitých obdobiach, napríklad počas zápisu študentov, sa záťaž môže aj niekoľkonásobne zvýšiť. Iným príkladom môže byť daňový informačný systém, kde je možné očakávať vysoké špičky v záťaži najmä okolo 31. marca. Pokiaľ sa v špecifikácii nepočítalo s takýmto špičkovým výkonom, tak to môže viesť až k zlyhaniu systému počas tejto, síce nie bežnej, ale očakávateľnej záťaže.[38]

Pokiaľ sa očakáva významný nárast počtu používateľov/dát alebo výrazné záťažové špičky, tak je dôležitým aspektom riešenia aj jeho škálovateľnosť. Nemusí byť ekonomicky výhodné systém hneď od začiatku prevádzkovať na hardvéri dimenzovanom na špičkové zaťaženie alebo na zaťaženie, ktoré príde až po niekoľkých rokoch prevádzky a náraste počtu používateľov a dát.

[37] Ak sa systém používa iba interne v organizácii, počet jej zamestnancov môže byť relatívne stabilný. Na druhej strane, ak je systém voľne prístupný cez Internet, tak môže počet jeho používateľov aj exponenciálne narastať a nemusí byť limitovaný iba používateľmi zo Slovenska.

[38] Pre pružné a cenovo efektívne prekonanie záťažových špičiek sa ukazuje ako vhodná kombinácia horizontálne škálovateľného systému so službou PaaS s podporou rýchleho nasadenia nových a deaktivovaním nepotrebných serverov podľa aktuálnych výkonových požiadaviek.

Zato má význam požadovať jeho jednoduchú škálovateľnosť trvalým alebo dočasným pridaním ďalšieho hardvéru. Pridanie ďalšieho hardvéru (horizontálne škálovanie) je lepšia alternatíva ako jeho výmena za rýchlejší (vertikálne škálovanie). Na jednej strane sa zachová investícia do pôvodného hardvéru, na druhej strane výkon dnešného hardvéru stúpa hlavne pridávaním väčšieho počtu jadier a procesorov (horizontálne škálovanie) než zvyšovaním výkonu jedného jadra (vertikálne škálovanie). Efektívne využitie viacprocesorovej (alebo distribuovanej) architektúry vyžaduje použitie paralelných algoritmov. Klasické sériové algoritmy nedokážu efektívne využiť horizontálne škálovanie a nie je možné ich jednoducho upraviť na paralelné.

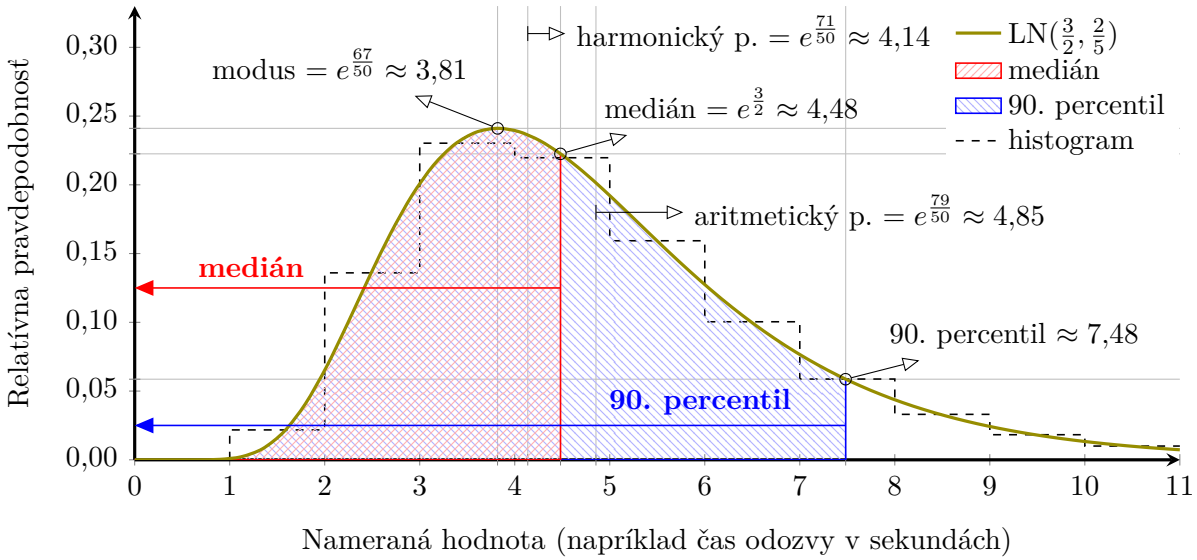
Keď pri špecifikovaní výkonu jednoúčelového programu hovoríme napríklad o rýchlosti, tak je väčšinou zrejmé, akú konkrétnu funkciu/činnosť programu máme na mysli. Napríklad, ak pri programe na komprimovanie súborov hovoríme o rýchlosti, tak je očividné, že máme na mysli koľko MB/s dokáže program skomprimovať. Pri zložitých systémoch však toto nemusí byť na prvý pohľad zrejmé a preto je potrebné identifikovať dôležité transakcie v systéme, ktoré predstavujú typické/časté (používateľmi opakovane vykonávané počas pracovného dňa) a pre oblasť pôsobnosti obstarávateľa kritické činnosti. Jednoduchým príkladom transakcie je prihlásenie používateľa do aplikácie, prechod na vyhľadávanie, vykonanie vyhľadávania, výber výsledku a následné odhlásenie. Vybrané transakcie sú potom základom väčšiny testov výkonnosti. Ich správna identifikácia je preto dôležitá pre výpovednú hodnotu týchto testov.

Pri špecifikovaní výkonových cieľov a zostavovaní transakcií treba myslieť aj na to, že pri akceptačnom testovaní je potrebné mať k dispozícii dostatočné množstvo kvalitných testovacích dát. Tieto dáta je možné pre testovacie účely vygenerovať, čo ale nie je triviálne, keďže treba myslieť na ich realistickosť (ako do rozsahu, tak aj do rozmanitosti). Pokiaľ existuje stará verzia systému je možné použiť časť dát z tohto systému. Treba ich však anonymizovať, aby sa ochránili prípadné osobné údaje alebo obchodné tajomstvá.

Výkon je možné merať v rôznych veličinách. Môže ísť napríklad o počet operácií, transakcií, či spracovaných udalostí za jednotku času (throughput – priepustnosť) alebo čas odozvy systému (response time), či prístupová doba (access time) v sekundách.

Vieme už teda aké veličiny chceme merať, na akých transakciách a na akých dátach. Ak pri akceptačnom testovaní komplexnejšieho systému opakovane spustíme výkonové testy, tak je veľmi pravdepodobné, že zakaždým nameriame iné hodnoty. Považujme teda výsledok merania za náhodnú premennú. (V nasledujúcom texte sa z dôvodu zjednodušenia výkladu úmyselne dopúšťame určitých nepresností a zamlčíme niektoré detaily. Pre podrobnosti pozri napríklad [5, 9].) Nech sa spravilo n zisťovaní jej hodnoty s výsledkami x_1, x_2, …, x_n (napríklad nech x_i je čas odozvy pri i-tom meraní v sekundách). Pri dostatočne veľkom n (povedzme 10 000 meraní) si môžeme zobraziť pravdepodobnosť, že nameraná hodnota je z intervalu $\langle 0, 1\rangle$, $\langle 1, 2\rangle$, $\langle 2, 3\rangle$, … pomocou histogramu, ktorý je na obrázku 9.4 znázornený prerušovanou čiarou. Čo je dostatočne veľké n závisí od rozdelenia pravdepodobnosti meranej náhodnej premennej a jej zisťovaných vlastností. V každom prípade, pri opakovanom meraní je potrebné brať do úvahy rôzne medzipamäte (cache), ktoré si môžu zapamätať výsledky posledných operácií. Pri opakovanom spustení rovnakej transakcie tak budú výsledky okamžite prístupné z medzipamäte a testovanie bude skreslené. Preto treba medzi testami medzipamäte vyprázdniť (napríklad databázovú medzipamäť).

Rozdelenie pravdepodobnosti znázornené na obrázku 9.4 neprerušovanou čiarou je tzv. lognormálne rozdelenie pravdepodobnosti spojitej náhodnej premennej, ktorá môže nadobúdať



Obr. 9.4: Log-normálne rozdelenie pravdepodobnosti – LN(μ, σ^2).

iba kladné hodnoty. Známejšie normálne rozdelenie je vhodnejšie pre náhodné premenné, ktoré môžu nadobúdať aj záporné hodnoty, čo ale nie je vhodné napríklad pri meraní času. Navyše normálne rozdelenie je symetrické okolo strednej hodnoty a preto nie je vhodné na demonštrovanie rozdielu medzi modusom, priemerom a mediánom, ktoré sú v tom prípade rovnaké. V špecifikácii výkonnosti je potrebné jasne určiť ako interpretovať výsledky testovania, t.j. kedy test považovať za úspešný a kedy nie. Možností je hneď niekoľko:

Maximum – v špecifikácii sa napríklad uvedie, aký najdlhší čas môže trvať odozva systému. Povedzme: „Maximálna doba odozvy pre transakciu vyhľadávania je päť sekúnd.“[39] Výhodou maxima je, že používateľ má garantované, že za žiadnych okolností nebude výkon horší. Na druhej strane, pokiaľ testovaný výkonový parameter nie je stabilný a má občasné extrémy, tak môže zriedkavo nastať prekročenie stanoveného maxima, aj keď to z používateľského hľadiska nemusí byť problém. Napríklad pravdepodobnosť, že nameraná hodnota bude väčšia ako 11 je na obrázku 9.4 iba 1,24 %. Ako maximum však nie je možné zvoliť ani hodnotu 20, pretože pri 10 000 meraniach môže byť zhruba jedno meranie ešte väčšie.

***N*-tý percentil** – Vo všeobecnosti N-tý percentil (čo je to isté ako $^N/_{100}$-kvantil) predstavuje hodnotu, od ktorej by malo byť N % meraní menších. Na príklade z obrázku 9.4 je hodnota 90. percentilu zhruba 7,48. To znamená, že z 10 000 meraní bude 9 000 menších než 7,48. Pri tom istom rozdelení je 99. percentil približne 11,37 a 99,9. percentil je 15,43. Výhodou percentilu je, že nie je natoľko ovplyvnený málo častými extrémami ako maximum. V špecifikácii sa uvedie napríklad: „99. percentil doby odozvy pre transakciu vyhľadávania môže byť maximálne 12 sekúnd.“

[39] Podľa [10] je desatina sekundy hranica, pri ktorej má používateľ ešte pocit okamžitej odozvy. Jedna sekunda je zas hranica pre neprerušenie používateľových myšlienok. Desať sekúnd je limit pre udržanie pozornosti. Pri dlhšej odozve začne používateľ počas čakania na odpoveď riešiť iné úlohy.

Medián je vlastne 50. percentil. Predstavuje hodnotu, ktorá bude po utriedení nameraných hodnôt v strede zoznamu (polovica bude menších a polovica väčších). Na príklade z obrázku 9.4 je hodnota mediánu zhruba 4,48. V špecifikácii sa uvedie napríklad: „Medián doby odozvy pre transakciu vyhľadávania môže byť maximálne 4,48 sekundy."

Modus predstavuje najpravdepodobnejšiu, teda najčastejšie nameranú hodnotu. Na histograme z obrázku 9.4 vidíme, že najpravdepodobnejšie sú hodnoty z intervalu $\langle 3, 4\rangle$. Takýchto hodnôt bude pri 10 000 meraniach približne 2 300.

Priemer – Existuje viacero druhov priemerov. Najčastejšie používaný je aritmetický priemer. V špecifikácii sa môže uviesť napríklad: „Aritmetický priemer doby odozvy pre transakciu vyhľadávania môže byť maximálne 4,85 sekundy."

Ďalšími dvomi najznámejšími priemermi sú harmonický a geometrický priemer. Popíšeme si ich vhodnosť na sumarizáciu jednotlivých výkonových meraní.

Aritmetický – Je vhodný v prípadoch, keď súčet nameraných hodnôt má nejakú zmysluplnú interpretáciu. Napríklad súčet časov jednotlivých odoziev má prirodzenú interpretáciu ako celkový čas odozvy. Takže aritmetický priemer je vhodný na sumarizáciu nameraných časov. Vzorec pre výpočet aritmetického priemeru $A(x_1, x_2, \ldots, x_n)$ z n nameraných hodnôt x_i je asi každému známy:

$$A(x_1, x_2, \ldots, x_n) = \frac{x_1 + x_2 + \cdots + x_n}{n}$$

Na príklade z obrázku 9.4 je hodnota aritmetického priemeru zhruba 4,85.

Aritmetický priemer však nie je vhodný pre sumarizáciu rýchlostí (napríklad priepustností) [5, časť 3.3]. Predstavme si, že sme spustili 10 000 transakcií a ich vykonanie trvalo 10 sekúnd. Na základe tohto prvého testu vieme, že priepustnosť systému bola 1 000 tr./s. Pri opakovanom teste vykonanie tých istých 10 000 transakcií trvalo 20 sekúnd. Na základe druhého testu sme teda zistili, že priepustnosť systému bola iba 500 tr./s. Ak by sme z týchto dvoch testov chceli vypočítať priemernú priepustnosť, môžeme sa na ne pozrieť ako na jeden test s 20 000 transakciami, ktorý trval 30 sekúnd. Priemerná priepustnosť je teda $20\,000/30 \approx 666{,}66$ [tr./s.]. Aritmetický priemer 1 000 a 500 je však 750. V tomto prípade potrebujeme použiť iný priemer.

Harmonický – Je vhodný pre sumarizáciu rýchlostí, ale zas nie je vhodný pre sumarizáciu meraní, na ktoré je vhodný aritmetický priemer. Vzorec pre výpočet harmonického priemeru $H(x_1, x_2, \ldots, x_n)$ z n nameraných hodnôt x_i je:

$$H(x_1, x_2, \ldots, x_n) = \frac{n}{\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_n}}$$

Na príklade z obrázku 9.4 je hodnota harmonického priemeru zhruba 4,14. Ak sa vrátime k predošlého prípadu dvoch priepustností o hodnote 1 000 tr./s a 500 tr./s tak dostávame:

$$H(1\,000, 500) = \frac{2}{\frac{1}{1\,000} + \frac{1}{500}} = \frac{2}{0{,}001 + 0{,}002} = \frac{2}{0{,}003} \approx 666{,}66$$

čo je presne hodnota, ktorú sme očakávali. (Harmonický priemer dvoch rýchlostí v_1 a v_2 je priemerná rýchlosť, ktorú dostaneme, keď rýchlosťou v_1 prejdeme nejakú

vzdialenosť a následne rovnakú vzdialenosť prejdeme rýchlosťou v_2. Aritmetický priemer dvoch rýchlostí v_1 a v_2 je priemerná rýchlosť ktorú dostaneme keď rýchlosťou v_1 pôjdeme nejaký čas a potom rovnaký čas pôjdeme rýchlosťou v_2.)

Geometrický priemer $G(x_1, x_2, \ldots, x_n)$ z hodnôt x_i je definovaný vzorcom:

$$G(x_1, x_2, \ldots, x_n) = \sqrt[n]{x_1 x_2 \cdots x_n}$$

Na príklade z obrázku 9.4 je hodnota geometrického priemeru zhruba 4,48. (Pre log-normálne rozdelenie je totiž geometrický priemer zhodný s mediánom.)

Podľa [5, časť 3.5] nie je geometrický priemer vhodný pre sumarizáciu časov, ani rýchlostí a uvádzame ho len pre úplnosť. (Je vhodný napríklad pri sumarizácii ročných percentuálnych výnosov.) Pri porovnávaní jednotlivých priemerov sa zíde aj nasledovný, všeobecne platný vzťah medzi nimi:

$$\min(x_1, \ldots x_n) \leq H(x_1, \ldots x_n) \leq G(x_1, \ldots x_n) \leq A(x_1, \ldots x_n) \leq \max(x_1, \ldots x_n)$$

Spomenuté štatistické parametre je možné navzájom kombinovať, prípadne k nim pridať niektoré, ktoré sme nespomínali (napríklad štandardnú odchýlku, určenie intervalov spoľahlivosti, ...). V špecifikácii sa potom môže požadovať: „Doba odozvy pre transakciu vyhľadávania môže byť v priemernom prípade (myslí sa aritmetický priemer) maximálne 4,85 s a jej 99. percentil môže byť maximálne 12 s.“

Dva najčastejšie testy výkonnosti sú:

Záťažový (load) test je test výkonu, pri ktorom je aplikácia zaťažená až po plánovaný počet používateľov a ich súčasných prístupov. Cieľom je splniť výkonnostné ciele týkajúce sa dostupnosti, priepustnosti a doby odozvy. Záťažový test by mal čo najvernejšie odrážať skutočné používanie systému a preto zahŕňa simuláciu interakcie používateľov so systémom. Patria sem napríklad aj oneskorenia a pauzy, ktoré sa vyskytujú počas zadávania údajov používateľmi, ako aj ich odpovede na informácie vrátené systémom. [9]

Stres test má úplne iný cieľ ako záťažový test. Cieľom stres testu je spôsobiť zlyhanie systému alebo jeho časti za účelom zistenia horných limitov jeho výkonu a kapacity. Stres test teda pokračuje, kým sa niečo nepokazí, napríklad kým sa už nemôže prihlásiť ďalší používateľ, čas odozvy prekročí definovanú prijateľnú hodnotu, alebo sa aplikácia stane nedostupnou. Pokiaľ zistené horné limity výkonu systému sú veľmi blízko plánovaným (očakávaným v bežnej prevádzke), tak to poukazuje na skutočnosť, že je k dispozícii len veľmi malá rezerva. Je dôležité poznať horné limity, najmä ak je ťažké predpovedať budúci rast používanosti systému. [9]

Formulácie

Ministerstvo financií SR, Sekcia informatizácie spoločnosti v spolupráci s Úradom pre verejné obstarávanie vydali už v januári roku 2013 metodický pokyn pre verejné obstarávanie IKT, kde v prílohe 2: „Definovanie predmetu zákazky – špecifikácia požiadaviek na softvér“ [8] odporúčajú v bode 3.4 špecifikovať nasledovné výkonové charakteristiky:

1. Reakčná doba na transakciu (priemer, maximum).

2. Priepustnosť (throughput) [počet transakcií za sekundu].
3. Kapacita meraná napríklad počtom zákazníkov alebo transakcií, ktoré dokáže systém obslúžiť / zabezpečiť.
4. Obmedzené režimy (degradation modes), t.j. úroveň prijateľnosti operácií v prípade, že bol výkon systému nejakým spôsobom znížený.
5. Používané zdroje (pamäť, disk, výkon procesora, komunikácia a podobne).

Tieto informácie je možné doplniť konkrétnymi formuláciami spomenutými v popise jednotlivými parametrov uvedených vyššie.

Kontroly

1. Pri akceptačnom testovaní treba na dostatočne reprezentatívnych dátach vykonať špecifikované testy výkonnosti a potvrdiť, že aplikácia dosahuje požadovanú výkonnosť.
2. Pokiaľ nie je použitý testovací nástroj, ktorý požadované parametre sám vypočíta, tak sa nesmie zabudnúť na dostatočný počet opakovaní, aby bolo možné vypočítať požadované parametre (napríklad 99. percentil) s dostatočnou spoľahlivosťou.
3. Pri opakovaní testov sa nesmie zabudnúť na priebežné vyprázdňovanie medzipamätí (databázy, súborového systému, ...) aby sa zachovala realistickosť testovania.

Údržba

1. Po inštalácii aktualizácií, či bezpečnostných záplat, je potrebné opätovne overiť výkon, aby sa potvrdilo že nedošlo k regresii (t.j. k zníženiu výkonu).
2. Priebežne treba monitorovať výkon systému a v prípade potreby včas začať plánovať jeho navýšenie.

Referencie

[7], [8, bod 3.4], [9], [5]

Literatúra

[1] N. Bartol, D. Dunn, C. Glantz, E. Goff, K. Jereza, A. Lee, R. Massello, D. Norton, L. R. O'Neil, T. Overman a M. Seader. *Cybersecurity Procurement Language for Energy Delivery Systems*. Energy Sector Control Systems Working Group (ESCSWG), apr. 2014. URL: https://energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014 (citované na stranách: 241, 242, 247, 250).

[2] *Cyber Security Procurement Language for Control Systems*. United States Department of Homeland Security, sept. 2009. URL: https://www.hsdl.org/?view&did=7968 (citované na stranách: 233, 241, 242, 247, 250, 251).

[3] A. Drougkas, D. Liveri, A. Zisi a P. Kyranoudi. *Procurement Guidelines for Cybersecurity in Hospitals*. European Union Agency for Network and Information Security (ENISA), feb. 2020. ISBN: 978-92-9204-312-4. DOI: 10.2824/943961. URL: https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services (citované na stranách: 233, 234, 245, 247).

[4] C. Karsberg a M. Dekker. *Security Guide for ICT Procurement*. European Union Agency for Network and Information Security (ENISA), dec. 2014. ISBN: 978-92-9204-117-5. DOI: 10.2824/994989. URL: https://www.enisa.europa.eu/publications/security-guide-for-ict-procurement (citované na strane 233).

[5] D. J. Lilja. *Measuring Computer Performance: A Practitioner's Guide*. Cambridge University Press, 2000. ISBN: 978-0-511-61239-8. DOI: 10.1017/CBO9780511612398 (citované na stranách: 253, 255–257).

[6] *MDCG 2019-16 – Guidance on Cybersecurity for medical devices*. Medical Device Coordination Group (MDCG), dec. 2019. URL: https://ec.europa.eu/docsroom/documents/41863 (citované na strane 239).

[7] *Metodický pokyn pre štandardné náležitosti opisu predmetu zákazky, štandardné podmienky účasti vo verejnom obstarávaní a optimálne zmluvné podmienky v súvislosti s projektmi v oblasti informačnokomunikačných technológií (verzia 1.51)*. Ministerstvo financií SR, Sekcia informatizácie spoločnosti v spolupráci s Úradom pre verejné obstarávanie, jan. 2013. URL: http://www.informatizacia.sk/ext_dok-metodicky_pokyn_std_obstaravanie_1-51/15664c (citované na stranách: 233, 257).

[8] *Metodický pokyn pre verejné obstarávanie IKT, Príloha 2: Definovanie predmetu zákazky – špecifikácia požiadaviek na softvér*. Ministerstvo financií SR, Sekcia informatizácie spoločnosti v spolupráci s Úradom pre verejné obstarávanie, jan. 2013. URL: http://www.informatizacia.sk/ext_dok-metodicky_pokyn_std_obstaravanie_priloha2/15178c (citované na stranách: 233, 245, 256, 257).

[9] I. Molyneaux. *The Art of Application Performance Testing*. 1. vyd. Sebastopol, CA 95472: O'Reilly Media, Inc., jan. 2009. ISBN: 978-0-596-52066-3 (citované na stranách: 253, 256, 257).

[10] J. Nielsen. *Usability Engineering*. 1. vyd. Morgan Kaufmann, jan. 1993. ISBN: 978-0125184069 (citované na strane 254).

Kapitola 10

Kryptológia

Martin Stanek

Cieľom tejto kapitoly je poskytnúť pragmatický pohľad na kryptológiu, s dôrazom na používané kryptografické konštrukcie a ich súvis s bezpečnostnými požiadavkami. Napriek tomu, že detaily a vlastnosti kryptografických konštrukcií majú primárne matematickú povahu, obmedzíme túto stránku výkladu na minimum, aj za cenu niektorých zjednodušení. Záujemcom o hlbší pohľad na problematiku možno odporučiť špecializovanú odbornú literatúru.

Kryptológia ako vedná oblasť zahŕňa kryptografiu a kryptoanalýzu. Kryptografia sa venuje návrhu bezpečnostných konštrukcií (vo forme algoritmov, protokolov a schém) s cieľom zabezpečiť ochranu bezpečnostných atribútov dát. Kryptoanalýza skúma možnosti útokov na kryptografické konštrukcie.

10.1 Základné pojmy, kryptografické konštrukcie a ich ciele

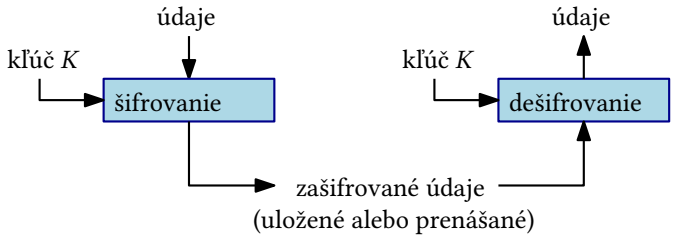
V tejto časti popisujeme základné kryptografické konštrukcie zabezpečujúce dôvernosť, integritu a autentickosť (prípadne aj nepopierateľnosť autorstva) údajov. Zo základných bezpečnostných atribútov vynecháme dostupnosť, ktorú kryptografia samotná zabezpečiť nedokáže. Dostupnosť je otázkou vhodne zvolenej redundancie dát, komponentov a komunikačných pripojení, v súčinnosti s ďalšími technickými riešeniami a prevádzkovými postupmi.

10.1.1 Šifrovanie

Šifrovanie slúži na zabezpečenie dôvernosti údajov. Detaily konkrétneho riešenia, akým spôsobom je šifrovanie použité, sa obvykle líšia podľa toho, či sú šifrované údaje uložené na nosiči dát (napr. disky, pásky) alebo sú prenášané počítačovými sieťami. Šifrovanie transformuje údaje pomocou šifrovacieho algoritmu a šifrovacieho kľúča do ich šifrovanej/zašifrovanej podoby. Opačný postup, teda získanie pôvodných dát z ich zašifrovanej podoby sa nazýva dešifrovanie a využíva sa pri ňom dešifrovací algoritmus a dešifrovací kľúč.

Symetrické šifrovanie

V prípade, že šifrovací a dešifrovací kľúč sú rovnaké, hovoríme o symetrických šifrách (pozri obr. 10.1).



Obr. 10.1: Symetrické šifrovanie

Z hľadiska bezpečnosti pri symetrickom šifrovaní očakávame, že útočník bez kľúča nie je schopný zo zašifrovaných údajov získať ich pôvodnú podobu napriek tomu, že pozná šifrovací algoritmus. V súčasnosti používaných šifrách je kľúč vyberaný ako náhodná postupnosť bitov pevnej dĺžky.

Najznámejším a najpoužívanejším symetrickým šifrovacím algoritmom je v súčasnosti AES (Advanced Encryption Standard). AES má tri varianty, líšiace sa okrem iného aj dĺžkou použitého kľúča: AES-128, AES-192, AES-256. Názov AES-n označuje variant s dĺžkou kľúča n bitov.

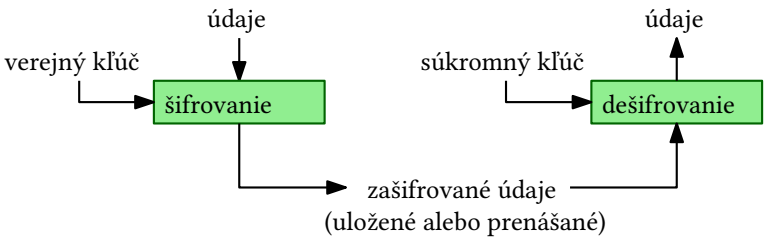
Dĺžka kľúča je dôležitým parametrom pre bezpečnosť šifrovacieho algoritmu – ovplyvňuje počet potenciálnych kľúčov, ktoré musí útočník vyskúšať v prípade, že sa rozhodne prezrieť priestor všetkých kľúčov. Takýto útok úplným preberaním je možné realizovať vždy, bez ohľadu na šifrovací algoritmus. Preto má počet potenciálnych kľúčov znemožňovať efektívne vyskúšanie všetkých kľúčov. V súčasnosti možno považovať kľúče s dĺžkou 128 bitov (teda 2^{128} potenciálnych kľúčov) za dostatočne bezpečné, pokiaľ nie sú slabiny v samotnom šifrovacom algoritme alebo v spôsobe generovania, distribúcie a ochrany použitých kľúčov.

Z hľadiska efektívnosti sú symetrické šifrovacie algoritmy dostatočne rýchle na transparentné šifrovanie a dešifrovanie diskov osobných počítačov, komunikácie v počítačových sieťach a podobne, pričom spomalenie spôsobené takýmto dodatočným spracovaním údajov je zanedbateľné. Viaceré hardvérové zariadenia sú v súčasnosti konštruované so zabudovanou podporou pre kryptografické operácie, napríklad novšie procesory obsahujú podporu špeciálnych inštrukcií pre implementáciu AES.

Asymetrické šifrovanie

Samostatná trieda šifrovacích algoritmov využíva na šifrovanie iný kľúč ako na dešifrovanie, pozri obr. 10.2, pričom dešifrovací kľúč nie je možné efektívne vypočítať zo šifrovacieho kľúča. V tomto prípade hovoríme o asymetrickom šifrovaní, prípadne o šifrovaní s verejným kľúčom. Ako názov napovedá, šifrovací kľúč, bežne označovaný ako verejný kľúč, je zvyčajne zverejnený a teda ktokoľvek môže šifrovať. Dešifrovať je možné len so znalosťou dešifrovacieho kľúča, ten je obvykle označovaný ako súkromný kľúč. Najznámejším príkladom asymetrického šifrovania je RSA schéma.

Asymetrické šifry sú konštruované s využitím vhodných matematických problémov, napr. rozklad (faktorizácia) veľkých čísel na súčin prvočiniteľov. Svoju bezpečnosť opierajú o zložitosť riešenia týchto problémov. Kľúče v asymetrických šifrách preto reprezentujú konkrétne matematické objekty (a nie sú to náhodne volené postupnosti bitov). Pri rovnakej miere kryp-



Obr. 10.2: Asymetrické šifrovanie

tografickej odolnosti šifry je dĺžka kľúčov asymetrických šifier zvyčajne podstatne dlhšia ako dĺžka kľúčov symetrickej šifry. Napríklad dĺžka RSA kľúčov 3072 bitov poskytuje rovnakú mieru kryptografickej odolnosti ako AES-128 [7].

Z hľadiska bezpečnosti asymetrického šifrovania očakávame, že útočník nie je schopný bez znalosti súkromného kľúča zo zašifrovaných údajov získať ich pôvodnú podobu (alebo nejakú netriviálnu informáciu o pôvodných údajoch). Pripomeňme, že šifrovací kľúč je verejne známy, a teda útočník má možnosť zašifrovať ľubovoľné údaje.

Hybridné šifrovanie

Asymetrické šifrovanie a dešifrovanie sú z hľadiska výpočtových nárokov oveľa náročnejšie ako ich symetrické náprotivky. Sú vhodné najmä na šifrovanie krátkych údajov, tými sú v praxi najčastejšie symetrické kľúče v tzv. hybridných šifrovacích schémach. Hybridná šifrovacia schéma kombinuje symetrický a asymetrický šifrovací algoritmus nasledujúcim spôsobom (pozri obr. 10.3):

Šifrovanie – odosielateľ

Vstup: dáta M, verejný kľúč príjemcu
Posielané údaje (výstup): EK, EM

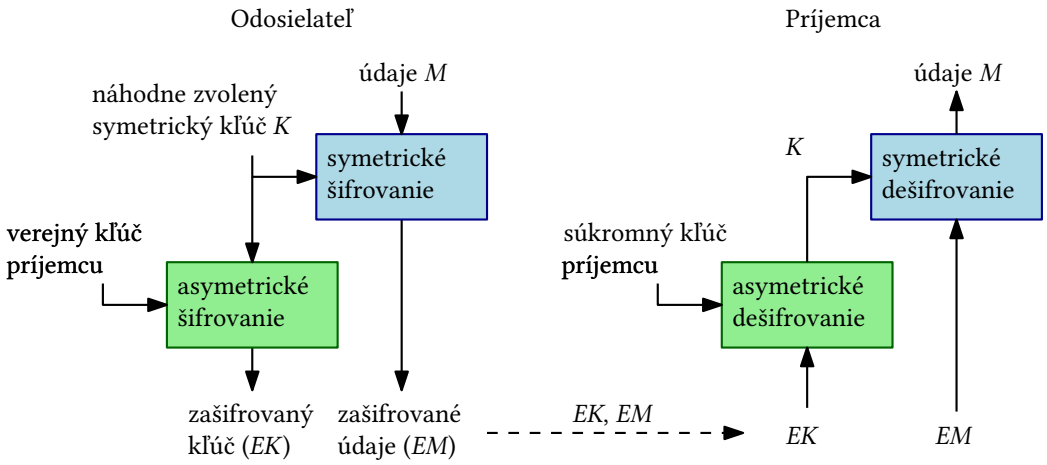
1. odosielateľ vygeneruje náhodný symetrický kľúč K
2. zašifruje údaje M symetrickou šifrou s použitím kľúča K (výsledok označme EM)
3. zašifruje kľúč K asymetrickým šifrovaním s použitím verejného kľúča príjemcu (výsledok označme EK)

Dešifrovanie – príjemca

Vstup: EK, EM, vlastný súkromný kľúč
Výstup: M

1. príjemca získa K dešifrovaním EK, pričom použije svoj súkromný kľúč
2. získa pôvodné dáta dešifrovaním EM, pričom použije kľúč K

Popis predpokladá posielanie údajov odosielateľom k príjemcovi, avšak hybridný prístup môže byť použitý aj v prípade, že šifrovanie a dešifrovanie vykonáva rovnaká osoba (vlastník súkromného kľúča) a dáta sú ukladané lokálne, napr. na disk.



Obr. 10.3: Hybridné šifrovanie

Výhodou hybridného prístupu je efektívne šifrovanie, keď rozsahom veľké údaje sú šifrované rýchlym symetrickým algoritmom, pričom bezpečnú distribúciu symetrického kľúča rieši asymetrické šifrovanie. Pred použitím takejto schémy stačí dôveryhodným spôsobom distribuovať verejného kľúča príjemcu. Obvykle tento problém rieši infraštruktúra verejných kľúčov (pozri časť 10.3.3). Verejný kľúč je nemenný dlhší čas, napr. jeden rok, a môže byť používaný opakovane.

Porovnanie a použitie

Typické rozdiely medzi symetrickým a asymetrickým šifrovaním sumarizuje nasledujúca tabuľka:

	Symetrické šifrovanie	Asymetrické šifrovanie
Primárne použitie	dôvernosť údajov ľubovoľnej veľkosti	dôvernosť krátkych dát (typicky napr. kľúče pre symetrické šifrovanie)
Komunikácia	1:1 – obvykle dvaja účastníci (jeden odosielateľ, jeden príjemca)	N:1 – ľubovoľný počet odosielateľov (šifrovací kľúč je verejný), jeden príjemca (súkromný dešifrovací kľúč)
Efektívnosť	rýchle šifrovanie aj dešifrovanie	pomalé šifrovanie aj dešifrovanie
Dĺžka kľúčov	obvykle 128 až 256 bitov (náhodný reťazec bitov)	v závislosti na konkrétnom algoritme, niekoľko sto až niekoľko tisíc bitov
Distribúcia kľúčov	obvykle potrebné použiť kryptografické protokoly na distribúciu (dohodnutie) kľúča	relatívne jednoduchá distribúcia verejného kľúča (avšak potrebné overiť jeho autentickosť)

Šifrovací algoritmus, či už symetrický alebo asymetrický, neposkytuje ochranu integrity ani autentickosti prenášaných údajov. Teda skutočnosť, že údaje boli prenášané/uložené zašif-

rované a úspešne sme ich dešifrovali neznamená, že počas prenosu/uloženia zašifrované dáta neboli útočníkom zmenené. Výnimkou sú špecifické konštrukcie módov symetrických šifier, tzv. autentizované šifrovanie. V súčasnosti sú v praxi používané čoraz častejšie a príkladmi takýchto módov sú GCM (Galois/Counter Mode) a CCM (Counter with CBC-MAC). Použitie AES v týchto módoch býva potom označené ako AES-GCM, resp. AES-CCM. Pokiaľ nevyužívame autentizované šifrovanie, je potrebné na zabezpečenie integrity a autentickosti údajov použiť iné kryptografické konštrukcie, najčastejšie autentizačné kódy správ (pozri časť 10.1.2).

Šifrovanie možno nájsť v praxi vo veľkom počte rôznorodých aplikácií, pričom pre symetrické šifrovanie sa štandardne využíva AES (v módoch vhodných pre daný účel). Uveďme niekoľko príkladov:

- Šifrovanie diskov osobných počítačov, kde sa údaje transparentne pri čítaní z disku dešifrujú a pri zápise na disk šifrujú – BitLocker (štandardný nástroj v operačnom systéme Windows), VeraCrypt (multiplatformová aplikácia), FileVault 2 (štandardný nástroj v macOS). Cieľom takýchto riešení je znížiť riziko prezradenia údajov, napr. pri odcudzení prenosného počítača.
- Šifrovanie komprimovaných archívov (napr. zip) – viaceré aplikácie pre prácu s komprimovanými archívmi údajov umožňujú okrem komprimácie vzniknuté archívy aj zašifrovať s použitím symetrického šifrovania (napr. 7-Zip, WinZip používajú AES). Šifrovací kľúč je vypočítaný zo zadaného hesla. Zašifrovaný archív je následne možné dešifrovať a rozbaliť len s použitím tohto hesla. V prípade ad-hoc potreby poslať citlivé údaje, pričom nemáme k dispozícii verejný kľúč príjemcu (alebo tento ani žiadny verejný kľúč nemá), je často najjednoduchším riešením údaje zabaliť do šifrovaného archívu s použitím dostatočne silného hesla. Následne archív pošleme príjemcovi mailom a heslo oznámime iným komunikačným kanálom (povedzme SMS). Samozrejme, pokiaľ útočník získa zašifrovaný archív aj prenášané heslo, dokáže dešifrovať rovnako ako príjemca.
- Šifrovanie komunikácie v nezabezpečených sieťach, napr. na internete. V súčasnosti je prezeranie väčšiny web stránok zabezpečené protokolom TLS (Transport Layer Security). Jeho použitie je signalizované v adrese stránky prostredníctvom „https://“ namiesto „http://“, ako aj vizuálnym indikátorom, najčastejšie v podobe zámku. TLS okrem iných atribútov zabezpečuje aj dôvernosť prenášaných údajov symetrickým šifrovaním, pričom konkrétny použitý algoritmus sa dohodne pri nadviazaní spojenia medzi internetovým prehliadačom a webovým serverom.

10.1.2 Hašovacie funkcie a autentizačné kódy správ

Hašovacie funkcie

Kryptografické hašovacie funkcie sú algoritmy, ktoré z prakticky ľubovoľne dlhého vstupu vypočítajú hodnotu – reťazec bitov pevnej dĺžky (ten nazveme odtlačok). Ide o deterministické algoritmy, teda pre rovnaký vstup je vypočítaný vždy rovnaký odtlačok. Úlohou odtlačku je jednoznačne reprezentovať vstupné údaje/dokument. Pre bežne používané hašovacie funkcie má odtlačok dĺžku 256 bitov v prípade SHA-256 alebo 512 bitov v prípade SHA-512. V niektorých konštrukciách a starších protokoloch sa možno stretnúť aj s hašovacími funkciami SHA-1 resp. MD5 (s odtlačkami dĺžky 160 resp. 128 bitov). Z hľadiska rýchlosti spracovania vstupu sú hašovacie funkcie porovnateľné so symetrickými šifrovacími algoritmami.

Primárne použitie hašovacích funkcií je v ďalších kryptografických konštrukciách, napríklad v autentizačných kódoch správ, schémach digitálnych podpisov a pod. Hašovacie funkcie nevyužívajú žiadny kľúč a teda ktokoľvek vie vypočítať odtlačok k ľubovoľnému vstupu. Preto má samostatné použitie hašovacích funkcií význam len pre detekciu narušenia integrity údajov pri náhodnej (necielenej) zmene, alebo v situáciách, keď útočník nemá úplnú kontrolu nad všetkými komunikačnými kanálmi a nemôže okrem údajov modifikovať aj ich odtlačok. V opačnom prípade útočník ľahko dopočíta korektný odtlačok k pozmeneným údajom. Uveďme dva ilustračné príklady použitia hašovacích funkcií na kontrolu integrity:

- Distribúcia objemných súborov (softvér, video a pod.) na internete, kde je na webovej stránke zverejnený odtlačok takéhoto súboru. Po stiahnutí súboru môže používateľ lokálne vypočítať jeho odtlačok a porovnať hodnotu s odtlačkom zverejneným na internete. Nesúlad vypočítaného a zverejneného odtlačku signalizuje, že pri prenose údajov došlo k modifikácii, napríklad spôsobenej nespoľahlivým prenosom alebo zámernou úpravou. Samozrejme, pokiaľ útočník dokáže zmeniť pri prenose nielen údaje samotné, ale aj informáciu o odtlačku z webovej stránky, používateľ nič podozrivé nespozoruje. Zdôraznime, že hašovacie funkcie vo všeobecnosti nezabezpečujú autentickosť údajov.
- Ochrana integrity súborov vypočítaním ich odtlačkov. Pokiaľ odtlačky odložíme (napr. na neprepisovateľné médium), dokážeme neskôr opätovným výpočtom odtlačkov a ich porovnaním s odloženými hodnotami zistiť, či a ktorý zo súborov bol modifikovaný. Keďže odtlačky sú obvykle podstatne kratšie ako zdrojové súbory, tento spôsob ochrany poskytuje len detekciu narušenia integrity a neumožňuje rekonštruovať pôvodný obsah súborov (na tento účel slúži zálohovanie). Na druhej strane je porovnávanie odtlačkov prevádzkovo jednoduchšie ako porovnávanie celých kópií súborov.

Pri prezentácii odtlačkov v čitateľnej forme je obvykle použitý zápis v šestnástkovej (hexadecimálnej) sústave využívajúcej cifry `0`, `1`, ..., `9`, `A`, `B`, `C`, `D`, `E`, `F`. Príklady odtlačkov niekoľkých reťazcov pomocou SHA-256:

vstupný reťazec	SHA-256
Kryptologia	`928926C86A99D03F47FECA0A85F52298D9D7F2AEEB31CAFEC7B76198DB9A8E61`
kryptologia	`4978DBF2A4D3B02ABA050EFAB96B86CB844C18E9DDF4044B047BF32DF9914B99`

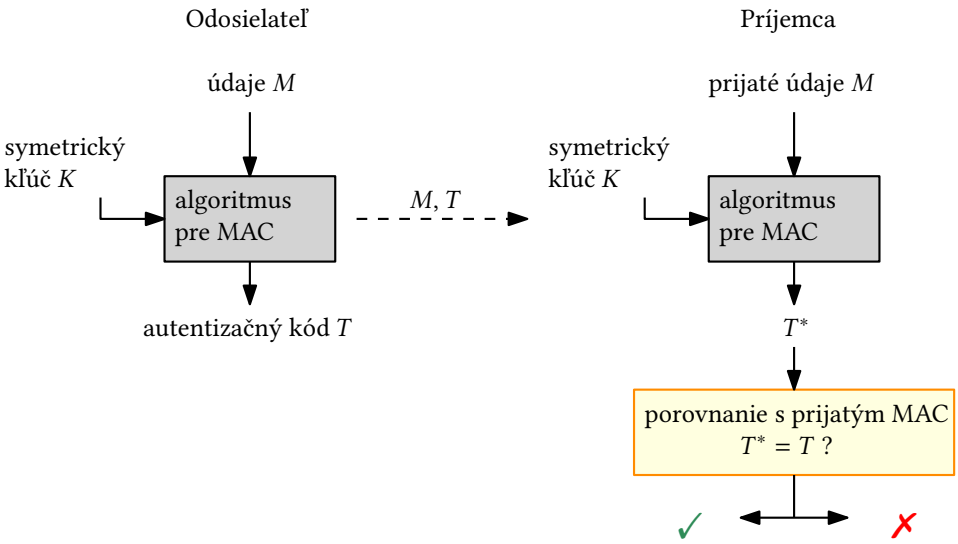
Použitie hašovacích funkcií v kryptografických konštrukciách vyžaduje, aby hašovacie funkcie mali vhodné bezpečnostné vlastnosti. Dve základné vlastnosti sú odolnosť vzoru a odolnosť voči kolíziám:

- Odolnosť vzoru: k danému odtlačku nie je efektívne možné vypočítať vstup s takýmto odtlačkom.
- Odolnosť voči kolíziám: nie je efektívne možné vypočítať dva rôzne vstupy s rovnakým odtlačkom.

Autentizačné kódy správ

Autentizačný kód správy (angl. Message Authentication Code, skrátene MAC) je v podstate odtlačok správy, pri výpočte ktorého bol použitý kľúč. Algoritmy pre výpočet autentizačných kódov správ sú akoby hašovacie funkcie s kľúčom, pričom sú často konštruované práve z hašovacích funkcií. Najznámejšou konštrukciou je HMAC – ide o všeobecnú konštrukciu, kde konkrétny algoritmus dostaneme voľbou „podkladovej“ hašovacej funkcie (napr. HMAC-SHA1 je HMAC skonštruovaný z hašovacej funkcie SHA-1).

Keďže výpočet odtlačku závisí na kľúči, autentizačné kódy správ zabezpečujú autentickosť údajov. Samozrejme, iba v prípade ak je kľúč známy len oprávneným používateľom. Najčastejšie použitie autentizačných kódov je pri ochrane komunikácie v počítačovej sieti (pozri obr. 10.4). V takom prípade kľúč poznajú spoločne odosielateľ a príjemca. Pri posielaní údajov k nim odosielateľ pripojí autentizačný kód. Príjemca vypočíta z prijatých údajov a kľúča autentizačný kód a porovná ho s prijatým autentizačným kódom. V prípade zhody je potvrdená autentickosť údajov. Pokiaľ útočník nepozná kľúč použitý pri výpočte odtlačku, nedokáže údaje nepozorovane modifikovať, lebo nevie dopočítať správny autentizačný kód.



Obr. 10.4: Použitie autentizačných kódov správ

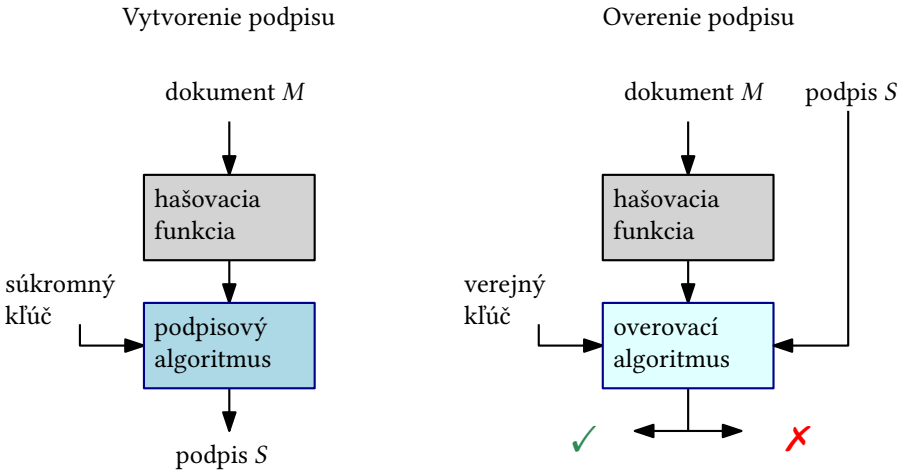
Dohodnutie/distribúcia konkrétneho kľúča na takýto účel je zvyčajne úlohou vhodného kryptografického protokolu pri nadväzovaní spojenia (napríklad niektoré varianty TLS protokolu alebo IKE protokol v rámci IPsec). Následne je výpočtom autentizačného kódu zabezpečený každý prenášaný paket – algoritmy pre MAC sú dostatočne rýchle (porovnateľne so symetrickým šifrovaním).

Autentizačné kódy nezabezpečujú nepopierateľnosť autorstva prenášaných správ. Keďže príjemca má k dispozícii rovnaký kľúč ako odosielateľ, autentizačný kód ľubovoľnej správy vie vypočítať sám. To znamená, že odosielateľ dokáže poprieť autorstvo správy.

10.1.3 Digitálne podpisy

Schémy pre digitálne podpisy sú asymetrické kryptografické konštrukcie, pozostávajúce z podpisového algoritmu a z overovacieho algoritmu. Používateľ vytvorí inštanciu schémy vygenerovaním dvojice kľúčov – súkromného a verejného. Podpisový algoritmus vytvára digitálny podpis z dokumentu a zo súkromného kľúča. Overovací algoritmus overuje korektnosť konkrétneho podpisu na základe dokumentu a verejného kľúča. Verejný kľúč je obvykle zverejnený a teda podpis môže overiť ktokoľvek.

Z dôvodu efektívnosti aj z bezpečnostných dôvodov nie je fakticky podpisovaný dokument ako taký, ale jeho odtlačok vypočítaný zvolenou hašovacou funkciou (pozri obr. 10.5). Preto je dôležité, aby hašovacia funkcia spĺňala vlastnosti spomínané v časti 10.1.2. Napríklad možnosť nájsť kolízie v hašovacej funkcii (teda dva rôzne dokumenty M_1, M_2 s rovnakým odtlačkom) znamená, že podpis dokumentu M_1 je zároveň korektným podpisom dokumentu M_2.



Obr. 10.5: Schéma pre digitálne podpisy

Najznámejšími schémami pre digitálne podpisy sú RSA a DSA (Digital Signature Algorithm, niekedy vo variante ECDSA využívajúcom tzv. eliptické krivky). Poznamenajme, že štandardná RSA podpisová schéma sa od RSA schémy pre asymetrické šifrovanie líši vo viacerých implementačných detailoch. Napriek tomu je matematická povaha asymetrického páru kľúčov rovnaká a niekedy je jeden pár kľúčov používaný na oba účely (teda v schéme pre asymetrické šifrovanie aj v schéme pre digitálne podpisy), hoci sa to neodporúča.

Napriek tomu, že verejný kľúč aj podpisový a overovací algoritmus sú známe, nie je efektívne možné bez znalosti súkromného kľúča vytvoriť k ľubovoľnému dokumentu korektný podpis. To znamená, že digitálne podpisy poskytujú ochranu integrity a autentickosti údajov. Navyše, ak je používateľ jediný, kto pozná svoj súkromný kľúč, tak korektný podpis dokumentu znemožňuje používateľovi poprieť vlastný podpis (hovoríme o nepopierateľnosti autorstva). Samozrejme, praktické použitie digitálnych podpisov si vyžaduje vyriešiť dôveryhodnú distribúciu verejných kľúčov, možnosť vyhlásiť neplatnosť verejného kľúča po prípadnom prezradení súkromného kľúča a množstvo ďalších praktických otázok. Tie sa snaží riešiť tzv. infraštruktúra verejných kľúčov (pozri časť 10.3.3) aj s príslušným právnym rámcom[1].

[1] V prostredí EÚ je to Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifi-

Tabuľka 10.1 porovnáva základné charakteristiky hašovacích funkcií, autentizačných kódov a digitálnych podpisov.

	Hašovacie funkcie	Autentizačné kódy	Digitálne podpisy
Integrita	áno	áno	áno
Autentickosť	nie	áno	áno
Nepopierateľnosť autorstva	nie	nie	áno
Kľúče	žiadne	symetrické	asymetrický pár kľúčov
Efektívnosť	rýchle	rýchle	pomalé
Typická aplikácia	kontrola integrity statických dát	autentickosť paketov pri prenose v sieti	autentickosť dokumentov

Tabuľka 10.1: Porovnanie hašovacích funkcií, autentizačných kódov a digitálnych podpisov

10.2 Protokoly

Kryptografické protokoly sú postupnosť krokov a výmen správ medzi dvoma alebo viacerými účastníkmi, s cieľom naplniť konkrétne bezpečnostné požiadavky. Pritom protokoly využívajú rôzne kryptografické konštrukcie. Pokiaľ spracovanie údajov zahŕňa interakciu a prenos údajov medzi systémami alebo používateľmi, je z hľadiska bezpečnosti typicky potrebné zabezpečiť dve základné požiadavky:

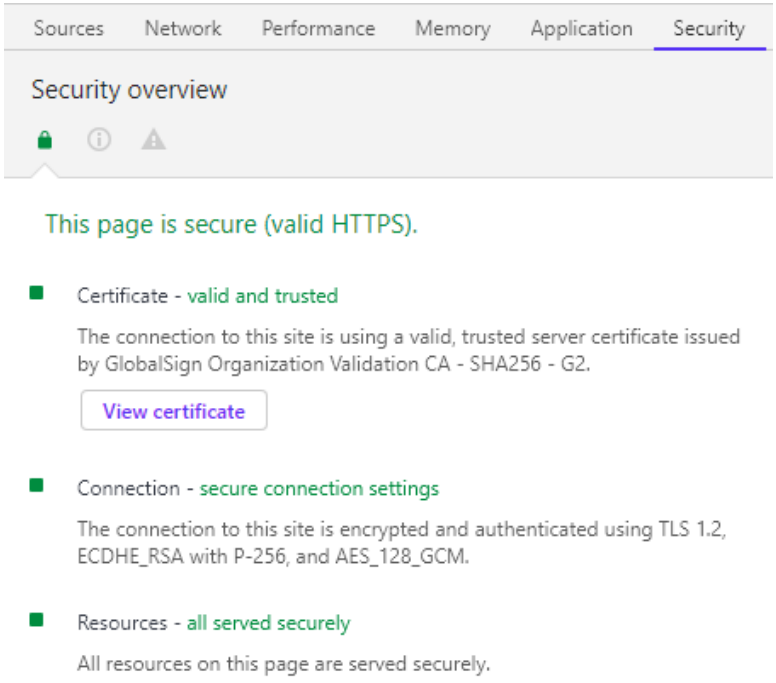
1. Autentizácia komunikujúcich účastníkov – každý účastník si vie overiť, že komunikuje so želaným partnerom.
2. Dohodnúť a distribuovať kryptografické kľúče (a ďalšie parametre), ktoré sa v následnej komunikácii použijú na šifrovanie, výpočet autentizačných kódov, prípadne na zabezpečenie iných bezpečnostných atribútov pomocou vhodných kryptografických konštrukcií.

Uvedené požiadavky napĺňa najvýznamnejšia trieda kryptografických protokolov – protokoly pre autentizáciu a dohodnutie kľúčov. Prirodzene, tieto protokoly sú obvykle vykonané pri nadväzovaní spojenia. Najpoužívanejším protokolom tohto typu je TLS (Transport Layer Security), niekedy sa možno stretnúť aj so starším označením SSL (Secure Sockets Layer). Ďalším príkladom je IKE (Internet Key Exchange), využívaný v rámci štandardu IPsec. Účastníka možno autentizovať len na základe nejakých dôveryhodne distribuovaných informácií. Takou informáciou môže byť verejný kľúč, napr. vo forme certifikátu (najčastejší spôsob v prípade autentizácie webového servera v TLS) alebo spoločná tajná informácia dohodnutá a distribuovaná dôveryhodným spôsobom vopred (pomerne častý spôsob v prípade IPsec). V prípade

kácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu (známe aj ako eIDAS) a súvisiace politiky a štandardy.

verejného kľúča dokazuje účastník svoju identitu tým, že preukáže znalosť prislúchajúceho súkromného kľúča – typicky podpíše vhodnú správu využijúc svoj súkromný kľúč, alebo je schopný dešifrovať dáta šifrované s použitím jeho verejného kľúča.

Keďže používateľ sa pri používaní webu stretne s TLS, ilustrujme použitie kryptografických techník práve na tomto protokole. V TLS je použitý komunikačný model klient-server, pričom klient je ten účastník protokolu, ktorý zahajuje komunikáciu, napr. webový prehliadač používateľa. V úvode protokolu si klient a server dohodnú sadu nimi preferovaných a podporovaných kryptografických techník. TLS ponúka istú flexibilitu pri voľbe algoritmov a metód dohodnutia kryptografických kľúčov, skúsme sa preto zamerať na jednu z možností, pričom sa opäť nevyhneme značnému zjednodušovaniu. Server pošle klientovi svoj verejný kľúč vo forme certifikátu podpísaného nejakou certifikačnou autoritou. Pokiaľ má klient vhodným spôsobom získaný verejný kľúč certifikačnej autority a dôveruje jej, dokáže overiť digitálny podpis na certifikáte a tým autentickosť verejného kľúča servera. Server použije svoj súkromný kľúč na podpísanie údajov slúžiacich pre dohodnutie kľúčov, ktoré spolu s popisom pošle klientovi. Následne klient prostredníctvom verejného kľúča servera overí autentickosť získaných údajov. Klient vytvorí vlastné údaje, ktoré spoločne s údajmi servera umožnia odvodiť kľúče a ďalšie potrebné parametre. Zároveň tieto údaje pošle aj serveru, ktorý vykoná rovnaké odvodenie. Po získaní kľúčov je nadviazanie spojenia dokončené a vytvorený zabezpečený komunikačný kanál je k dispozícii aplikácii (teda napr. webovému prehliadaču).



Obr. 10.6: Parametre TLS na stránke Európskej komisie, https://ec.europa.eu (november 2020)

Obrázok 10.6 ilustruje informácie o TLS spojení, ktoré vytvorí prehliadač s webovým serverom Európskej komisie. Z uvedeného si možno všimnúť verziu TLS protokolu (1.2), šifrovací algoritmus (AES s kľúčom dĺžky 128 bitov), použitý mód (GCM zabezpečujúci autentizované šifrovanie) a mechanizmus použitý na dohodnutie kľúčov (ECDHE_RSA využívajúci eliptickú

krivku P-256). Zároveň je vidieť, že certifikát verejného kľúča webového servera vydala certifikačná autorita GlobalSign, pričom ďalšie informácie o certifikáte sú k dispozícii samostatne.

Základné charakteristiky TLS sú zhrnuté v tabuľke 10.2. Poznamenajme, že konkrétne techniky podstatne závisia na verzii TLS ako aj na konfigurácii klienta a servera. Napríklad vo verzii TLS 1.3, štandardizovanej v roku 2018, sú na šifrovanie prípustné výlučne konštrukcie poskytujúce autentizované šifrovanie.

	TLS (v závislosti na verzii a konfigurácii)
Autentizácia servera	povinná (znalosť súkromného kľúča k verejnému kľúču uvedenom v certifikáte)
Autentizácia klienta	voliteľná (málokedy používané, obvykle riešené po vytvorení TLS spojenia samostatne)
Distribúcia kľúčov	viaceré protokoly (odvodenie kľúčov a ďalších parametrov pre šifrovanie, prípadne pre autentizačné kódy)
Dôvernosť	symetrické šifrovanie (podpora rôznych algoritmov a módov)
Autentickosť	autentizačné kódy alebo autentizované šifrovanie (podpora rôznych algoritmov)
Úprava aplikácie využívajúcej protokol	zvyčajne potrebné v aplikácii špecificky inicializovať komunikačný kanál

Tabuľka 10.2: Základné charakteristiky TLS

10.3 Heslá a kryptografické kľúče

10.3.1 Heslá

Heslá sú najpoužívanejším autentizačným prostriedkom. Sú príkladom autentizácie založenej na znalosti, na rozdiel od autentizačných mechanizmov založených na vlastníctve (niečo čo máte, typicky rôzne hardvérové tokeny) alebo identite (niečo čím ste, typicky biometrické metódy). Heslo je reťazec znakov a obvykle ho volí používateľ sám. V niektorých systémoch/aplikáciách je obmedzená dĺžka ako aj abeceda hesla – napr. v prípade PIN kódov používaných pri platobných kartách, pri SIM kartách v mobilných telefónoch, alebo v prípade bezpečnostného osobného kódu (BOK) k eID karte.

Na bezpečnosť autentizácie využívajúcej heslá vplýva viacero faktorov, uveďme tie najvýznamnejšie:

- Dĺžka a „náhodnosť“ hesla – čím je heslo dlhšie a náhodnejšie, tým viac pokusov potrebuje útočník na jeho uhádnutie. Pri heslách volených používateľmi je dostatočná náhodnosť problematická (aj schopnosť pamätať si náhodné heslá). V praxi je preto zvyčajne požiadavka na dĺžku hesla dôležitejšia ako jeho náhodnosť.
- Spôsob prenosu a overovania hesla – heslo má byť prenášané cez komunikačný kanál so zabezpečenou dôvernosťou, ako prevencia pred odpočutím hesla útočníkom.

- Spôsob uloženia hesla na strane používateľa – v ideálnom prípade si používateľ heslá pamätá, používa rôzne heslá v rôznych systémoch a nemá spoločné heslá s inými používateľmi. Vhodnou alternatívou je použitie aplikácií na správu hesiel.
- Spôsob uloženia hesla na strane systému (servera) – heslá nie sú uložené v otvorenom tvare, pre zníženie dopadov kompromitácie servera (ak útočník získa neoprávnený prístup k údajom servera).
- Ďalšie parametre autentizácie – definovanie počtu neúspešných pokusov zadania hesla, po ktorom sa prístup používateľa zablokuje (v prípade PIN kódov obvykle 3), vynútenie zmeny iniciálneho hesla a iné opatrenia znižujúce pravdepodobnosť úspešného útoku.

Ďalší spôsob použitia hesiel je odvodenie symetrických kryptografických kľúčov. Predstavme si situáciu, že používateľ má svoj súkromný kľúč pre podpisovú schému uložený v súbore na lokálnom disku. Pre minimalizáciu rizika prezradenia kľúča je tento súbor zašifrovaný (obvykle aj s nejakou formou ochrany integrity). Keďže používateľ si pravdepodobne nie je schopný zapamätať povedzme 128 bitov dlhý, náhodne zvolený symetrický kľúč, tento sa v podobných situáciách odvodí z hesla. Teda z hesla zvoleného používateľom je vypočítaný symetrický šifrovací kľúč a ten následne použitý na šifrovanie alebo dešifrovanie súboru so súkromným kľúčom. Podobne sa kľúče z hesiel odvádzajú aj v iných situáciách. Samozrejme, náhodnosť takto získaného kľúča je nižšia ako keby bol volený skutočne náhodne. Na druhej strane je používateľ schopný si heslo zapamätať. Bezpečnosť takéhoto použitia hesiel je ovplyvnená aj konkrétnym algoritmom, ktorým sa heslo transformuje na kľúč. Podobne ako pre iné kryptografické konštrukcie, aj v tomto prípade existujú vhodné štandardy (napr. PBKDF2 – Password-Based Key Derivation Function 2 [6]).

Koľko bitov náhodnosti sa skrýva v hesle? Porovnanie odhadovanej náhodnosti hesiel volených používateľom voči dĺžke náhodného symetrického kľúča nie je priamočiare. Schopnosť útočníka hádať heslo závisí na tom, či je heslo alebo jeho podstatná časť zo slovníka, rôznorodosti znakov, použití číselných postupností, opakovaní znakov, dĺžke a pod. Silu zvoleného hesla odhadujú niektoré webové stránky pri vytvorení účtu, programy na správu hesiel alebo špecializované aplikácie. Na ilustráciu uvádzame v nasledujúcej tabuľke porovnanie odhadov sily niekoľkých hesiel prostredníctvom programu na správu hesiel KeePass[2] a knižnice zxcvbn[3] určenej na odhad sily hesiel. Čísla v tabuľke vyjadrujú ekvivalentnú dĺžku symetrického kľúča v bitoch.

heslo	KeePass	zxcvbn
`qwerty`	12	2.32
`password1`	8	7.57
`JE38bslk@psl`	67	39.86
`spidersarecoolandfun`	72	50.66

O sile používateľských hesiel je možné urobiť si predstavu z útokov v reálnom prostredí. V roku 2012 bola publikovaná databáza odtlačkov hesiel približne 6,5 milióna používateľov

[2] https://keepass.info (november 2020)
[3] https://github.com/dropbox/zxcvbn (november 2020)

služby LinkedIn. Jednoduchý slovníkový útok bez špeciálneho hardvéru umožnil v priebehu 4 hodín zistiť heslá cca. 900 tisíc používateľov. Ďalšie pokračovanie v slovníkovom útoku viedlo celkovo k takmer 2 miliónom zistených hesiel. Nezanedbateľná časť používateľov volí a používa pomerne slabé heslá. Podobný záver možno spraviť aj z databáz uniknutých hesiel rôznych webových služieb. Pätnásť najčastejších hesiel v takýchto databázach v roku 2019 sú v nasledujúcej tabuľke (pričom autori analýzy[4] uvádzajú, že takmer 10% používateľov použilo niektoré heslo z top 25):

1.	123456	6.	12345678	11.	abc123
2.	123456789	7.	12345	12.	qwerty123
3.	qwerty	8.	iloveyou	13.	1q2w3e4r
4.	password	9.	111111	14.	admin
5.	1234567	10.	123123	15.	qwertyuiop

10.3.2 Kľúče

Spôsob narábania s kryptografickými kľúčmi je najvýznamnejším faktorom ovplyvňujúcim bezpečnosť kryptografických konštrukcií v praxi. Správa kryptografických kľúčov zahŕňa hlavne nasledujúce činnosti:

1. Generovanie kľúčov – postupy vytvárania kľúčov, vrátane použitých zdrojov náhodnosti. Kľúče musia byť nepredikovateľné, vyberané z dostatočne veľkej množiny.

2. Distribúcia kľúčov – spôsob doručenia kľúčov používateľom alebo na cieľový systém/server, vrátane naplnenia bezpečnostných požiadaviek pri distribúcii kľúčov (napr. dôvernosť, autentickosť).

3. Ukladanie a prístup ku kľúčom – spôsob uloženia kľúčov a opatrenia pre riadenie prístupu k nim nielen počas prevádzky, ale aj pri zálohovaní a archivácii.

4. Ničenie kľúčov – spôsob vymazania kľúčov, ktoré už nie sú potrebné.

Pri správe kľúčov je vhodné definovať aj postupy pri kompromitácii alebo pri zneplatňovaní kľúčov, intervaly výmen kľúčov a pod.

V prípade adekvátnej správy kľúčov je bezpečnosť kryptografických konštrukcií určená hlavne ich kryptografickou kvalitou a dĺžkou používaných kľúčov. Inštitúcie ako NIST (National Institute of Standards and Technology), NSA (National Security Agency), BSI (nemecký Bundesamt für Sicherheit in der Informationstechnik) a iné vydávajú odporučenia pre vhodné algoritmy a dĺžky kľúčov. Napríklad NSA zverejnila požiadavky na dĺžky kľúčov a algoritmy v tzv. Commercial National Security Algorithm (CNSA) Suite [1], pre kryptografickú ochranu údajov klasifikovaných až po TOP SECRET. Pre zabezpečenie dôvernosti je požadovaný AES-256, pre digitálne podpisy RSA schéma s aspoň 3072 bitov dlhým verejným kľúčom alebo ECDSA schéma konkrétnou štandardizovanou eliptickou krivkou, atď.

[4] SplashData's Top 50 Worst Passwords of 2019; štatistika na základe niekoľko miliónov uniknutých hesiel.

Z povahy kryptografických konštrukcií vyplýva, že útočník môže hľadať symetrický kľúč vyskúšaním všetky možností. Podobne môže riešiť konkrétny matematický problém v prípade asymetrických šifrovacích schém alebo schém pre digitálne podpisy. Ilustrujme schopnosť útočníka prezrieť redukovaný priestor kľúčov pre algoritmus AES-128 v nasledujúcej tabuľke. Súčasné procesory sú schopné s hardvérovou podporou AES realizovať niekoľko sto miliónov dešifrovacích operácií AES-128 za sekundu (využijúc všetky jadrá). Predpokladajme 300 miliónov operácií za sekundu. V stĺpcoch je uvažovaný individuálny útočník s jedným počítačom, a stredne veľká firma s 500 počítačmi. Hodnoty v tabuľke vyjadrujú veľkosť priestoru, ktorý dokáže útočník za daný čas prezrieť, pričom veľkosť priestoru je vyjadrená dĺžkou symetrického kľúča v bitoch (napr. 40 bitov je $2^{40} = 1\,099\,511\,627\,776$ možností).

Čas útoku	Individuálny útočník (1 procesor)	Stredne veľká firma (500 procesorov)
1 minúta	34	43
1 hodina	40	49
1 deň	45	54
30 dní	49	58
1 rok	53	62
100 rokov	60	69

Tabuľka má výlučne ilustratívny charakter, iné algoritmy majú inú rýchlosť, procesory sa postupne zrýchľujú a zlacňujú, špecializované zákaznícke integrované obvody skonštruované na takýto účel majú v pomere k cene vyšší výkon. Napríklad 1024 krát rýchlejší procesor by znamenal pripočítanie 10 k hodnotám uvedeným v tabuľke. Bez ohľadu tieto fakty, ponúka tabuľka dobrú predstavu o exponenciálnom raste počtu potenciálnych kľúčov s rastom ich dĺžky a snáď aj o dostatočnej dĺžke 128 alebo 256 bitového kľúča.

Je dôležité si uvedomiť, že tabuľka ukazuje možnosti útočníka v situácii, keď sú kľúče volené skutočne náhodne a s rovnakou pravdepodobnosťou. Útočník je v oveľa lepšej situácii, ak sú niektoré kľúče pravdepodobnejšie ako iné, prípadne ak sa niektoré kľúče určite nepoužijú. To platí napríklad v situácii, ak sú kľúče odvodené z hesiel.

Viaceré kryptografické konštrukcie, napr. niektoré podpisové schémy a protokoly, využívajú ďalšie náhodne volené parametre. Náhodnosť, prípadne dôvernosť týchto parametrov má priamy dopad na bezpečnosť konštrukcií. Ilustratívnym príkladom je implementácia digitálnych podpisov v herných konzolách PlayStation 3 spoločnosti Sony, s cieľom zabrániť nahratiu a spusteniu neautorizovaného (nepodpísaného) kódu. Použitie statického namiesto náhodného parametra pri podpisovaní algoritmom ECDSA viedlo v roku 2010 k prezradeniu súkromného podpisového kľúča a útočník následne dokázal podpísať akýkoľvek kód.

10.3.3 Infraštruktúra verejných kľúčov

Asymetrické kryptografické konštrukcie, či už pre šifrovanie alebo digitálne podpisy, majú výhodu v tom, že verejné kľúče môžu byť zverejnené a teda nie je potrebné zabezpečovať ich dôvernosť. Problémom je však autentickosť verejných kľúčov. Ako sa odosielateľ údajov uistí o tom, že verejný šifrovací kľúč patrí naozaj adresátovi, a teda nepošle údaje šifrované verejným

kľúčom, ktorý podstrčil útočník? Ako sa vieme presvedčiť, že verejný kľúč, ktorý použijeme na overenie digitálneho podpisu, skutočne patrí konkrétnemu autorovi dokumentu?

Tento problém je ľahko riešiteľný v prostredí s malým počtom účastníkov, ktorí sa navzájom poznajú a môžu si svoje verejné kľúče odovzdať osobne. Takéto riešenie sa však nedá aplikovať vo všeobecnom prípade veľkého počtu vzdialených alebo vopred neznámych účastníkov. Cieľom infraštruktúry verejných kľúčov je definovať technické (kryptografické) a organizačné metódy a postupy na dosiahnutie dôveryhodnej distribúcie verejných kľúčov. Infraštruktúra verejných kľúčov (PKI – public key infrastructure) prenáša dôveru účastníkov na dôveryhodný subjekt – certifikačnú autoritu. Certifikačná autorita vydáva certifikáty verejných kľúčov, čo sú digitálne podpísané dátové štruktúry obsahujúce, okrem ďalších atribútov (podrobnejší príklad je uvedený v prílohe):

- jednoznačnú identifikáciu subjektu, pre ktorý je certifikát vydaný, napríklad doménové meno web servera, meno a e-mailová adresa používateľa a pod.,
- verejný kľúč subjektu, vrátane identifikácie konkrétneho kryptografického algoritmu, pre ktorý je kľúč určený,
- účel použitia verejného kľúča, či slúži na šifrovanie alebo overovanie podpisov (tým zároveň hovorí o účele použitia zodpovedajúceho súkromného kľúča),
- interval platnosti certifikátu, určujúci odkedy a dokedy je certifikát platný,
- digitálny podpis certifikačnej autority, umožňujúci overiť autentickosť všetkých údajov v certifikáte.

Fungovanie PKI sa opiera o dva predpoklady. Prvým je dôvera účastníkov, že certifikačná autorita si plní svoje úlohy čestne a bezpečne. Druhým je dôveryhodná distribúcia verejného kľúča certifikačnej autority, pomocou ktorého si vedia účastníci overiť podpis certifikačnej autority v certifikátoch a teda autentickosť údajov v nich obsiahnutých. Obvykle sa takáto distribúcia vykoná zároveň s distribúciou softvéru, napr. webové prehliadače obsahujú po inštalácii zoznam niekoľkých desiatok certifikátov verejných kľúčov certifikačných autorít (tzv. koreňových certifikátov), ktorým používatelia implicitne dôverujú. V organizáciách sa často certifikáty certifikačných autorít, napr. vlastných, používaných na interné účely, distribuujú prostredníctvom nástrojov na správu koncových zariadení (PC, notebooky, mobilné telefóny). Verejný kľúč certifikačnej autority sa distribuuje vo formáte „samopodpísaného“ certifikátu, teda podpis je možné overiť verejným kľúčom, ktorý je uvedený v certifikáte. Samozrejme, samopodpísaný certifikát s ľubovoľnou sadou atribútov si vie vygenerovať ktokoľvek, preto je dôležitý mechanizmus, akým sa certifikáty certifikačných autorít distribuujú.

Hlavnou úlohou certifikačnej autority je vydávať certifikáty verejných kľúčov. To vyžaduje overiť identitu subjektu, ktorý žiada o certifikát, aby nemohol útočník žiadať certifikát napríklad pre server accounts.google.com alebo www.paypal.com. Zároveň certifikačná autorita overuje ďalšie skutočnosti, napr. znalosť súkromného kľúča zodpovedajúceho k verejnému kľúču subjektu. Činnosti certifikačnej autority, ktoré nevyžadujú prácu so súkromným kľúčom sú často delegované na registračnú autoritu, zabezpečujúcu kontakt so zákazníkmi (teda subjektmi so záujmom o vydanie vlastného certifikátu). Sú známe príklady, keď bezpečnostné

zlyhania certifikačnej autority alebo jej registračnej autority viedli k vydaniu falošných certifikátov. Holandská certifikačná autorita DigiNotar v dôsledku bezpečnostných problémov vyhlásila v roku 2011 bankrot. V rovnakom roku zápasila s kompromitáciou používateľského účtu v registračnej autorite certifikačná autorita Comodo. Pochybná prax pri vydávaní certifikátov certifikačnými autoritami prevádzkovanými spoločnosťou Symantec (Thawte, GeoTrust a ďalšie) viedla v rokoch 2017 a 2018 postupne až k tomu, že webové prehliadače prestali dôverovať certifikátom vydaným týmito certifikačnými autoritami pred decembrom 2017. Aktivity Symantecu v tejto oblasti prevzala spoločnosť DigiCert.

Infraštruktúra verejných kľúčov musí byť pripravená aj na situáciu, keď bude súkromný kľúč niektorého subjektu prezradený. V takom prípade je potrebné zneplatniť certifikát ešte pred uplynutím intervalu platnosti uvedeného v certifikáte. V princípe sa používajú dve riešenia:

- zoznam zneplatnených certifikátov (CRL, Certificate revocation list) – periodicky vydávaný zoznam podpísaný certifikačnou autoritou, obsahujúci sériové čísla zneplatnených certifikátov;
- interaktívny protokol (OCSP, Online Certificate Status Protocol), ktorý umožňuje spýtať sa certifikačnej autority na platnosť konkrétneho certifikátu online.

10.4 Zraniteľnosti a kryptografia

Najznámejšou databázou softvérových zraniteľností je NVD (National Vulnerability Database), ktorú prevádzkuje NIST. NVD zraniteľnosti klasifikuje podľa typu, závažnosti a iných atribútov. V roku 2019 bolo v NVD publikovaných viac ako 17 300 zraniteľností[5]. Samozrejme, samotný počet zraniteľností nehovorí nič o ich závažnosti alebo reálnej zneužiteľnosti v praxi. Nakoniec, stačí jedna zraniteľnosť na kompromitáciu práve vášho systému, servera, siete alebo aplikácie.

Kategória	Počet
Cryptographic issues	48
Improper Certificate Validation	112
Use of Hard-coded Credentials	124
Missing Encryption of Sensitive Data	82
Cleartext Storage of Sensitive Information	63
Cleartext Transmission of Sensitive Information	70
Key Management Errors	21
Inadequate Encryption Strength	57
Use of a Broken or Risky Cryptographic Algorithm	35
Use of Cryptographically Weak Pseudo-Random Number Generator	10
Improper Verification of Cryptographic Signature	44
Insufficient Entropy	7

Tabuľka 10.3: Počty zraniteľností vo vybraných kategóriách NVD v roku 2019

[5]Zdroj: https://nvd.nist.gov (november 2020)

Štatistiku NVD zneprehľadňuje použitie väčšieho počtu detailných kategórií, takže jednoznačne určiť všetky „kryptografické“ zraniteľnosti nie je priamočiare. Počty zraniteľností pre vybrané kategórie uvádzame v tabuľke 10.3[6]. Častým problémom je absencia kryptografických opatrení ako takých – napríklad prenos citlivých údajov alebo aktualizácia softvéru cez nezabezpečené spojenie. Tabuľka poukazuje aj na ďalšie problémy súvisiace s implementáciou kryptografie:

- použitie fixných hesiel alebo kľúčov pre servisné účty alebo takéto heslá/kľúče odvodené z verejne známych údajov,
- nedostatočná (neúplná) kontrola certifikátov alebo podpisov,
- chyby pre správe kľúčov,
- použitie neadekvátnych kryptografických algoritmov (slabé šifrovacie algoritmy alebo algoritmy s nedostatočnou dĺžkou kľúča, slabé generátory pseudonáhodných čísel), atď.

Iný pohľad na zraniteľnosti súvisiace s kryptografiou ponúka napr. správa spoločnosti Veracode [9], kde na základe výsledkov testovania softvéru pomocou analýzy kódu boli Cryptographic issues treťou najčastejšie sa vyskytujúcou kategóriou zraniteľností (nachádzané v takmer dvoch tretinách testovaných aplikácií), tesne za Information leakage a CRLF Injection.

10.5 Štandardy a legislatívne požiadavky

Väčšina v praxi používaných kryptografických konštrukcií je štandardizovaná. Šifrovacie algoritmy (symetrické aj asymetrické schémy), hašovacie funkcie, autentizačné kódy, schémy pre digitálne podpisy, protokoly, ako aj ďalšie konštrukcie sú k dispozícii vo forme štandardov. To zvyšuje vzájomnú interoperabilitu a čiastočne predchádza bezpečnostným zraniteľnostiam a chybám vďaka otvorenej možnosti ich analyzovať a pripomienkovať. Najčastejšie používané štandardy vydáva NIST a z pochopiteľných dôvodov sú široko akceptované výrobcami softvéru a hardvérových zariadení. Kryptografické protokoly, napr. TLS, IPSec, SSH a podobne, sú najčastejšie štandardizované vo forme RFC (Request for Comments).

Štandardy v oblasti informačnej bezpečnosti sa venujú kryptografii skôr okrajovo, pričom sa sústredia najmä na správu kľúčov a používanie štandardných kryptografických konštrukcií. Medzinárodný štandard ISO/IEC 27001:2013 [4] definuje pre systém riadenia informačnej bezpečnosti nasledujúce požiadavky v oblasti kryptografie (vhodné naplnie požiadaviek prostredníctvom opatrení možno potom nájsť v ISO/IEC 27002:2013 [5]):

- Politika používania kryptografických opatrení na ochranu informácií – zahŕňa vytvorenie a implementáciu príslušnej politiky.
- Správa kľúčov – zahŕňa vytvorenie a implementáciu politiky týkajúcej sa používania a ochrany kryptografických kľúčov počas ich životného cyklu.

[6] Len na porovnanie spomeňme, že v rovnakom období bolo publikovaných 2334 zraniteľností typu XSS a 539 zraniteľností typu CSRF.

Bezpečnostné hodnotenie a certifikácia IT systémov je cieľom Spoločných kritérií na hodnotenie bezpečnosti informačných technológií[7], známych ako „Common Criteria“. Konkrétna verzia bola vydaná aj ako štandard ISO/IEC 15408. Podľa Spoločných kritérií je možné hodnotiť rôzne komponenty ako sú napríklad operačný systém, čipová karta, firewall, databázový server, smerovač a pod. Zoznam certifikovaných produktov je dostupný na stránke projektu. Z hľadiska kryptografie definujú Spoločné kritériá vo verzii 3.1 funkčnú triedu *Kryptografická podpora* s dvoma množinami požiadaviek:

- Správa kryptografických kľúčov – zahŕňa všeobecné požiadavky na generovanie, distribúciu, prístup a deštrukciu kľúčov s tým, že v systéme sú používané štandardizované konštrukcie.
- Prevádzka kryptografie – všeobecná požiadavka na vykonávanie kryptografických operácií v súlade s explicitne definovanými štandardami.

Štandard FIPS 140-2 vydal NIST a definuje bezpečnostné požiadavky pre kryptografické moduly. Ide o najčastejšie používaný štandard pre bezpečnostné posúdenie kryptografických modulov. Moduly môžu byť rôznorodé – kryptografická knižnica operačného systému, šifrovaný pamäťový USB kľúč, čipová karta, hardvérový bezpečnostný modul a pod. Štandard definuje 4 bezpečnostné úrovne, od úrovne 1 až po úroveň 4 s postupne sprísňovanými požiadavkami. Medzi oblasti, v ktorých sú požiadavky definované patria špecifikácia modulu, role, služby, autentizácia, fyzická bezpečnosť modulu, samotestovanie, správa kľúčov, elektromagnetické vyžarovanie a ďalšie. Počet vydaných osvedčení pre jednotlivé úrovne v roku 2019 je uvedený v nasledujúcej tabuľke. Pre zaujímavosť uveďme, že k novembru 2020 existujú celkovo len 3 moduly s platnými certifikátmi na úrovni 4 podľa FIPS 140-2 (a 12 ďalších s historickými, už neplatnými certifikátmi).

Úroveň podľa FIPS 140-2	2019
Level 1	132
Level 2	72
Level 3	26
Level 4	1

NIST vydal v roku 2019 novú verziu štandardu FIPS 140-3 [8]. Ten vychádza zo štandardov ISO/IEC 19790:2012 [2] a ISO/IEC 24759:2017 [3], v ktorých niektoré časti modifikuje a spresňuje vlastnými požiadavkami. Testovanie kryptografických modulov podľa FIPS 140-3 malo začať v septembri 2020 a testovanie podľa FIPS 140-2 má byť ukončené v septembri 2021[8].

Podotknime, že certifikácia konkrétneho produktu nie je zárukou jeho bezpečnosti. Certifikácia je overenie splnenia konkrétnych požiadaviek a nie bezpečnostná analýza. Ilustratívnym príkladom boli šifrované pamäťové USB kľúče spoločností Verbatim, Kingstone a SanDisk, certifikované na úrovni 2 podľa FIPS 140-2. V roku 2010 sa ukázalo, že k dešifrovaniu a získaniu

[7] https://www.commoncriteriaportal.org (november 2020)
[8] https://csrc.nist.gov/projects/fips-140-3-transition-effort (november 2020)

prístupu k údajom postačuje jednoduchá úprava riadiaceho programu bez znalosti prístupového kľúča. Ďalším príkladom je DUHK (Don't Use Hard-coded Keys) útok, publikovaný v roku 2017, ktorý využíva použitie schváleného (do roku 2016), avšak zastaraného generátora náhodných čísel spolu s pevne nastavenou iniciálnou hodnotou. Dôsledkom takejto kombinácie je schopnosť útočníka predikovať výstup generátora, čo v niektorých prípadoch znamená získanie kryptografických kľúčov. Zaujímavosťou je, že k identifikácii zraniteľných certifikovaných zariadení prispeli práve dokumenty z certifikačného procesu FIPS 140-1 a 140-2.

Napriek uvedenému majú certifikáty produktov svoj význam – hovoria o tom, že tvorcovia museli naplniť isté bezpečnostné požiadavky. Produkt s vhodnou úrovňou certifikácie podľa Spoločných kritérií a FIPS 140-2 vzbudzuje väčšiu dôveru ako produkt bez certifikácie.

10.5.1 Legislatíva SR

Niektoré kryptografické požiadavky možno nájsť aj v normatívnych právnych aktoch SR. V tejto časti uvedieme vybrané príklady. Poznamenajme, že požiadavky obvykle s istým oneskorením reflektujú realitu, dostupnosť konkrétnych technológií a sú formulované všeobecne. Záujemcom o skúmanie týchto a ostatných zmienok o kryptografii v právnych predpisoch možno odporučiť funkciu vyhľadávania na portáli Slov-Lex[9].

Vyhláška č. 78/2020 Z.z. o štandardoch ITVS

Vyhláška č. 78/2020 Z. z. Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu o štandardoch pre informačné technológie verejnej správy[10] uvádza:

- (§3) používanie skupiny protokolov Internet Procotol Security (IPsec) na zabezpečenie sieťových protokolov;
- (§4, §6, §7, §10) podpora kryptografického protokolu Transport Layer Security (TLS) pre chránený prenos dát, pri prenose elektronických poštových správ, pri chránenom prístupe k verejným elektronickým poštovým službám, pri chránenom verejnom prístupe k adresárovým službám;
- (§8) používanie formátu Secure/Multipurpose Internet Mail Extensions (S/MIME) pri chránenom prenose elektronických poštových správ;
- (§9) používanie protokolu Hypertext Transfer Protocol (HTTP) s Transport Layer Security (TLS) na zabezpečenie prenosu dát medzi klientom a webovým serverom a medzi webovými servermi.

Pre obsah webového sídla (§15) požaduje výnos zverejnenie kontaktnej informácie, na ktorej je možné získať kontrolný reťazec znakov na overenie pravosti certifikátov a verejných kľúčov používaných orgánom riadenia pre elektronické služby verejnej správy a elektronické správy; zverejnenie najmenej jedného verejného kľúča pre chránený prenos elektronických správ, ak orgán riadenia takýto prenos poskytuje. Ďalšie požiadavky možno nájsť v časti venovanej správe cloud computingu a inde.

[9] https://www.slov-lex.sk/ (november 2020)
[10] https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2020/78/20200501 (november 2020)

Vyhláška č. 179/2020 Z.z. – kategorizácia a obsah bezpečnostných opatrení ITVS

Vyhláška č. 179/2020 Z. z. Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu, ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy, určuje aj niektoré kryptografické opatrenia (v závislosti na kategorizácii ITVS). V prílohe č. 2 ich možno nájsť vo viacerých častiach:

- I. Sieťová a komunikačná bezpečnosť
- J. Akvizícia, vývoj a údržba informačných technológií verejnej správy
- N. Kryptografické opatrenia

Iné

Štandardizáciu a v oblasti elektronických podpisov a súvisiacej infraštruktúry potrebnú pre implementáciu nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu (eIDAS) má na starosti ETSI (Európsky inštitút pre telekomunikačné normy). Detaily o prípustných kryptografických algoritmoch možno nájsť v technických normách a špecifikáciách pripravovaných príslušnou technickou komisiou ETSI.

Do pôsobnosti zákona č. 215/2004 o ochrane utajovaných skutočností v znení neskorších prepisov patrí aj šifrová ochrana informácií, teda zabezpečenie ochrany utajovaných skutočností kryptografickými metódami. Keďže bezpečnostné štandardy pre oblasť šifrovej ochrany informácií (a ďalšie podrobnosti o kryptografických metódach) sú utajovanými skutočnosťami Národného bezpečnostného úradu, nie sú verejne prístupné.

10.6 Praktické rady na záver

Cieľom tejto časti je ponúknuť niektoré základné praktické rady týkajúce sa výberu a použitia kryptografických konštrukcií. Odporúčania nie sú vyčerpávajúce, ide o čisto subjektívne názory autora.

- ✓ Používajte štandardné kryptografické algoritmy, schémy a protokoly. Kryptografia nie je miesto na kreativitu a ad-hoc riešenia.
- ✓ Používajte kryptografické konštrukcie na dosiahnutie tých bezpečnostných atribútov, pre ktoré sú určené. Napríklad (štandardné, „neautentizované“) šifrovanie nezabezpečuje integritu ani autentickosť údajov, autentizačné kódy ani digitálne podpisy nezabezpečujú dôvernosť údajov.
- ✓ Používajte dostatočné dĺžky kľúčov a dbajte na kvalitu (náhodnosť) generovania kľúčov.
- ✓ Pravidelne meňte kľúče. Dlhodobo nezmenené kľúče považujte za prezradené.
- ✓ Voľte dostatočne dlhé heslá. Obvykle je heslo najslabším „kľúčom“ v systéme. Voľte rozličné heslá pre rôzne systémy a zvážte použitie aplikácie pre správu hesiel.
- ✓ Majte premyslené, čo robiť po kompromitácii kľúčov alebo hesiel.

- ✓ Ak môžete, použite certifikované riešenia. Poznajte rozsah a podmienky certifikácie. Pamätajte, že certifikácia nie je náhradou bezpečného používania.
- ✓ Poznajte konfiguračné možnosti kryptografických riešení a ich bezpečnostné dopady. Preferujte nastavenia podľa best-practice odporučení v danej oblasti.
- ✓ Dôsledne overujte certifikáty verejných kľúčov – meno subjektu, certifikačná autorita, aktuálna platnosť, interval platnosti, účel použitia a pod. Samopodpísaný certifikát nehovorí nič o autentickosti verejného kľúča.
- ✓ Koreňové certifikáty certifikačných autorít získajte dôveryhodným spôsobom.
- ✓ Venujte pozornosť relevantným bezpečnostným hrozbám a rizikám. Kryptografia nenahradí iné organizačné a technické bezpečnostné opatrenia.

10.7 Otázky a úlohy

Riešenie jednoduchých úloh a zamyslenie sa nad vybranými otázkami súvisiacimi s používaním kryptografických techník má pomôcť k lepšiemu pochopeniu a možno aj prehĺbeniu prebraných tém. Úlohy zámerne nemajú jediné riešenie.

1. Pomocou vhodného programu vytvorte šifrovaný archív (napr. zip). Aký šifrovací algoritmus je pritom použitý? Pokúste sa rozbaliť archív s nesprávnym aj so správnym heslom.
2. Stiahnite ostatnú bezpečnostnú aktualizáciu pre niektorý produkt spol. Microsoft[11] a overte jej SHA-256 odtlačok s tým, ktorý je publikovaný na webe.
3. Nájdite stránky testujúce kvalitu hesiel a vyskúšajte kvalitu niekoľkých hesiel. Akým spôsobom je prezentovaná kvalita hesla a aké parametre o kvalite rozhodujú?
4. Pre vybranú webovú stránku pomocou prehliadača zistite, aká certifikačná autorita vydala certifikát servera, pre aký algoritmus je určený verejný kľúč a aký je interval platnosti certifikátu.
5. Pre vybranú webovú stránku pomocou prehliadača zistite, aké sú parametre TLS spojenia – verzia, použité algoritmy.
6. Konfiguráciu TLS protokolu na webových serveroch dostupných z internetu možno otestovať viacerými voľne dostupnými službami. Najznámejšou je SSL Server Test[12]. Vyskúšajte, aké hodnotenie a výstupy služba produkuje pre vami zvolené web servery.
7. Zistite, akým certifikačným autoritám dôveruje váš prehliadač. Koľko ich je?
8. Na stránke NVD nájdite niektorú zraniteľnosť aplikácie, databázového systému alebo operačného systému, ktorý používate. Všimnite si rozsah evidovaných informácií a atribútov.

[11] napr. ostatný Cumulative Update pre Exchange Server 2019, https://docs.microsoft.com/en-us/exchange/new-features/build-numbers-and-release-dates (november 2020)

[12] https://www.ssllabs.com/ssltest (november 2020)

9. Vyberte si niektorý kryptografický modul certifikovaný podľa FIPS 140-2. Pozrite sa na to, aké informácie o module sú uvedené v certifikáte a v súvisiacej dokumentácii (Security Policy).

10. Nájdite kryptografické algoritmy prípustné pre podpisové schémy v rámci eIDAS. Ktorá technická norma ETSI ich definuje? Aké sú požadované dĺžky kľúčov?

Literatúra

[1] *Commercial National Security Algorithm (CNSA) Suite Factsheet*. National Security Agency. 2015. URL: https://apps.nsa.gov/iaarchive/library/ia-guidance/ia-solutions-for-classified/algorithm-guidance/commercial-national-security-algorithm-suite-factsheet.cfm (cit. 11/2020) (citované na strane 271).

[2] *ISO/IEC 19790:2012, Information technology – Security techniques – Security requirements for cryptographic modules*. International Organization for Standardization, 2012 (citované na strane 276).

[3] *ISO/IEC 24759:2017, Information technology – Security techniques – Test requirements for cryptographic modules*. International Organization for Standardization, 2017 (citované na strane 276).

[4] *ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements*. International Organization for Standardization, 2013 (citované na strane 275).

[5] *ISO/IEC 27002:2013, Information technology – Security techniques – Code of practice for Information Security Controls*. International Organization for Standardization, 2013 (citované na strane 275).

[6] K. Moriarty, B. Kaliski a A. Rusch. *PKCS #5: Password-Based Cryptography Specification Version 2.1*. RFC 8018. 2017. URL: https://tools.ietf.org/html/rfc8018 (citované na strane 270).

[7] *NIST Special Publication 800-57 Recommendation for Key Management – Part 1: General (Revision 5)*. National Institute of Standards and Technology, 2020. DOI: 10.6028/NIST.SP.800-57pt1r5 (citované na strane 261).

[8] *Security requirements for cryptographic modules*. FIPS PUB 140-3. National Institute of Standards and Technology, 2019. DOI: 10.6028/NIST.FIPS.140-3 (citované na strane 276).

[9] *State Of Software Security*. Volume 11. Veracode, 2020. URL: https://www.veracode.com/state-of-software-security-report (cit. 11/2020) (citované na strane 275).

Dodatok: Príklad štruktúry certifikátu

Uvádzame príklad štruktúry certifikátu, v tomto prípade z web stránky Európskej komisie. Na získanie a zobrazenie certifikátu sme použili program OpenSSL vo verzii 1.1.1.

```
$ openssl s_client -connect ec.europa.eu:443 </dev/null 2>/dev/null |
  openssl x509 -outform PEM >ec.pem
```

```
$ openssl x509 -in ec.pem -noout -text
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      34:d7:e3:da:71:a3:7d:6f:96:27:fa:6d
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C = BE, O = GlobalSign nv-sa,
            CN = GlobalSign Organization Validation CA - SHA256 - G2
    Validity
      Not Before: Jul 14 05:17:02 2020 GMT
      Not After : May 30 14:41:01 2021 GMT
    Subject: C = BE, ST = Brussels-Capital Region, L = Brussels,
             O = European Commission, CN = *.ec.europa.eu
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
        RSA Public-Key: (2048 bit)
          Modulus:
            00:d2:7a:2b:d6:3e:66:5d:9a:3b:c2:a5:bd:14:5b:
            ... vynechaných 16 riadkov ...
            71:69
          Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Key Usage: critical
        Digital Signature, Key Encipherment
      Authority Information Access:
        CA Issuers -
          URI:http://secure.globalsign.com/cacert/gsorganizationvalsha2g2r1.crt
        OCSP - URI:http://ocsp2.globalsign.com/gsorganizationvalsha2g2
      X509v3 Certificate Policies:
        Policy: 1.3.6.1.4.1.4146.1.20
        CPS: https://www.globalsign.com/repository/
        Policy: 2.23.140.1.2.2
      X509v3 Basic Constraints:
        CA:FALSE
      X509v3 CRL Distribution Points:
        Full Name:
        URI:http://crl.globalsign.com/gs/gsorganizationvalsha2g2.crl
      X509v3 Subject Alternative Name:
        DNS:*.ec.europa.eu, DNS:ec.europa.eu
      X509v3 Extended Key Usage:
        TLS Web Server Authentication, TLS Web Client Authentication
      X509v3 Authority Key Identifier:
        keyid:96:DE:61:F1:BD:1C:16:29:53:1C:C0:CC:7D:3B:83:00:40:E6:1A:7C
      X509v3 Subject Key Identifier:
        4E:BF:29:D5:1A:8B:E6:DC:5F:85:B3:EF:50:DD:F5:E3:44:F1:35:95
      CT Precertificate SCTs:
```

```
        Signed Certificate Timestamp:
          Version   : v1 (0x0)
          Log ID    : EE:C0:95:EE:8D:72:64:0F:92:E3:C3:B9:1B:C7:12:A3:
                      69:6A:09:7B:4B:6A:1A:14:38:E6:47:B2:CB:ED:C5:F9
          Timestamp : Jul 14 05:17:05.738 2020 GMT
          Extensions: none
          Signature : ecdsa-with-SHA256
                      30:46:02:21:00:A8:39:A4:B0:2F:D6:5E:7C:C5:07:28:
                      ... vynechané 3 riadky ...
                      D3:C5:9B:5D:C3:80:30:C8
          Signed Certificate Timestamp:
          Version   : v1 (0x0)
          Log ID    : F6:5C:94:2F:D1:77:30:22:14:54:18:08:30:94:56:8E:
                      E3:4D:13:19:33:BF:DF:0C:2F:20:0B:CC:4E:F1:64:E3
          Timestamp : Jul 14 05:17:05.788 2020 GMT
          Extensions: none
          Signature : ecdsa-with-SHA256
                      30:44:02:20:30:74:05:DC:51:23:E2:B8:74:4B:D2:99:
                      ... vynechané 3 riadky ...
                      7E:12:7D:6E:6F:11
    Signature Algorithm: sha256WithRSAEncryption
      8e:c5:73:2a:1e:1c:6c:87:bc:6c:25:63:78:48:f3:4a:e1:01:
      ... vynechaných 13 riadkov ...
      e5:cf:78:95
```

Kapitola 11

Kryptológia 2

Martin Stanek

Kapitola voľne nadväzuje na predchádzajúcu kapitolu *Kryptológia*, pričom postupne prehlbuje informácie o kryptografických konštrukciách. Napriek tomu, že obmedzíme matematickú stránku výkladu a v texte použijeme zjednodušenia, nevyhneme sa niektorým matematickým pojmom a zápisom. Predpokladáme, že čitateľ je oboznámený s poznatkami prezentovanými v predchádzajúcej kapitole *Kryptológia*. Záujemcom o podrobnejší a širší pohľad na túto problematiku možno znova odporučiť špecializovanú odbornú literatúru.

11.1 Symetrické konštrukcie

Symetrické šifry možno rozdeliť na blokové a prúdové. V praxi sú väčšinou používané blokové šifry. Dôvodom je fakt, že najdôležitejšie štandardy (napr. vydané NIST) primárne štandardizujú blokové šifry (v minulosti DES, v súčasnosti AES). Navyše, voľbou vhodného módu možno blokovú šifru používať aj ako prúdovú šifru.

11.1.1 Blokové šifry

Blokové šifry sú definované pre bloky bitov pevnej dĺžky, teda pre ľubovoľný kľúč šifra zobrazuje blok vstupných dát na rovnako dlhý blok zašifrovaných dát. Napríklad AES má dĺžku bloku 128 bitov, pre ľubovoľný variant dĺžky kľúča (teda 128, 192 alebo 256 bitov). Blokové šifry sú najčastejšie konštruované viacnásobnou iteráciou jednoduchšej transformácie (nazývanej „kolo“ algoritmu). Pre každé kolo sa používa špecifický kľúč, ktorý je odvodený presne definovaným spôsobom zo šifrovacieho kľúča.

Najpoužívanejšou blokovou šifrou súčasnosti je AES. Z hľadiska používania AES sú dôležité nasledujúce fakty:

- Viaceré procesory majú v hardvéri implementované špeciálne inštrukcie pre AES algoritmus. To znamená výrazné urýchlenie šifrovania a dešifrovania pre aplikácie/knižnice, ktoré takúto implementáciu vedia využiť. Ilustráciu výkonových rozdielov možno vidieť v časti 11.6.1.

- Použitie AES s dlhšími kľúčmi znamená mierne spomalenie šifrovania a dešifrovania, keďže AES-128 má 10 kôl, AES-192 má 12 kôl a AES-256 má 14 kôl. Pre praktické použitie je toto spomalenie zanedbateľné.

V starších systémoch sa možno stretnúť aj so šifrou 3DES (dĺžka bloku 64 bitov), niekedy označovaná ako Triple DES alebo TDEA. Šifra má varianty s kľúčmi dĺžky 56, 112, alebo 168 bitov. Pokiaľ je možné, odporúča sa 3DES v ľubovoľnom variante nepoužívať a migrovať na AES [25].

Operačné módy blokových šifier

Pre šifrovanie dát dlhších ako jeden blok je potrebné použiť šifru vo vhodnom operačnom móde. Nielen dĺžka dát však motivuje použitie rôznych módov. Tie sa navzájom odlišujú účelom použitia (napr. šifrovanie komunikácie alebo diskov), implementačnými vlastnosťami (napr. možnosť paralelizovať šifrovanie a/alebo dešifrovanie), bezpečnostnými požiadavkami (dôvernosť a autentickosť) a pod. NIST rozdeľuje operačné módy podľa účelu použitia do nasledujúcich kategórií[1]:

- dôvernosť (celkovo 5 módov: ECB, CBC, OFB, CFB, CTR)
- autentickosť (CMAC)
- autentizované šifrovanie (CCM) a autentizované šifrovanie s vysokou priepustnosťou (GCM)
- dôvernosť pre blokovo-orientované úložiská dát, napr. disky (XTS)
- dôvernosť a integrita kryptografických kľúčov (KW, KWP, TKW)
- formát zachovávajúce šifrovanie (FF1, FF3)

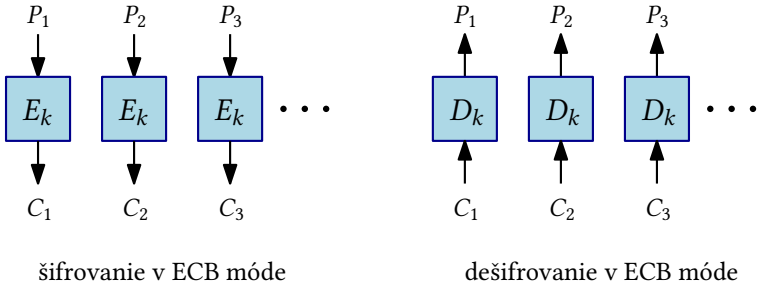
Poznamenajme, že uvedené módy nevyčerpávajú možnosti a rôznorodosť spôsobov použitia blokových šifier.

Pokiaľ ide o operačné módy určené výlučne pre dôvernosť údajov, najčastejšie sa v praxi možno stretnúť s CBC (Cipher Block Chaining) a CTR (Counter). Napríklad AES-128 v CBC móde je povinnou súčasťou v implementáciách TLS 1.2[2] a CTR mód zabezpečuje dôvernosť dát v GCM móde pre autentizované šifrovanie, pričom AES-128 v GCM móde je povinnou súčasťou implementácií TLS 1.3[3].

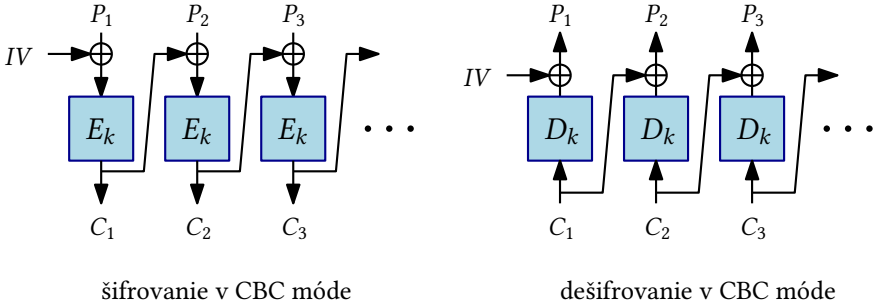
Schematické zobrazenie ECB, CBC a CTR módov je na obrázkoch 11.1, 11.2 a 11.3. Symboly P_1, P_2, P_3 označujú prvé tri bloky vstupných dát a C_1, C_2, C_3 zodpovedajúce bloky zašifrovaných dát. Šifrovací, resp. dešifrovací algoritmus pre jeden blok s využitím kľúča k je označený E_k, resp. D_k. V prípade CBC módu je IV inicializačný vektor a $\oplus$ označuje operáciu XOR dvojice blokov po jednotlivých bitoch (sčítanie modulo 2). CTR mód využíva pri šifrovaní

[1] NIST Special Publication 800-38A, ..., 800-38G (Recommendation for Block Cipher Modes of Operation), resp. https://csrc.nist.gov/Projects/Block-Cipher-Techniques/BCM/Current-Modes (november 2020)
[2] The Transport Layer Security (TLS) Protocol, Version 1.2, RFC 5246, 2008.
[3] The Transport Layer Security (TLS) Protocol, Version 1.3, RFC 8446, 2018.

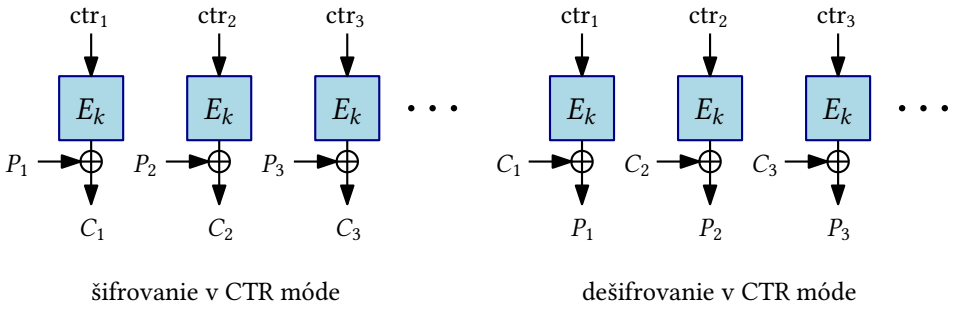
a dešifrovaní počítadlo, inkrementované pre každý nasledujúci blok. Na obrázku 11.3 označuje ctr_i hodnotu počítadla pri šifrovaní bloku P_i.



Obr. 11.1: ECB (Electronic Codebook) mód



Obr. 11.2: CBC (Cipher Block Chaining) mód



Obr. 11.3: CTR (Counter) mód

Z praktického hľadiska je pri implementácii CBC ale aj ECB potrebné doriešiť spôsob šifrovania potenciálne neúplných posledných blokov v prípade, keď dĺžka otvoreného textu nie je násobkom dĺžky bloku. Obvyklé riešenie je použitie vhodnej výplne/zarovnania (tzv. padding). Ďalšou implementačnou otázkou pri CBC je voľba a prenos inicializačného vektora. Ten síce nemusí byť tajný, možno ho posielať spolu so zašifrovaným textom, ale má byť pre útočníka nepredikovateľný.

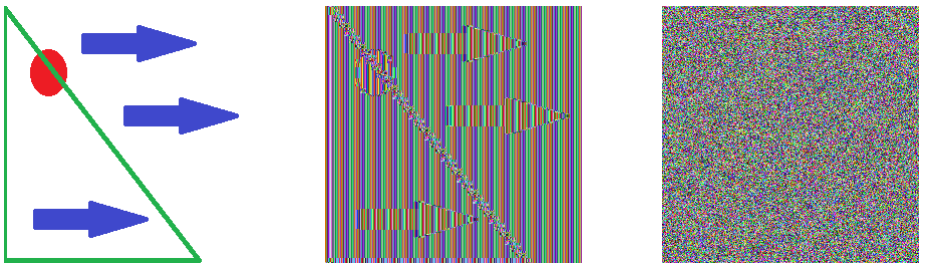
Pri implementácii CTR módu síce nie je potrebné riešiť šifrovanie neúplných posledných blokov (stačí pre XOR použiť len príslušnú časť výstupu z E_k), avšak pozornosť si vyžaduje voľba iniciálnej hodnoty počítadla. Požadujeme, aby sa hodnoty ctr_i neopakovali nielen v rámci

šifrovania jednej správy, ale aj medzi všetkými správami šifrovanými rovnakým kľúčom. Preto sú niekedy bloky ctr_i rozdelené na dve časti – prvá je inicializačný vektor unikátny pre každú správu a druhá samotné počítadlo.

Správne implementovaný CBC alebo CTR mód sú bezpečné spôsoby použitia blokovej šifry pre zabezpečenie dôvernosti dát. Nevhodná implementácia v konkrétnej aplikácii však môže viesť k problémom. Príkladom je tzv. BEAST útok na staršie verzie protokolov SSL/TLS [8]. BEAST útok využíva nevhodný spôsob prenášania inicializačných vektorov v CBC móde medzi samostatnými správami (paketmi) v protokole. Podobne aj ostatné módy vyžadujú starostlivú implementáciu pre dosiahnutie želaných bezpečnostných vlastností. Iným príkladom je nevhodné použitie variantu CFB módu v Netlogon protokole, ktoré viedlo až ku kompromitácii Windows doménových radičov, tzv. Zerologon zraniteľnosť [23].

Nie každý operačný mód blokovej šifry je vhodný na ľubovoľné použitie. Príkladom je použitie ECB módu pri šifrovaní používateľských hesiel spoločnosťou Adobe v roku 2013. Odhliadnime teraz od skutočnosti, že heslá je potrebné ukladať inak (viac v časti 11.5.2). Použitie ECB módu bolo jednou z príčin, že po úniku databázy používateľov aj so zašifrovanými heslami, bolo možné heslá mnohých používateľov určiť. Zhoda dvoch blokov otvoreného textu v ECB móde totiž vedie k zhode príslušných blokov zašifrovaného textu. To znamená, že rovnaké bloky znakov hesiel rôznych používateľov, sú v zašifrovanom tvare ľahko rozpoznateľné. Druhým významným faktorom pre následné určenie hesiel bol uniknutý obsah „nápovied“, ktoré si používatelia zadávali pre prípad zabudnutia hesla.

Obrázok 11.4 vizuálne ilustruje vyššie uvedený fakt o ECB móde. Pri šifrovaní obrázka pomocou AES-256 (v tomto prípade na konkrétnej šifre až tak nezáleží) v ECB móde sú všetky bloky obsahujúce iba bielu zašifrované rovnako (hoci nie nutne na monochromatický blok). Podobne pre „modré“ bloky, atď. To znamená, že zo zašifrovaného obrázka je možné získať aj bez kľúča nejaké informácie o pôvodom obrázku. Na ilustráciu je priložený aj ten istý obrázok šifrovaný v CTR móde.



vstupné dáta | AES-256 v ECB móde | AES-256 v CTR móde

Obr. 11.4: Šifrovanie obrázka v ECB a CTR móde

Autentizované šifrovanie

Autentizované šifrovanie je taký spôsob symetrického šifrovania, ktorý okrem dôvernosti zabezpečuje súčasne aj autentickosť údajov. Tradičný spôsob dosiahnutia oboch požiadaviek je kombinácia šifrovania a autentizačných kódov správ. Existuje viacero spôsobov, ako tieto konštrukcie kombinovať, z ktorých niektoré nie sú (teoreticky) bezpečné alebo vhodné v konkrétnej situácii.

Autentizované šifrovanie spája obe operácie do jednej. Výhodou autentizovaného šifrovania je fakt, že algoritmus je popísaný jednoznačne a nie je potrebné ho ďalej kombinovať ani sa pri implementácii rozhodovať medzi viacerými možnosťami. Niektoré operačné módy blokových šifier sú navrhnuté práve pre autentizované šifrovanie. Najznámejšími módmi tohto typu sú GCM (Galois/Counter Mode) a CCM (Counter with CBC-MAC).

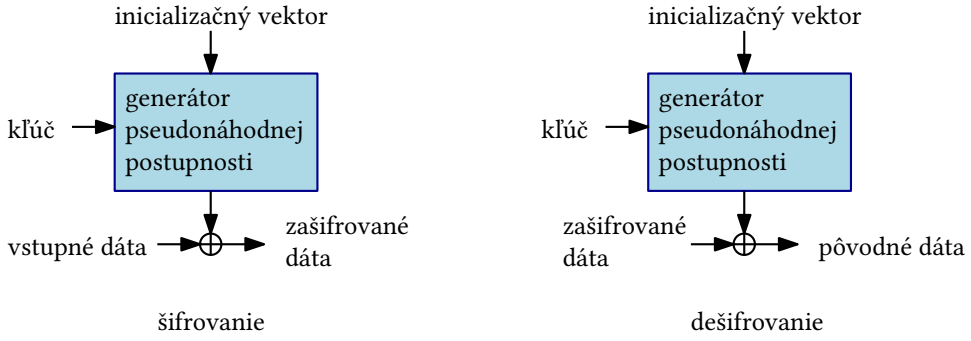
GCM používa na zabezpečenie dôvernosti dát interne CTR mód a na výpočet autentizačného tagu funkciu GHASH. Pri dešifrovaní sa následne overuje aj autentizačný tag a nesúlad medzi prijatým a vypočítaným autentizačným tagom znamená, že zašifrovaný text bol náhodne alebo úmyselne modifikovaný. Výhodou GCM je aj vyššia priepustnosť oproti generickej kombinácii CTR módu so štandardnou konštrukciou autentizačných kódov (ako napr. HMAC). Podobne ako iné módy, aj GCM si vyžaduje starostlivú implementáciu. Jedným zo vstupných parametrov módu je vektor, ktorý musí byť rôzny pre všetky správy šifrované tým istým kľúčom. V opačnom prípade je možné falšovať autentizačné tagy. Tento útok sa nazýva zakázaný útok (forbidden attack), keďže špecifikácia GCM voľbu opakujúcich sa vektorov zakazuje. V prípade TLS komunikácie s AES-GCM bola reálna situácia testovaná v roku 2016 [4], kde boli identifikované zraniteľné servery, pri ktorých dochádzalo k opakovaniu vektorov.

CCM používa na zabezpečenie dôvernosti dát, podobne ako GCM, interne CTR mód a na výpočet autentizačného tagu konštrukciu CBC-MAC. CCM je povinnou súčasťou implementácie štandardu IEEE 802.11i-2004 (WPA2) a je aj súčasťou WPA3 Personal. Poznamenajme, že WPA3 Enterprise pripúšťa v rámci EAP (Extensible Authentication Protocol) výlučne AES v GCM móde.

Niekedy je možné v praxi stretnúť pojem autentizované šifrovanie s asociovanými /dodatočnými dátami (AEAD – authenticated encryption with associated data). Taká konštrukcia pripúšťa dva typy vstupných dát – jeden, pre ktorý zabezpečí dôvernosť aj autentickosť údajov, a druhý, pre ktorý zabezpečí iba autentickosť bez dôvernosti.

11.1.2 Prúdové šifry

Prúdové šifry sú konštruované najčastejšie ako generátor pseudonáhodného prúdu bitov pripočítavaného modulo 2 (teda operácia XOR) k bitom vstupných dát do zašifrovaného textu. Pri dešifrovaní je pripočítaný rovnaký prúd bitov k zašifrovanému textu, pozri obrázok 11.5.



Obr. 11.5: Synchrónna prúdová šifra

Špecializované prúdové šifry majú obvykle jednoduchšiu štruktúru ako blokové šifry a sú vhodné najmä pre hardvérovú implementáciu. Príkladom prúdovej šifry je Snow 3G, ktorý

je základom pre niektoré algoritmy zabezpečujúce dôvernosť a integritu údajov v mobilných LTE sieťach. Prúdová šifra optimalizovaná z pohľadu softvérovej implementácie je ChaCha, ktorá je najmä vo variante ChaCha20 používaná vo viacerých aplikáciách (napr. aj ako jedna z možností v TLS protokole). Atraktivita ChaCha20 spočíva v tom, že pri porovnateľnej úrovni bezpečnosti môže dosahovať vyšší výkon ako AES na platformách, ktoré nemajú k dispozícii hardvérovú akceleráciu pre AES.

Keďže blokové šifry je možné vhodným módom (napr. OFB, CTR alebo CFB) použiť aj ako prúdové šifry, v praxi sú väčšinou používané práve blokové šifry, na ktoré sa zameriavajú aj rôzne štandardizačné aktivity.

11.1.3 Hašovacie funkcie

Od univerzálne použiteľnej hašovacej funkcie požadujeme dve základné bezpečnostné vlastnosti:

1. Odolnosť vzoru: k danému odtlačku nie je efektívne možné vypočítať vstup s takýmto odtlačkom.
2. Odolnosť voči kolíziám: nie je efektívne možné vypočítať dva rôzne vstupy s rovnakým odtlačkom.

Kolízie pre ľubovoľnú hašovaciu funkciu možno hľadať tzv. „narodeninovým“ útokom. Tento útok vytvorí odtlačky veľkého počtu rôznych správ/dokumentov a následne hľadá medzi odtlačkami aspoň jednu dvojicu rovnakých. V prípade, že odtlačok hašovacej funkcie má dĺžku n bitov, tak zložitosť útoku je $\sim 2^{n/2}$. Pripomeňme, že pre ľubovoľnú symetrickú šifru možno hľadať kľúče úplným preberaním v najhoršom prípade so zložitosťou $\sim 2^k$ (kde k je dĺžka kľúča v bitoch). Preto majú štandardizované hašovacie funkcie dĺžky odtlačkov zodpovedajúce dvojnásobku dĺžok kľúčov štandardizovaných symetrických šifier. Typickým príkladom je AES-128, AES-192, AES-256 vs. SHA-256, SHA-384, SHA-512.

V súčasnosti najpoužívanejšie hašovacie funkcie sú tie, ktoré patria do sady hašovacích funkcií SHA-2 [19], resp. SHA-3 [21]:

sada	hašovacie funkcie
SHA-2	SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256
SHA-3	SHA3-224, SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256

Špecifické postavenie majú funkcie SHAKE128 a SHAKE256, ktoré majú voliteľnú dĺžku výstupu. Flexibilita konštrukcie, z ktorej vychádza SHA-3 štandard, umožňuje jej elegantné použitie aj pre výpočet autentizačných kódov správ (funkcia KMAC), paralelizovateľný výpočet odtlačkov dlhých vstupov (ParallelHash) a pod. [20]. Otázne je, či sa niektoré z týchto konštrukcií presadia výrazne v praxi.

Z hľadiska bezpečnosti je dôležité spomenúť, že v súčasnosti nie je potrebná migrácia z SHA-2 na SHA-3.

V rôznych aplikáciách možno stále naraziť na použitie predchádzajúceho štandardu SHA-1. Ide o hašovaciu funkciu s dĺžkou výstupu 160 bitov. Problém s hašovacou funkciou SHA-1 je ten, že je možné prakticky konštruovať kolízie. Prvá kolízia bola publikovaná v roku 2017, v podobe dvoch rôznych PDF dokumentov s rovnakými odtlačkami[4]. Neskôr boli objavené ďalšie vylepšenia útokov na SHA-1 vedúce ku kolíziám s útočníkom zvoleným prefixom [13]. Momentálne by sa hašovacia funkcia SHA-1 nemala používať v akýchkoľvek konštrukciách, ktoré vyžadujú odolnosť voči kolíziám. Jednou z takých konštrukcií sú podpisové schémy, používané napr. pri certifikátoch verejných kľúčov. Všetky hlavné webové prehliadače ukončili podporu SHA-1 v certifikátoch verejných kľúčov v priebehu roku 2017. Nasledujúca tabuľka sumarizuje vývoj podielu certifikátov webových serverov, ktorých podpisová schéma využíva SHA-1 resp. SHA-256[5]:

	01/2015	01/2016	01/2017	01/2018	01/2019
SHA-1	66.7%	13.2%	1.5%	0.0%	0.0%
SHA-256	33.3%	86.8%	98.4%	99.8%	99.8%

Z uvedeného možno konštatovať, že v súčastnosti sa pri podpisovaní certifikátov verejných kľúčov na webe takmer výlučne používa hašovacia funkcia SHA-256.

11.1.4 Autentizačné kódy správ

Najčastejšou konštrukciou autentizačných kódov správ je HMAC, ktorú je možné skonštruovať z ľubovoľnej hašovacej funkcie H takto:

$$\mathrm{HMAC}(k, m) = H((k \oplus \mathrm{opad}) \,||\, H((k \oplus \mathrm{ipad}) \,||\, m)),$$

kde k označuje symetrický kľúč a m správu, ktorej autentizačný kód počítame. Hodnoty ipad a opad sú konštanty, obvykle definované v konkrétnom štandarde. Operácia $\oplus$ označuje XOR a operácia $||$ označuje zreťazenie hodnôt. Napriek dvojitej aplikácii hašovacej funkcie H je výpočet HMAC v podstate (pre dlhšie správy) rovnako rýchly ako výpočet odtlačku správy, keďže vonkajšia aplikácia H sa vykoná už len na krátkom vstupnom reťazci.

Pre bezpečnosť HMAC nie je podstatná odolnosť použitej hašovacej funkcie (s „klasickou“ konštrukciou) voči kolíziám, takže napriek nájdeniu kolízií v SHA-1 je HMAC konštrukcia s touto hašovacou funkciou (momentálne) bezpečná.

Dĺžka výstupu HMAC konštrukcie je rovnaká ako dĺžka výstupu hašovacej funkcie. V praxi sa výstup HMAC niekedy skracuje tak, že sa zoberie len definovaný počet výstupných bitov. Výhodou takéhoto prístupu je menší objem prenášaných dát v situáciách, keď sa autentizačný kód počíta ku každému (potenciálne krátkemu) paketu. Napríklad IPsec umožňuje použiť HMAC-SHA1-96, čo je HMAC počítaný s použitím hašovacej funkcie SHA-1, kde zo 160 bitov dlhého výsledku je na výstup daných prvých 96 bitov. Skracovanie výstupu nemá vplyv na rýchlosť výpočtu HMAC, hoci objektívne znižuje bezpečnostné parametre algoritmu.

[4] https://shattered.io/ (november 2020)
[5] SSL Pulse, https://www.ssllabs.com/ssl-pulse/ (november 2020)

Autentizačné kódy správ je možné konštruovať aj z blokových šifier pomocou špecifických autentizačných módov (napr. CMAC). Taktiež niektoré hašovacie funkcie umožňujú konštruovať MAC jednoduchšie ako HMAC konštrukciou. Napríklad SHA-3 dovoľuje vypočítať MAC ako odtlačok s tým, že kľúč sa pripojí na začiatok správy (KMAC – KECCAK Message Authentication Code). Poznamenajme, že takáto konštrukcia s hašovacou funkciou SHA-1 alebo s ľubovoľnou funkciou zo sady SHA-2 by bola triviálne napadnuteľná[6].

11.2 Asymetrické konštrukcie

Bezpečnosť asymetrických konštrukcií je postavená na matematických problémoch, o ktorých predpokladáme, že nie sú efektívne riešiteľné. V súčasnosti sú najčastejšie používané problémy:

1. Faktorizácia veľkých čísel – pre zadané n, ktoré je súčinom dvoch prvočísel p a q, je úlohou nájsť tieto prvočísla. O zložitosť tohto problému pre dostatočne veľké n sa opiera RSA schéma.

2. Diskrétny logaritmus – pre zadanú hodnotu $g^x \bmod p$[7], kde p je prvočíslo, g je vhodný prvok z $\{2, 3, \ldots, p-2\}$ a x je náhodné, je úlohou vypočítať x. O zložitosť tohto problému pre dostatočne veľké p sa opiera konštrukcia napr. DSA (Digital Signature Algorithm), Diffieho-Hellmanov protokol (pozri časť 11.3) a pod. Problém diskrétneho logaritmu možno sformulovať aj na iných matematických objektoch, nielen v modulárnej aritmetike. Častou, prakticky používanou oblasťou sú eliptické krivky a operácie s bodmi na eliptických krivkách. Algoritmy na výpočet diskrétneho logaritmu na eliptických krivkách majú väčšiu zložitosť ako tie, ktoré problém riešia v modulárnej aritmetike. To znamená, že na dosiahnutie rovnakej bezpečnosti stačí pri eliptických krivkách používať kratšie kľúče (pozri časť 11.5.1).

Shorov algoritmus objavený v roku 1996 umožňuje efektívne počítať faktorizáciu veľkých čísel aj riešiť problém diskrétneho logaritmu na kvantových počítačoch. Pre používané parametre asymetrických schém presahuje veľkosť potrebných kvantových počítačov technické možnosti súčasnosti. Také veľké kvantové počítače jednoducho zatiaľ nemáme k dispozícii. Keďže technický pokrok je ťažké predvídať a prechod na nové algoritmy si vyžiada nejaký čas, NIST sa rozhodol štandardizovať tzv. postkvantové kryptografické algoritmy postupom[8], ktorý bol úspešne použitý pri výbere algoritmov pre štandardy AES a SHA-3. V súčasnosti prebieha analýza, spresňovnie a výber vhodných algoritmov v kategóriách asymetrické šifrovanie (šifrovanie s verejným kľúčom) určené na zapúzdrenie symetrických kryptografických kľúčov (KEM – key encapsulation mechanism) a podpisové schémy. Zavŕšenie výberu sa predbežne očakáva v roku 2022. Matematické problémy používané pri konštrukciách postkvantových schém sú z oblasti mriežok, teórie kódovania a pod.

[6] K správe m a jej autentizačnému kódu by bolo možné dopočítať aj bez kľúča korektný autentizačný kód k ľubovoľnému predĺženiu pôvodnej správy, teda pre akúkoľvek správu $m \,||\, m'$.

[7] Operácia mod p označuje výpočet celočíselného zvyšku po delení p, napr. $17 \bmod 5 = 2$, $2^{11} \bmod 13 = 2048 \bmod 13 = 7$.

[8] https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization (november 2020)

11.2.1 Asymetrické šifrovanie

Asymetrické šifrovanie je najčastejšie používané v hybridných schémach na šifrovanie symetrických kľúčov. Často používanou asymetrickou schémou je RSA (navyše sa najjednoduchšie prezentuje), ktorej „učebnicovú“ verziu uvádzame:

- Inicializácia: zvolíme dve veľké rôzne prvočísla p, q a vypočítame verejný modul $n = p \cdot q$. Následne zvolíme hodnotu e a dopočítame d tak, aby platil vzťah $e \cdot d \equiv 1 \pmod{(p-1)(q-1)}$[9].
- Verejný kľúč je dvojica (e, n). Súkromný kľúč je hodnota d, niekedy nazývaná súkromný exponent.
- Šifrovanie je definované pre m z množiny $\{0, 1, \ldots, n-1\}$ takto: $E(m) = m^e \bmod n$.
- Dešifrovanie zašifrovaných údajov c sa vykoná s pomocou súkromného exponentu nasledovne: $D(c) = c^d \bmod n$.

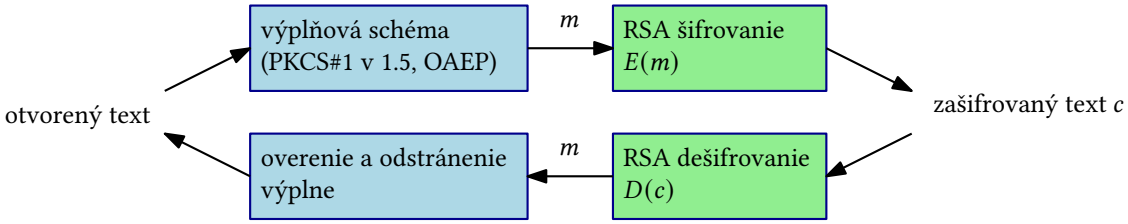
Bez dopadu na bezpečnosť schémy je možné hodnotu e, nazývanú aj verejný exponent, zvoliť ako krátke číslo, čo má priaznivý vplyv na rýchlosť verejnej operácie v RSA. Najčastejšou voľbou býva $e = 65537 = (10000000000000001)_2$, vďaka vhodnej binárnej reprezentácii čísla. Pokiaľ sa hovorí o dĺžke RSA kľúča, napr. 2048 alebo 4096 bitov, myslí sa dĺžka n. Navyše, rovnakú dĺžku má takmer vždy aj súkromný exponent d.

Dôsledkom rozlične dlhých exponentov je podstatne rýchlejšia verejná RSA transformácia ako súkromná transformácia (pozri časť 11.6.1). V praxi sa dešifrovanie urýchľuje alternatívnym výpočtom s využitím matematických vlastností modulárnej aritmetiky. To si vyžaduje pamätať dodatočné hodnoty ako súčasť súkromného kľúča, preto je dátová štruktúra obsahujúca súkromný RSA kľúč obvykle „bohatšia“. Príklad vytvorenia RSA inštancie ako aj jej použitie na asymetrické šifrovanie je uvedený v prílohe.

Priamočiare použitie RSA schémy vyššie popísaným spôsobom sa z bezpečnostných dôvodov neodporúča. Problémy sú napríklad determinizmus schémy, umožňujúci komukoľvek testovať kandidátske otvorené texty, výpočet krátkeho otvoreného textu pre malé e, tzv. „meet in the middle“ útok pre urýchlenie hľadania otvoreného textu oproti úplnému preberaniu a pod. Praktické RSA šifrovanie používa vhodnú výplňovú schému (padding). Obvykle používanými schémami sú staršia PKCS#1 v1.5 a novšia OAEP (Optimal Asymetric Encryption Padding)[10]. OAEP má lepšie bezpečnostné vlastnosti a pri spracovaní otvoreného textu pred samotnou verejnou RSA transformáciou využíva ďalšie kryptografické konštrukcie (hašovaciu funkciu, pseudonáhodný generátor). Samozrejme, pri dešifrovaní je po súkromnej RSA transformácii ešte potrebné na získanie pôvodných dát odstrániť vplyv výplňovej schémy, pričom sa správnosť výplne skontroluje (pozri obrázok 11.6).

[9] Symbol $\equiv$ znamená, že $e \cdot d$ má po celočíselnom delení hodnotou $(p-1)(q-1)$ zvyšok 1.

[10] Obe sú definované napr. v Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.2, RFC 8017, 2016.



Obr. 11.6: Použitie RSA s výplňovou schémou

11.2.2 Podpisové schémy

Podobne ako v prípade asymetrického šifrovania, učebnicová RSA podpisová schéma je jednoduchá. Použijeme rovnaké označenia pre RSA schému ako v predchádzajúcej časti. Podpisovaný dokument označíme m a hašovaciu funkciu H. Podpisovanie odtlačku dokumentu $H(m)$ je realizované s pomocou súkromného kľúča takto: $s = H(m)^d \bmod n$, kde s je výsledný podpis. Keďže ide o súkromnú RSA transformáciu, možno využiť rovnaké urýchľovanie ako pri RSA dešifrovaní. Overenie podpisu s k dokumentu m spočíva v porovnaní hodnôt $H(m)$ a $s^e \bmod n$, pričom používame verejný kľúč tvorcu podpisu. Podpis je korektný, ak sú obe hodnoty rovnaké.

V praxi sa opäť používajú vhodné výplňové schémy. Najznámejšími a najpoužívanejšími výplňovými schémami sú PKCS#1 v1.5 pre podpisy (zdôraznime, že je to iná schéma ako pri šifrovaní) a novšia PSS (Probabilistic Signature Scheme)[11]. RSA-PSS opäť využíva aj ďalšie kryptografické konštrukcie (hašovaciu funkciu, pseudonáhodný generátor). Príklad použitia podpisovej RSA schémy je uvedený v prílohe.

Napriek tomu, že z matematického pohľadu nič nebráni používať rovnakú inštanciu RSA (teda hodnoty e, n, d a ďalšie) v podpisovej schéme aj na účely asymetrického šifrovania, takéto použitie sa neodporúča.

Podpisová schéma RSA (s oboma výplňovými schémami spomínanými vyššie) je spolu s DSA a ECDSA súčasťou štandardu [5]. V súčasnosti sú v praxi používané najmä RSA a ECDSA. Za zmienku stojí fakt, že v návrhu nového štandardu [6] je schéma DSA vypustená a sú doplnené niektoré ďalšie varianty podpisových schém na eliptických krivkách.

Nielen v akademickej sfére pri výskume, ale aj pri štandardizácii kryptografických schém je zreteľný príklon ku konštrukciám, ktorých bezpečnosť je možné matematicky dokázať. Samozrejme, dôkazy majú svoje predpoklady (o zložitosti niektorých problémov alebo o tom, aké vlastnosti majú komponenty použité v analyzovanej konštrukcii, napr. hašovacie funkcie alebo pseudonáhodné generátory) a počítajú s konkrétnym modelom útočníka. To znamená, že aj takéto konštrukcie môžu byť napadnuté, ak sa ukáže nejaký predpoklad nepravdivý, napr. vinou nevhodnej implementácie, alebo útočník postupuje iným spôsobom ako predpokladal model. Na druhej strane konštrukcie s explicitne sformulovanými predpokladmi a dôkazmi vzbudzujú väčšiu dôveru ako ad-hoc konštrukcie, kde takéto dôkazy absentujú. V tejto súvislosti je povšimnutiahodné, že prvý dôkaz bezpečnosti RSA podpisovej schémy s výplňou PKCS#1 v1.5 bol nájdený v roku 2018 [11] (RFC 2313, ktoré pôvodne PKCS#1 v1.5 definovalo, je z roku 1998).

[11] Obe definované v RFC 8017.

11.3 Protokoly na dohodnutie kľúča

Úlohou protokolov na dohodnutie kľúča (niekedy nazývaných aj protokoly na výmenu, prípadne distribúciu kľúča) je ustanoviť medzi komunikujúcimi stranami kryptografické kľúče a iné parametre, ktoré budú následne použité na ochranu prenášaných údajov šifrovaním, výpočtom autentizačných kódov a pod. V praxi majú tieto protokoly obvykle aj cieľ vzájomne autentizovať jedného alebo oboch účastníkov. Kľúče dohodnuté pomocou týchto protokolov sú označované ako kľúče spojenia (session keys), keďže ich platnosť je zvyčajne obmedzená na jedno komunikačné spojenie a pri ďalšom spojení v budúcnosti si účastníci dohodnú nové kľúče spojenia.

Diffieho-Hellmanov protokol (ďalej „DH protokol“) slúži na dohodnutie kľúča a vo svojej pôvodnej podobe je bez autentizácie. Priebeh protokolu pre účastníkov A a B je nasledujúci:

1. $A \to B$: p, g, $g^x \bmod p$,
   kde p je veľké prvočíslo, g je vhodné číslo z množiny $\{2, 3, \ldots, p-2\}$ a x je náhodne zvolené. V prípade, ak sú p a g vopred dohodnuté parametre, nie je potrebné ich prenášať.
2. $B \to A$: $g^y \bmod p$,
   kde y je náhodne zvolené.
3. A vypočíta hodnotu $K = (g^y)^x = g^{xy}$ a B vypočíta rovnakú hodnotu $K = (g^x)^y = g^{xy}$ (v oboch prípadoch rátajúc modulo p), z ktorej následne môžu obaja odvodiť symetrické kľúče pre šifrovanie, pre výpočet autentizačných kódov a pod.

DH protokol je okrem počítania v modulárnej aritmetike možné sformulovať a implementovať aj na eliptických krivkách. Bezpečnosť DH protokolu pri pasívnom útočníkovi, ktorý odpočúva ale nezasahuje do komunikácie medzi A a B, sa opiera o predpoklad, že pre vhodné p a g nie je možné z hodnôt $g^x \bmod p$ a $g^y \bmod p$ efektívne vypočítať hodnotu K. Pokiaľ však uvažujeme o útočníkovi, ktorý môže prenášané správy v protokole meniť, je možné na DH protokol útočiť tzv. MITM „man in the middle“ útokom (útočníka v popise označíme M):

1. $A \to M(B)$: p, g, $g^x \bmod p$
   M zachytí správu určenú pre B
2. $M \to B$: p, g, $g^z \bmod p$
   M pošle B namiesto toho inú správu, kde si z zvolil sám
3. $B \to M(A)$: $g^y \bmod p$
   M zachytí správu určenú pre A
4. $M \to A$: $g^w \bmod p$
   M pošle A namiesto toho inú správu, kde si w zvolil sám
5. A vypočíta hodnotu $K_A = (g^w)^x = g^{xw}$ a B vypočíta hodnotu $K_B = (g^z)^y = g^{yz}$ (v oboch prípadoch modulo p), a teda s vysokou pravdepodobnosťou každý odvodí iné kľúče. Útočník M vie vypočítať obe hodnoty takto: $K_A = (g^x)^w = g^{xw}$ a $K_B = (g^y)^z = g^{yz}$. Následne dokáže M komunikovať s A aj B, v ich vzájomnú komunikáciu môže čítať a prešifrovávať, prípadne aj do nej zasahovať.

DH protokol je základom pre dohodnutie kľúča v mnohých prakticky používaných protokoloch, pričom tieto obvykle používajú varianty DH protokolu tak, aby zamedzili MITM útoku:

- TLS 1.2 (RFC 5246 a nadväzné RFC) je v súčasnosti najpoužívanejšia verzia TLS protokolu[12]. Špecifikácia obsahuje nasledujúce varianty DH protokolu:
  - `DH_anon` – anonymný DH protokol bez autentizácie, zraniteľný na MITM útok. Pri konfigurácii webových služieb je tento variant štandardne zakázaný.
  - `DHE_RSA`, `DHE_DSS` – server generuje parametre p, g, pričom tieto spolu so svoju hodnotu $g^x \bmod p$ (pre náhodné x) podpíše s použitím podpisovej RSA schémy alebo s použitím DSA algoritmu (ten je súčasťou štandardu DSS). Server v takomto prípade má certifikát verejného kľúča, ktorý pošle klientovi a ten následne môže podpis overiť.
  - `DH_RSA`, `DH_DSS` – v tomto prípade sú parametre DH protokolu súčasťou certifikátu servera. Suffixy `_RSA` a `_DSS` sú uvádzané z historických dôvodov, klient môže prípustné podpisové schémy pre certifikát servera signalizovať v rozšírení TLS protokolu. Podotknime, že tieto metódy sú v praxi podporované málokedy.

  Okrem uvedených variantov DH protokolu existujú aj varianty postavené na eliptických krivkách – v takom prípade sú označené prefixom `EC`, napr. `ECDHE_RSA`.

  Ďalšou možnosťou pri dohodnutí kľúča v TLS 1.2 je RSA metóda, kde klient zašifruje náhodne zvolenú hodnotu s použitím verejného RSA kľúča servera (verejný kľúč servera je súčasťou certifikátu). Hlavným nedostatkom je fakt, že tento spôsob nezabezpečuje pre dohodnuté kľúče vlastnosť dopredného utajenia (forward secrecy, niekedy perfect forward secrecy). Diskusia k nej je na konci tejto časti.

- TLS 1.3 (RFC 8446) – oproti TLS 1.2 bol zredukovaný počet metód, akými je možné dohodnúť kľúče spojenia. Vo väčšine bežných situácií bude pri nadväzovaní nového spojenia použitý nejaký variant DH protokolu (v modulárnej aritmetike alebo nad eliptickými krivkami), s podpísaním parametrov serverom.

- IPsec – pre vzájomnú autentizáciu a dohodnutie kľúča sa používa protokol IKE (Internet Key Exchange), v staršej a novšej verzii: IKEv1 a IKEv2. V oboch prípadoch prebieha dohodnutie kľúča pomocou DH protokolu, pričom autentizácia je vykonaná prostredníctvom šifrovania alebo podpisov s využitím verejných kľúčov/certifikátov, autentizačných kódov s využitím spoločného tajomstva (tzv. „preshared secret“) alebo v prípade IKEv2 aj prostredníctvom vhodnej EAP metódy (EAP – Extensible Authentication Protocol).

- SSH 2 (Secure Shell, RFC 4253 a nadväzné RFC) – jednou z metód na dohodnutie kľúča je použitie DH protokolu s tým, že server svoje parametre podpisuje, čím sa zároveň zabezpečuje ich autentickosť.

- WPA3 (Wi-Fi Protected Access) – štandard pre bezpečnosť Wi-Fi publikovaný v roku 2018 obsahuje v rámci WPA3-Personal protokol SAE (Simultaneous Authentication of

[12] Podľa štatistiky SSL Pulse (https://www.ssllabs.com/ssl-pulse/) bol podiel web serverov podporujúcich TLS 1.2 v októbri 2020 99% a podiel web serverov s podporou TLS 1.3 približne 40%.

Equals, variant Dragonfly protokolu), ktorý rieši dohodnutie kľúčov spojenia a vzájomnú autentizáciu komunikujúcich strán. SAE využíva modifikovný DH protokol, s úpravami potrebnými pre zabezpečenie autentickosti komunikácie prostredníctvom spoločného kľúča (hesla) a zároveň ochrany pred offline slovníkovým útokom.

Forward secrecy.

Táto vlastnosť protokolov na dohodnutie kľúča znamená, že súčasné kľúče spojenia nie sú bezprostredne kompromitované ani keď útočník v budúcnosti získa tajné parametre – či už budúce kľúče spojenia alebo súkromné kľúče účastníkov. Samozrejme, forward secrecy nechráni pred nájdením nových útokov na použité kryptografické konštrukcie, napr. symetrické šifry, alebo na riešenie problémov využitých pri konštrukcii protokolu.

Ilustrujme vlastnosť forward secrecy na príkladoch. Nech v protokole účastník A vygeneruje kľúč spojenia a pošle ho zašifrovaný RSA schémou druhému účastníkovi B (s využitím verejného kľúča B). Tento postup nemá forward secrecy vlastnosť. Útočník, ktorý odpočuje zašifrovaný kľúč spojenia, ho dokáže ľahko dešifrovať, ak kedykoľvek v budúcnosti získa súkromný kľúč účastníka B. Na druhej strane v DH protokole je kľúč spojenia odvodený z hodnoty $K = g^{xy}$, pričom x aj y sú v každom behu protokolu volené nanovo a náhodne. To znamená, že hodnoty K v jednotlivých behoch DH protokolu sú navzájom nezávislé a prezradenie niektorej z nich nevedie ku kompromitácii ostatných. Súkromné kľúče, ktoré sú prípadne použité v podpisovej schéme na zabezpečenie autentickosti niektorých správ DH protokolu, nemajú žiadny súvis s dôvernosťou výsledných kľúčov spojenia. Teda ani prezradenie takýchto súkromných kľúčov nevedie ku kompromitácii predchádzajúcich kľúčov spojenia.

11.4 Infraštruktúra verejných kľúčov

Základom pre získanie certifikátu verejného kľúča (ďalej len „certifikát“) je vytvorenie páru kryptografických kľúčov pre asymetrickú schému a súboru s požiadavkou na vydanie certifikátu. Požiadavka je vo formáte CSR (Certificate signing request) a pripája sa k žiadosti o vydanie certifikátu. Súčasťou CSR sú informácie o subjekte a ďalšie aribúty potrebné pre následné využitie certifikátu, napríklad doménové meno pre web server. Certifikačné autority poskytujú vlastné nástroje uľahčujúce konštrukciu CSR, prípadne návody na správne vygenerovanie CSR pre najčastejšie používané serverové platformy. Napríklad v IIS 10 možno použiť IIS Manager, v Exchange 2019 Exchange Admin Center, pre Apache obvykle openssl, pre Tomcat nástroj keytool, atď. CSR okrem verejného kľúča a atribútov, ktoré sa majú ocitnúť v certifikáte, obsahuje aj podpis týchto dát vytvorený s použitím súkromného kľúča. Vďaka tomu je zrejmé, že tvorca CSR pozná súkromný kľúč a atribúty neboli zmenené (identitu subjektu však musí overiť registračná/certifikačná autorita inak). Príklad vytvorenia CSR pomocou openssl je uvedený v prílohe.

Certifikačné autority zverejňujú pravidlá a postupy svojej činnosti v tzv. certifikačnom poriadku (Certification Practice Statement – CPS). Popis vydávania certifikátov, archivácie záznamov, zneplatňovania a obnovy certifikátov, bezpečnostných opatrení a ďalších činností napomáhajú zvyšovať dôveru v certifikačnú autoritu (ďalej CA). Dôvera býva obvykle umocnená nezávislým auditom CA[13].

[13]Napr. zoznam koreňových CA pre Mozilla Firefox (prirodzene, prienik so sadou CA v iných prehliada-

Certifikáty sa líšia aj tým, aké údaje a akým spôsobom CA overuje. Obvykle sa možno stretnúť s nasledujúcimi typmi certifikátov:

- Certifikáty s overením domény (Domain Validation, DV) – CA overí len vlastníctvo doménového mena, pre ktorý má vydať certifikát. Známou CA, ktorá vydáva výlučne certifikáty tohto typu je Let's Encrypt.
- Certifikáty s overením organizácie (Organization Validation, OV) – CA overí doménové meno, názov spoločnosti a prípadne ďalšie náležitosti, aby sa uistila, že certifikát bude obsahovať správne informácie.
- Certifikáty s rozšíreným overením (Extended Validation, EV) – CA dôkladnejšie overuje identitu o spoločnosti, doménových menách a pod. Pri EV certifikátoch sa napríklad overuje aj vlastníctvo ku každému doménovému menu, preto nemôžu byť vydané „hviezdičkové" certifikáty s EV. Príslušné pravidlá pre vydávanie EV certifikátov definuje CA/Browser Forum, dobrovoľná organizácia združujúca certifikačné autority a tvorcov webových prehliadačov[14]. EV certifikáty sa od OV certifikátov formálne líšia špecifickým atribútom v certifikáte (OID 2.23.140.1.1).

Webové prehliadače v stavovom riadku pri URL adrese v minulosti vizuálne odlišovali TLS spojenia, podľa toho, či má server EV alebo iný certifikát. Samozrejme hovoríme o dôveryhodnom certifikáte, overiteľnom prehliadačom až po explicitne dôveryhodnú CA, v opačnom prípade skončí pokus o nadviazanie spojenia chybou. TLS spojenia s EV certifikátom zobrazovali okrem symbolu zámku aj názov organizácie, pre ktorú bol certifikát vydaný. Ukázalo sa, že takéto bezpečnostné indikátory používatelia ignorujú a na ich správanie nemajú reálny vplyv [24]. Vzhľadom na otázny prínos pre bezpečnosť všetky významné webové prehliadače postupne upustili od používania týchto indikátorov.

CRL a OCSP.

Štandardné spôsoby ako overiť, či bol certifikát zneplatnený počas intervalu platnosti sú CRL (Certificate Revocation List) a OCSP (Online Certificate Status Protocol). V ideálnom prípade by pred použitím certifikátu mala byť jeho platnosť okrem ostatných testov overená aj voči CRL alebo pomocou OCSP. Aplikácia potom musí riešiť situáciu, keď tieto mechanizmy nie sú dostupné – pokračovať bez overenia alebo nepokračovať vôbec?

Adresy, na ktorých je možné nájsť CRL alebo službu OCSP sú uvedené v certifikáte. CRL sú pre koncové (klientske) certifikáty vydávané zvyčajne denne – interval je definovaný v certifikačnom poriadku konkrétnej CA. Zoznam sériových čísel zneplatnených certifikátov v CRL obsahuje aj dôvody zneplatnenia. Na zabezpečenie autentickosti je CRL podpísaný certifikačnou autoritou. Pri využívaní CRL je podstatné mať aktuálnu verziu CRL a overiť jeho autentickosť.

OCSP je alternatívny spôsob overenia predčasného zneplatnenia certifikátov. Výhodou oproti CRL je menší objem prenášaných údajov (keďže klient sa pýta na jeden konkrétny cer-

čoch je značný), vrátane odkazov na výsledky príslušných auditov týchto CA možno nájsť na https://ccadb-public.secure.force.com/mozilla/IncludedCACertificateReport (november 2020).

[14] Pravidlá sú k dispozícii na https://cabforum.org/extended-validation (november 2020).

tifikát) a teoreticky čerstvá[15], prakticky takmer čerstvá odpoveď o stave certifikátu. Odpoveď je podpísaná certifikačnou autoritou.

Problematika overovania certifikátov je najmä prehliadaní webu zložitejšia. Niektoré servery implementujú tzv. OCSP stapling, kde pridávajú už pri nadväzovaní spojenia odpoveď z OCSP (ktorú pravidelne aktualizujú), takže klient nemusí realizovať vlastný OCSP. Z hľadiska ochrany súkromia je ďalšou výhodou tohto prístupu to, že CA nie je informovaná, kam klient pristupuje. Prehliadače pristupujú k OCSP a CRL rôzne, napr. Chrome štandardne nevaliduje prostredníctvom CRL a OCSP[16], ale používa vlastný zoznam zneplatnených certifikátov CRLSets. Firefox okrem štandardných mechanizmov udržuje aj samostatný zoznam zneplatnených certifikátov OneCRL, určený najmä pre certifikáty nekoreňových CA.

HPKP a Certificate Transparency.

Používanie infraštruktúry verejných kľúčov v prostredí webu prinieslo viaceré praktické problémy. Kompromitácia CA alebo tzv. registračných autorít, prípadne podvodné konanie pri vydávaní certifikátov umožní útočníkovi nechať si vydať z pohľadu používateľov platné certifikáty pre webové servery. Takéto bezpečnostné problémy sú častokrát detegované s veľkým oneskorením. Server s platným certifikátom, spravovaný útočníkom, je využiteľný na odchytenie prihlasovacích údajov používateľov alebo na odpočúvanie kompletnej komunikácie s cieľovým serverom.

HTTP Public Key Pinning (HPKP, RFC 7469) rieši tento problém pomocou „prišpendlenia“ verejných kľúčov. Základná myšlienka je nasledovná: klient (webový prehliadač) je inštruovaný serverom, aby si na definované obdobie zapamätal odtlačok jedného alebo viacerých verejných kľúčov vyskytujúcich sa v reťazi certifikátov od certifikátu servera až po certifikát koreňovej CA. Počas tohto obdobia klient odmietne pripojenie na tento server, ak by reťaz certifikátov obsahovala verejný kľúč s iným odtlačkom. HPKP ponúka ochranu za predpokladu, že pri prvom prístupe komunikujeme s legitímnym serverom. Praktické nasadenie HPKP je pomerne zložité a musí brať do úvahy potrebu meniť certifikát servera. Nevhodná konfiguračná operácia, napr. prišpendlenie nevhodného certifikátu, môže mať za následok nedostupnosť webového servera pre používateľov. Ďalším problémom je nepriateľské prišpendlenie, keď útočník s podvodne získaným platným certifikátom oznámi klientom ním zvolenú konfiguráciu HPKP. Aj z týchto dôvodov napr. Chrome upustil od HPKP v roku 2018, ostatné prehliadače neskôr tento krok nasledovali.

V súčasnosti je hlavným spôsobom detekcie podvodne alebo chybne vydaných certifikátov Certificate Transparency. Ide o systém verejne prevádzkovaných služieb spravujúcich zoznamy vydaných certifikátov (certificate logs[17]), do ktorých je možné certifikáty len pridávať a nie je ich možné dodatočne meniť. Tieto vlastnosti sú zabezpečená kryptograficky (s využitím tzv. Merkleho hašovacích stromov) a navyše je možné verejne overiť, že server prevádzkujúci takúto službu sa správa v súlade s predpísanými pravidlami. Primárnymi prispievateľmi certifikátov do týchto zoznamov sú certifikačné autority. Používatelia, presnejšie webové prehliadače, môžu pri nadviazaní TLS spojenia požadovať, aby sa serverom prezentovaný certifikát nachádzal v jednom alebo viacerých zoznamoch – presvedčí ich o tom časová pečiatka certifikátu podpísaná

[15] pokiaľ klient aj OCSP server podporujú špecifické rozšírenie protokolu (nonce extension, RFC 6960)

[16] „Online (i.e. OCSP and CRL) checks are not, generally, performed by Chrome.“ https://dev.chromium.org/Home/chromium-security/crlsets (november 2020)

[17] Na stránkach Googlu sú preložené ako „verejné denníky transparentnosti certifikátov“.

prevádzkovateľom služby (Signed Certificate Timestamp, SCT). Tým sú CA a prevádzkovatelia webových serverov tlačení do publikovania certifikátov v zoznamoch. Následne môžu CA, prevádzkovatelia alebo ktokoľvek iný aktívne monitorovať svoje certifikáty a pružnejšie reagovať pri identifikácii podvodných certifikátov. Poznamenajme, že Certificate Transparency je primárne o včasnej identifikácii problematických certifikátov a nenahrádza štandardné mechanizmy pre zneplatňovanie certifikátov. Autorom a hlavným proponentom projektu Certificate Transparency je Google a podporu v súčasnosti možno nájsť vo viacerých prehliadačoch[18].

11.5 Kryptoanalýza a bezpečnosť kryptografických konštrukcií

Každá kryptografická konštrukcia je náchylná na tzv. generické útoky, ktoré nezávisia na podrobnostiach a kvalitách konštrukcie. Typickým príkladom je útok úplným preberaním (niekedy nazývaný aj útok hrubou silou) na symetrické šifrovanie, keď útočník vyskúša postupne všetky potenciálne kľúče. V takom prípade nezáleží na tom, či je použitá šifra AES alebo iná – útok sa dá realizovať vždy. Navyše, čím rýchlejšia šifra, tým rýchlejšie bude aj preberanie kľúčov. Zdôraznime, že generický útok je z hľadiska útočníka najhorší možný. Pri ľubovoľnej slabine kryptografickej konštrukcie, nevhodnej implementácii alebo napríklad pri zlom spôsobe voľby kľúčov môže byť útok efektívnejší. Teda kvalitné kryptografické konštrukcie a ich implementácie sa snažia dosiahnuť, aby bol generický útok zároveň najlepším útokom, ktorý má útočník k dispozícii. Tabuľka 11.1 sumarizuje generické útoky na základné kryptografické konštrukcie a v niektorých prípadoch uvádza aj ich asymptotickú časovú zložitosť.

Konštrukcia	Generický útok (k dĺžka kľúča, n veľkosť odtlačku/výstupu)
Symetrická šifra	Prehľadávanie priestoru všetkých kľúčov $\sim 2^k$
Hašovacia funkcia	Hľadanie kolízií: narodeninový útok $\sim 2^{n/2}$ Hľadanie vzoru: prehľadanie a vyskúšanie vzorov $\sim 2^n$
Autentizačné kódy	Prehľadávanie priestoru všetkých kľúčov $\sim 2^k$, resp. uhádnutie korektného autentizačného kódu k správe $\sim 2^n$.
Asymetrická šifra	Riešenie konkrétneho ťažkého problému (faktorizácia, výpočet diskrétneho logaritmu a pod.)
Podpisová schéma	Riešenie konkrétneho ťažkého problému, resp. útok na hašovaciu funkciu.

Tabuľka 11.1: Generické útoky na základné kryptografické konštrukcie

Kryptológia pri definícii bezpečnosti konštrukcií a ich analýze obvykle uvažuje s čo najsilnejším útočníkom. To znamená, že napríklad (neformálne a zjednodušene):

- Pri šifrovacích schémach očakávame, že útočník sa zo zašifrovaných dát c nedozvie o ich dešifrovanej podobe nič, napriek tomu, že budeme predpokladať schopnosť útočníka nechať si dešifrovať akýkoľvek zašifrovaný text (samozrejme s výnimkou c), resp. nechať si

[18] Podrobnosti o Certificate Transparency možno nájsť na https://www.certificate-transparency.org/ (november 2020).

zašifrovať ľubovoľné vstupné dáta. Prirodzene, pri asymetrických šifrách môže ktokoľvek, nielen útočník, šifrovať ľubovoľné dáta, keďže tam je príslušný kľúč verejný.

- Pri podpisových schémach predpokladáme schopnosť útočníka nechať si podpísať ľubovoľnú, ním zvolenú správu; napriek tomu očakávame, že útočník nedokáže vytvoriť korektný podpis k nejakej správe na ktorej podpis sa nepýtal.

Konštrukcie bezpečné pri veľmi silnom útočníkovi potom zostanú bezpečné aj v prípade scenára so slabším útočníkom.

11.5.1 Ekvivalentné dĺžky kľúčov

Pri používaní viacerých kryptografických konštrukcií je vhodné používať také dĺžky kľúčov, aby zložitosť útoku na každú použitú konštrukciu bola približne rovnaká. Existujú rôzne analýzy a odporučenia popisujúce ekvivalentné dĺžky kľúčov[19] a odporučenia na voľbu dĺžok kľúčov podľa citlivosti chránených údajov alebo potrebnej doby ich ochrany. Uveďme odporúčané dĺžky zo správy projektu ECRYPT CSA [1]. Všetky údaje v tabuľke sú uvedené v bitoch a sú to minimálne, navzájom ekvivalentné dĺžky parametrov.

Bezpečnosť	Symetrický kľúč	Hašovacia funkcia	RSA modul	Eliptická krivka
krátkodobá (aspoň 10 rokov)	128	256	3072	256
dlhodobobá (30–50 rokov)	256	512	15360	512

V praxi je použitá dĺžka kľúčov diktovaná hlavne tým, aké algoritmy a dĺžky kľúčov podporujú štandardné kryptografické knižnice/aplikácie. V prípade certifikátov verejných kľúčov sú dĺžky ovplyvnené tým, aké verejné kľúče je ochotná certifikovať vybraná certifikačná autorita. Predlžovanie kľúčov v certifikátoch zároveň zvyšuje výpočtovú zložitosť operácií a teda nároky na server, ktorý nadväzuje spojenia s veľkým počtom klientov (ilustračné výkonové charakteristiky sú uvedené v časti 11.6.1).

Ak sa pozrieme na 10 najnavštevovanejších web stránok v doméne .sk[20], nájdeme v certifikátoch 8 krát 2048 bitové RSA a 2 krát verejný kľúč pre schémy nad eliptickými krivkami (v oboch prípadoch pre štandardizovanú krivku P-256). Analogický zoznam Top 10 pre USA ukáže 6 krát použitý RSA-2048 a 4 krát verejný kľúč na eliptickej krivke P-256.

11.5.2 Ukladanie hesiel a kľúčov

Heslá sú stále najčastejším spôsobom autentizácie používateľov. Pre zníženie dopadov incidentov ako sú napr. kompromitácia servera, zraniteľnosť aplikácie, získanie zálohy databázy informačného systému útočníkom, nevhodné aktivity „zvedavého“ správcu a pod., nie je vhodné

[19] Prehľad možno nájsť na stránke https://www.keylength.com/ (november 2020).
[20] podľa rebríčka popularity stránok spoločnosti Alexa k novembru 2020 (https://www.alexa.com/topsites)

používateľské heslá v aplikácii/systéme ukladať v otvorenom tvare. V opačnom prípade potom uvedené hrozby môžu viesť k získaniu celého zoznamu používateľských hesiel. Myšlienka bezpečného ukladania hesiel spočíva v použití vhodnej transformačnej funkcie na spracovanie hesla, označme ju T, pričom následne uložíme v aplikácii jej výsledok $T(\text{heslo})$. Často sa používa terminológia, že heslo sa „hašuje“ a $T(\text{heslo})$ je odtlačok hesla. Pri autentizácii sa používateľom zadané heslo transformuje danou funkciou a výsledok sa porovná s uloženou hodnotou. V prípade zhody je autentizácia používateľa úspešná.

Požadujeme, aby T mala vlastnosť odolnosti vzoru[21], v opačnom prípade by bolo možné z uniknutého zoznamu rekonštruovať pôvodné heslá alebo ich ekvivalentné náhrady. Na ukladanie hesiel sa zvyknú používať špeciálne navrhnuté funkcie ako napr. PBKFD2 (táto funkcia je pôvodne navrhnutá na odvodenie symetrických kryptografických kľúčov z hesla), bcrypt, scrypt alebo Argon2. Nezriedka sa možno stretnúť aj s viacnásobne iterovanými hašovacími funkciami – typickým príkladom sú súčasné distribúcie Linuxu. Dôležité bezpečnostné parametre funkcií pre ukladanie hesiel sú:

- Počítadlo iterácií – slúži na jednoduché riadenie rýchlosti transformačnej funkcie T. Tá je iteratívna a nastavením počítadla je možné výpočet spomaľovať na želanú úroveň. Ukladanie hesiel je jedným z príkladov, keď je vysoký výkon kryptografickej konštrukcie prekážkou bezpečnosti. Pokiaľ totiž útočník získa hodnotu $T(\text{heslo})$, dokáže testovať potenciálne heslá opakovaným výpočtom funkcie T pre rôzne heslá a následným porovnaním výsledku s $T(\text{heslo})$. Samozrejme, zvyšovanie počítadla spomaľuje aj bežné overovanie hesla v aplikácii. Avšak kým povedzme 1000 násobné spomalenie z 0,5 ms na 0,5 sekundy je pre používateľa pri prihlásení určite akceptovateľné, spomalenie útoku preberaním hesiel napríklad z 1 mesiaca na 1000 mesiacov (83,3 roka) robí tento útok nerealistickým.

- Soľ – zvyčajne náhodný reťazec pridávaný pri spracovaní hesla. Soľ je volená pre každého používateľa zvlášť a zabezpečuje, že rovnaké heslá sa pre rôznych používateľov transformujú do rôznych výsledkov. V opačnom prípade, teda bez soli, útočník dokáže testovať heslá paralelne pre všetky získané hodnoty $T = \{T(\text{heslo}_1), \ldots, T(\text{heslo}_r)\}$. Alternatívne dokáže útočník predvypočítať hodnoty často používaných hesiel a po získaní množiny T paralelne vyhľadávať zhodu. Použitie soli tieto útoky redukuje opäť na útoky na individuálne heslá, navyše bez možnosti predvýpočtu.

Hľadanie hesla zo získanej hodnoty $T(\text{heslo})$ skúšaním rôznych hesiel je úloha, ktorá sa ľahko rieši paralelne. V ostatnom období sa na takúto úlohu používajú grafické karty, disponujúce tisíckami jadier na jednej karte[22]. Tabuľka 11.2 ilustruje rýchlosť preskúšania všetkých hesiel z danej množiny pri orientačnej rýchlosti GPU Nvidia RTX 2080 Ti a rôznych transformačných funkciách. V tabuľke označuje [a-z] množinu 26 malých písmen bez diakritiky a [a-9] množinu malých písmen, veľkých písmen a cifier (dokopy 62 znakov).

Na sťaženie použitia grafických kariet, prípadne programovateľných hradlových polí (FPGA – Field-programmable gate array) alebo špecifických zákaznických integrovaných obvodov (ASIC – Application-specific integrated circuit) sú navrhované transformačné funkcie, ktoré

[21] Pripomeňme: z výstupu y nie je možné efektívne vypočítať x také, že $T(x) = y$.
[22] napr. Nvidia RTX 2080 Ti má 4352 jadier

	Funkcia			
	SHA-1 (1 iterácia)	SHA-512 (5000 iterácií)	NTLM	bcrypt (32 iterácií)
Rýchlosť	16000 MH/s	220 kH/s	76000 MH/s	28000 H/s
Zloženie hesla				
[a-z] dĺžka 8	13 sekúnd	11 dní	3 sekundy	86 dní
[a-9] dĺžka 8	3,8 hodiny	31 rokov	48 minút	247 rokov
[a-9] dĺžka 10	607 dní	121000 rokov	127 dní	950000 rokov

Tabuľka 11.2: Ilustrácia rýchlosti prebratia hesiel pre rôzne transformačné funkcie

vyžadujú pri výpočte použitie dostatočne veľkej pamäte. Príkladom funkcií s parametrizovateľným využitím pamäte sú scrypt a Argon2.

Na záver pripomeňme, že ľubovoľný spôsob uloženia nezvýši odolnosť slabých hesiel. Databázy uniknutých hesiel umožňujú modelovať voľbu najčastejších používateľských hesiel nielen z hľadiska slovníkov hesiel ale aj z hľadiska používania rôznych „modifikácií“, zreťazovania slov, prefixov, sufixov a pod. Prax ukazuje, že väčšina používateľov volí heslá, ktorých nájdenie z uniknutej hodnoty $T(\text{heslo})$ je otázkou niekoľkých hodín – s technickým vybavením dostupným individuálnemu útočníkovi.

Ukladanie kľúčov

Bezpečnosť kryptografických konštrukcií podstatne závisí na uložení a používaní kľúčov. Jednou z možností je použitie tzv. hardvérových bezpečnostných modulov (Hardware Security Module), ktoré zároveň vykonávajú kryptografické operácie bez toho, aby súkromné alebo symetrické kľúče opustili modul v otvorenom tvare. Inak sú kľúče zvyčajne uložené v súbore, pričom jedným zo štandardných formátov je PKCS#12 (RFC 7292). Tento formát umožňuje ukladanie používateľských súkromných kľúčov, certifikátov, symetrických kľúčov a pod., pričom podporuje rôzne kombinácie módov pre dosiahnutie súkromia a integrity:

- Mód pre súkromie – použité šifrovanie prostredníctvom asymetrickej schémy, resp. použitím symetrického algoritmu s kľúčom odvodeným z hesla.
- Mód pre integritu – použitý autentizačný kód prostredníctvom HMAC s kľúčom odvodeným z hesla, resp. digitálny podpis prostredníctvom asymetrickej schémy.

Obvyklá kombinácia využíva symetrické mechanizmy odvádzajúce kľúče z používateľského hesla. Poznamenajme, že aj v týchto prípadoch sú pri odvodení kľúčov využívané soľ a počítadlo iterácií.

11.5.3 Implementačné a prevádzkové slabiny

Príčinou väčšiny útokov na kryptografické konštrukcie sú slabiny v správe kľúčov a slabiny v implementácii. V prípade protokolov je zvyčajne problém v samotnom protokole, teda v štruktúre a postupnosti prenášaných správ, bez ohľadu na kryptografickú kvalitu použitých algoritmov.

Bezpečná implementácia kryptografických konštrukcií nie je triviálna úloha. Vo všeobecnosti stačí jedna implementačná chyba (nedostatok) na narušenie bezpečnostných požiadaviek, kompromitáciu údajov alebo kľúčov. Situácia je komplikovaná tým, že niektoré implementačné nedostatky neovplyvňujú funkčnosť, teda nie sú „vidieť“ a používateľ ich nevníma. Uvedieme niekoľko príkladov.

Útoky postrannými kanálmi (side-channel attacks).

Útoky tohto typu využívajú informácie získané z prostredia ovplyvneného kryptografickou operáciou na získanie kľúča alebo chránených údajov. Napríklad tzv. „timing“ útok využíva situáciu, keď čas výpočtu závisí na hodnote kľúča a spracúvaných údajoch. Ak použijeme štandardnú implementáciu RSA[23], tak štatistickým spracovaním väčšieho množstva vzoriek typu ⟨zašifrovaný text, čas dešifrovania⟩ možno získať súkromný RSA kľúč. Iné typy postranných kanálov môžu využívať elektrický príkon, elektromagnetické vyžarovanie, prístupy do vyrovnávacej pamäte (cache) a pod. Jednoduchší príklad postranného kanála je zvuk. Existujú experimenty, ktoré rekonštruujú text (heslo) na základe zvuku vydávaného stlačením jednotlivých kláves na klávesnici (napr. [9]), PIN kódy zadávané na platobných termináloch (napr. [18]), text písaný na virtuálnej klávesnici mobilného telefónu alebo tabletu (napr. [22]) a mnohé ďalšie. Iným príkladom sú útoky využívajúce vlastnosti pamätí DRAM, kde sa v istých prípadoch ovplyvňujú susedné pamäťové bunky (zraniteľnosť Rowhammer). Využitie tejto zraniteľnosti na získanie citlivých dát bolo demonštrované na získaní súkromného RSA kľúča v OpenSSH a bolo publikované pod názvom RAMBleed [12].

Zraniteľnosti spôsobené nesplnením predpokladov.

Bezpečnosť kryptografických konštrukcií závisí na predpokladoch. Typickým predpokladom je napríklad náhodnosť niektorých parametrov v konštrukciách, počnúc generovaním samotných kľúčov, pokračujúc inicializačnými vektormi, parametrami výplňových schém a pod. Výskum v roku 2012 zistil, že 0,5% verejných RSA kľúčov v TLS certifikátoch na webe je možné ľahko faktorizovať a získať súkromný kľúč vďaka tomu, že mali spoločný faktor s iným verejným kľúčom [10] – išlo zväčša o „embedded“ zariadenia s nedostatočne inicializovaným generátorom náhodných čísel. Ďalším príkladom, ktorý sa dotkol aj občianskych preukazov s elektronickým čipom (eID) používaných v SR, je zraniteľnosť ROCA [15]. Nevhodná implementácia generovania prvočísel pre RSA schému viedla k možnosti vypočítať súkromný kľúč z verejného kľúča.

Slabiny v kryptografických protokoloch.

Minulosť aj súčasnosť je dokladom toho, že bezpečné kryptografické protokoly je ťažké navrhnúť aj implementovať. Ilustratívnym príkladom je najpoužívanejší kryptografický protokol súčasnosti na webe: SSL/TLS. Od úvodnej verzie SSL v roku 1994 prešiel protokolu viacerými iteráciami a verziami, ktoré odstraňovali aj bezpečnostné slabiny. Prehľad niektorých slabín do roku 2013 možno nájsť v práci [14]. Útok s názvom ROBOT, umožňujúci vykonávať dešifrovanie alebo podpisovanie so súkromným kľúčom servera [3], je ukážkou toho, ako sa dá v niektorých implementáciách TLS zneužiť 19 rokov známa zraniteľnosť (len využitá trocha iným spôsobom). Ani novšie protokoly na dohodnutie kľúča nie sú imúnne voči slabinám. Napríklad

[23] teda bez ochrany pred timing útokom

Dragonblood útok na WPA3 [26] umožňujúci off-line slovníkový útok na heslo, KNOB útok na Bluetooth BR/EDR vedúci k dohodnutiu kľúča s entropiou 1 bajt [2], alebo Selfie útok na vzájomnú autentizáciu klienta a servera na základe spoločného tajomstva v TLS 1.3 [7].

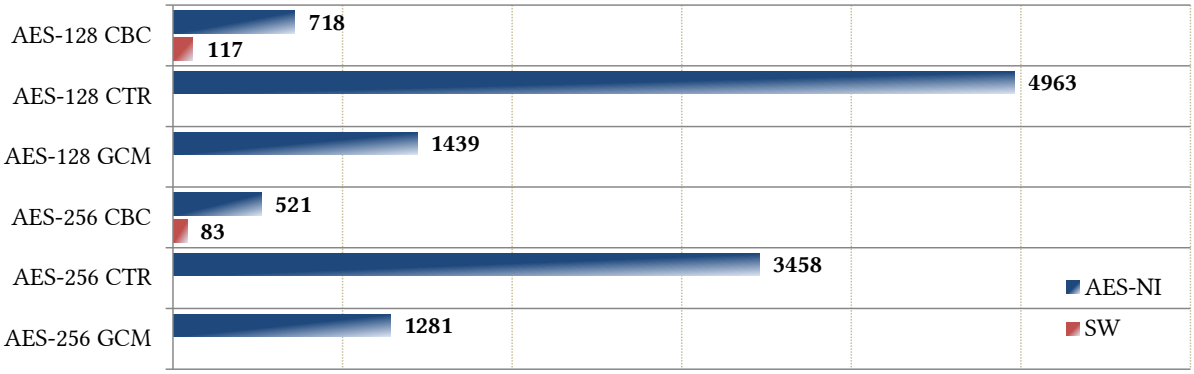
Napriek uvedeným príkladom, podobne ako pri iných kryptografických konštrukciách, je vhodné používať štandardné protokoly s pravidelne udržiavanou implementáciou. Návrh vlastného kryptografického protokolu a jeho implementácia dopadne s vysokou pravdepodobnosťou z bezpečnostného hľadiska zle.

11.6 Použitie kryptografických konštrukcií

11.6.1 Výkonové porovnanie

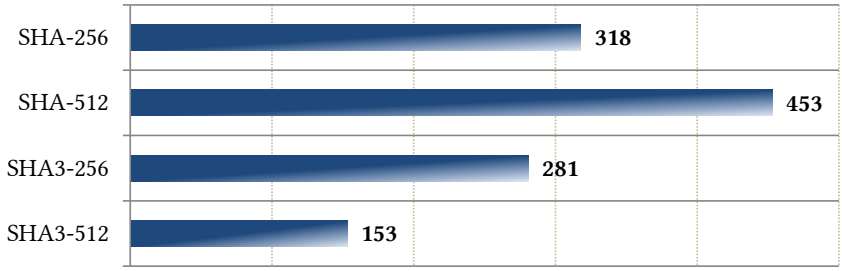
V tejto časti uvedieme výkonové porovnanie vybraných kryptografických algoritmov. Konkrétny výkon sa môže dramaticky líšiť pri rôznych platformách a implementáciách algoritmov. Častokrát sa výkon líši aj v závislosti od verzie použitých knižníc, prípadne volieb pri ich kompilácii. Preto uvedené hodnoty skôr ilustrujú relatívne výkonové rozdiely medzi jednotlivými algoritmami. Hodnoty boli získané v nasledujúcom prostredí: procesor i7-2600 (3,40 GHz), implementácia OpenSSL.

Obrázky 11.7 a 11.8 zobrazujú výkonové charakteristiky pre šifrovanie a hašovanie. V oboch prípadoch sa spracúvali bloky dĺžky 8KB blokov, pričom kryptografické operácie vykonávalo jedno aplikačné vlákno (thread). Obrázok 11.7 ukazuje výrazný rozdiel medzi softvérovou implementáciou a využitím hardvérovej podpory pre AES (ilustrované na CBC móde). Zároveň je vidieť rozdiel medzi jednotlivými módmi a medzi šifrovaním s rôznou dĺžkou kľúča (teda s rôznym počtom kôl).

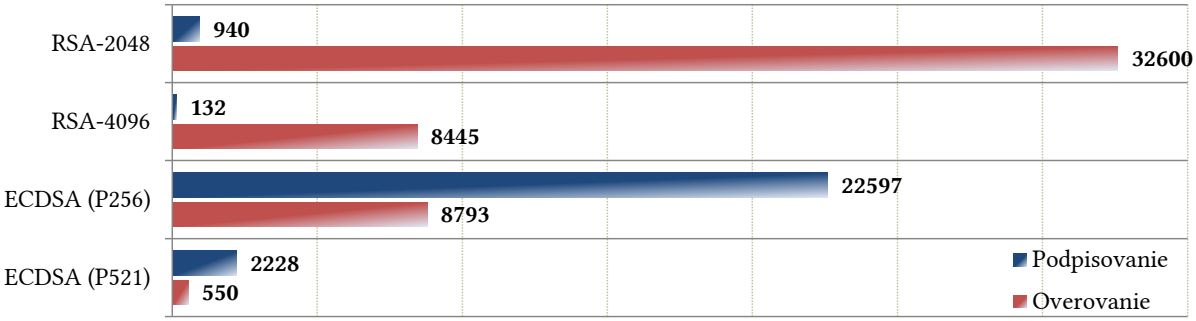


Obr. 11.7: Rýchlosť šifrovania 8KB blokov [MB/s]

Graf na obrázku 11.9 porovnáva výkon podpisových schém RSA a ECDSA pri rôznych dĺžkach kľúčov. V prípade ECDSA sú zvolené dve z eliptických kriviek štandardizovaných NIST. V prípade RSA schémy je to zároveň indikácia výkonu šifrovacej a dešifrovacej transformácie schém s rovnako dlhými kľúčmi. Pri interpretácii výsledkov je užitočné uvedomiť si, aké sú ekvivalentné dĺžky kľúčov medzi oboma schémami (pozri časť 11.5).



Obr. 11.8: Rýchlosť hašovania 8KB blokov [MB/s]



Obr. 11.9: Rýchlosť podpisovania a overovania podpisov [počet/s]

11.6.2 S/MIME a OpenPGP

S/MIME (Secure/Multipurpose Internet Mail Extensions) je štandard pre šifrovanie a podpisovanie elektronickej pošty, podporovaný väčšinou mailových klientov (napr. Outlook, Apple Mail, Thuderbird). V prípade webových poštových služieb je zvyčajne potrebné podporu S/MIME riešiť doplnkami prehliadačov. Verejné kľúče používateľov sú distribuované vo forme X.509 certifikátov. Formát správ je definovaný ako CMS (Cryptographic Message Syntax). V S/MIME sa používajú štandardné kryptografické konštrukcie. Prehľad povinne implementovaných konštrukcií v ostatných troch verziách S/MIME a v navrhovanej verzii 4.0 je uvedený v tabuľke 11.3. Podotknime, že implementácie v mailových klientoch zahŕňajú širšiu sadu algoritmov kvôli vzájomnej interoperabilite ako aj spätnej kompatibilite.

Iné riešenie pre zabezpečenie dôvernosti a autentickosti elektronickej pošty je štandard OpenPGP (RFC 4880), s voľne dostupnou implementáciou GnuPG. Hlavný rozdiel oproti S/MIME je jednoduchší spôsob správy a distribúcie kľúčov – bez použitia certifikátov, väzieb na certifikačné autority a pod. Inak poskytuje OpenPGP podobné kryptografické riešenie ako S/MIME, teda kombinuje symetrické a asymetrické šifrovanie s vhodnou podpisovou schémou. Použitie v mailových klientoch vyžaduje obvykle inštaláciu doplnku. OpenPGP formát sa často používa aj pri podpisovaní súborov, napr. pri distribúcii softvérových balíkov.

Elektronická pošta je oblasť, kde sa kryptografické konštrukcie používajú dlhodobo. Práve preto prekvapil v roku 2018 výskum v oblasti zraniteľností implementácií S/MIME a OpenPGP v mailových klientoch a ich rozšíreniach, publikovaný pod názvom EFAIL [17]. Identifikované zraniteľnosti sa týkali 23 z 35 testovaných S/MIME klientov a 10 z 28 testovaných OpenPGP klientov, zároveň však poukázali aj na nedostatky v samotných štandardoch. Bezpečná imple-

Povinné v CMS („MUST“)	3.0 (1999) RFC 2633	3.1 (2004) RFC 3851	3.2 (2010) RFC 5751	4.0 (2019) RFC 8551 *návrh*
Hašovacia funkcia	SHA-1	SHA-1	SHA-256	SHA-256 SHA-512
Podpisová schéma	DSA	RSA DSA	RSA	RSA ECDSA EdDSA
Asymetrické šifrovanie, resp. dohodnutie kľúča	DH	RSA	RSA	RSA ECDH
Symetrické šifrovanie	3DES CBC	3DES CBC	AES-128 CBC	AES-128 GCM AES-256 GCM AES-128 CBC

Tabuľka 11.3: Povinne implementované algoritmy v rôznych verziách S/MIME

mentácia a integrácia kryptografických mechanizmov v aplikáciách nie je jednoduchá úloha.

11.7 Rady na záver

Na záver len dve rady, ktorých naplnenie nie je jednoduché, ale pomôže zvýšiť kryptografickú bezpečnosť IT prostredia.

- ✓ Inšpirujte sa existujúcimi doporučeniami renomovaných inštitúcií a organizácií. Samozrejme, takých doporučení a štandardov existuje veľa, najznámejšie vydáva NIST. Ak si odmyslíme legislatívne a sektorové požiadavky (napr. PCI DSS pre oblasť platobných kariet[24]), zaujímavé môžu byť napríklad aj:
  - v oblasti kryptogafických mechanizmov, vrátane doporučení pre konfiguráciu protokolov TLS, IPsec a SSH, technické usmernenia nemeckého BSI TR-02102[25];
  - v oblasti aplikačnej bezpečnosti, vrátane požiadaviek súvisiacich s kryptografickými opatreniami, OWASP Application Security Verification Standard [16].
- ✓ Sledujte zraniteľnosti aj v tejto oblasti. Hoci zvyčajne je potrebné počkať na záplaty a aktualizácie výrobcov softvéru, v niektorých prípadoch je potrebná konfiguračná zmena používaných kryptografických mechanizmov.

[24] https://www.pcisecuritystandards.org/ (september 2019)
[25] https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/tr02102/tr02102_node.html (november 2020)

11.8 Otázky a úlohy

Riešenie rôznorodých úloh a zamyslenie sa nad vybranými otázkami súvisiacimi s používaním kryptografických techník má pomôcť k lepšiemu pochopeniu a snáď aj prehĺbeniu prebraných tém.

1. Zistite, koľko RSA podpisov pre dĺžku modulu 2048 a 4096 bitov zvládne za sekundu vykonať váš notebook.

2. Overte podpis softvérového balíka stiahnutého z internetu (napr. OpenSSL[26], KeePass[27]). Zmeňte v súbore 1 bajt a skúste podpis opätovne overiť.

3. Zistite, v koľkých certifikačných logoch (denníkoch transparentnosti) sa nachádza certifikát webového servera vašej organizácie, resp. iného servera. Aké certifikáty sú registrované v certifikačných logoch pre vašu doménu? Využite dostupné webové rozhrania[28].

4. Pri konfigurácii IPsec tunela máte možnosť vybrať štruktúru, v ktorej prebehne DH protokol v rámci IKEv2. Na výber máte tieto možnosti: group18 a group19. Zdôvodnite, ktorú zvoliť, ak je vašou prioritou bezpečnosť.

5. Vo vybratej distribúcii Linuxu zistite, aká funkcia je použitá na ukladanie hesiel. Kde je ukladaná soľ a ako viete ovplyvniť počet iterácií?

6. Zamyslite sa, či je pri zmene hesla vhodné vygenerovať aj novú soľ a prečo.

7. DNSSEC je sada rozšírení DNS s cieľom zabezpečiť autentickosť dát (teda klient dokáže overiť, že získané DNS informácie sú autentické). Zistite aká schéma a aký dlhý kľúč je použitý na podpisovanie záznamov v koreňovej (root) zóne.

8. Symetrický 128 bitový kľúč pre šifrovanie súboru bol vygenerovaný deterministickým generátorom, ktorý bol inicializovaný aktuálnym časom (s presnosťou na 1 ms). Útočník vie, v ktorý deň bol súbor zašifrovaný. Koľko kľúčov potrebuje útočník prezrieť a teda akej dĺžke symetrického kľúča zodpovedá skutočný priestor kľúčov?

9. Stiahnite aktuálny CRL vybratej certifikačnej autority. Aká je štruktúra CRL a koľko certifikátov obsahuje? Aký má význam atribút „Next Update“?

10. Používatelia využívajú rôzne služby na internete. Na jednostrannú autentizáciu používateľa a prenos ním zvoleného kľúča spojenia je použitý nasledujúci postup. Pri nadviazaní spojenia pošle používateľ na server služby B nasledujúcu správu: $A, E_B K, \mathrm{sig}_A$, kde A je identita používateľa (certifikát jeho verejného kľúča), $E_B(K)$ je verejným kľúčom služby B zašifrovaný kľúč spojenia K (zvolený používateľom) a sig_A je podpis pre $E_B(K)$, ktorý používateľ vytvorí s pomocou svojho súkromného kľúča. Server po prijatí správy overí platnosť certifikátu, pomocou verejného kľúča používateľa overí podpis sig_A pre $E_B(K)$. Ak je podpis korektný, tak dešifruje kľúč spojenia K. Identifikujte bezpečnostný problém.

[26] https://www.openssl.org/source/ (november 2020)
[27] https://keepass.info/integrity.html (november 2020)
[28] Napr. https://crt.sh/ alebo https://transparencyreport.google.com/https/certificates (november 2020)

Literatúra

[1] *Algorithms, Key Size and Protocols Report (2018)*. ECRYPT – Coordination & Support Action, 2018. URL: https://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf (cit. 08/2019) (citované na strane 299).

[2] D. Antonioli, N. O. Tippenhauer a K. B. Rasmussen. „The KNOB is Broken: Exploiting Low Entropy in the Encryption Key Negotiation Of Bluetooth BR/EDR“. Publik.: *28th USENIX Security Symposium (USENIX Security 19)*. USENIX Association, 2019, s. 1047–1061. URL: https://www.usenix.org/conference/usenixsecurity19/presentation/antonioli (cit. 11/2020) (citované na strane 303).

[3] H. Böck, J. Somorovsky a C. Young. „Return Of Bleichenbacher's Oracle Threat (ROBOT)“. Publik.: *27th USENIX Security Symposium (USENIX Security 18)*. USENIX Association, 2018, s. 817–849. URL: https://www.usenix.org/conference/usenixsecurity18/presentation/bock (cit. 11/2020) (citované na strane 302).

[4] H. Böck, A. Zauner, S. Devlin, J. Somorovsky a P. Jovanovic. „Nonce-Disrespecting Adversaries: Practical Forgery Attacks on GCM in TLS“. Publik.: *10th USENIX Workshop on Offensive Technologies (WOOT 16)*. USENIX Association, 2016. URL: https://www.usenix.org/conference/woot16/workshop-program/presentation/bock (citované na strane 287).

[5] *Digital Signature Standard (DSS)*. FIPS PUB 186-4. National Institute of Standards and Technology, 2013. DOI: 10.6028/NIST.FIPS.186-4 (citované na strane 292).

[6] *Digital Signature Standard (DSS)*. FIPS PUB 186-5 (Draft). National Institute of Standards and Technology, 2019. DOI: 10.6028/NIST.FIPS.186-5-draft (citované na strane 292).

[7] N. Drucker a S. Gueron. *Selfie: reflections on TLS 1.3 with PSK*. Cryptology ePrint Archive, Report 2019/347. 2019. URL: https://eprint.iacr.org/2019/347 (cit. 11/2020) (citované na strane 303).

[8] T. Duong a J. Rizzo. *Here Come The ⊕ Ninjas*. Unpublished manuscript. 2011 (citované na strane 286).

[9] T. Halevi a N. Saxena. „Keyboard acoustic side channel attacks: exploring realistic and security-sensitive scenarios“. Publik.: *International Journal of Information Security* 14.5 (2015), s. 443–456. DOI: 10.1007/s10207-014-0264-7 (citované na strane 302).

[10] N. Heninger, Z. Durumeric, E. Wustrow a J. A. Halderman. „Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices“. Publik.: *Proceedings of the 21st USENIX Security Symposium*. 2012. URL: https://factorable.net/weakkeys12.extended.pdf (cit. 11/2020) (citované na strane 302).

[11] T. Jager, S. A. Kakvi a A. May. „On the Security of the PKCS#1 V1.5 Signature Scheme“. Publik.: *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. CCS '18. ACM, 2018, s. 1195–1208. DOI: 10.1145/3243734.3243798 (citované na strane 292).

[12] A. Kwong, D. Genkin, D. Gruss a Y. Yarom. „RAMBleed: Reading Bits in Memory Without Accessing Them“. Publik.: *41st IEEE Symposium on Security and Privacy (S&P)*. 2020. URL: https://rambleed.com/docs/20190603-rambleed-web.pdf (cit. 11/2020) (citované na strane 302).

[13] G. Leurent a T. Peyrin. „From Collisions to Chosen-Prefix Collisions Application to Full SHA-1“. Publik.: *Advances in Cryptology – EUROCRYPT 2019*. Springer, 2019, s. 527–555 (citované na strane 289).

[14] C. Meyer a J. Schwenk. *Lessons Learned From Previous SSL/TLS Attacks - A Brief Chronology Of Attacks And Weaknesses*. Cryptology ePrint Archive, Report 2013/049. 2013. URL: https://eprint.iacr.org/2013/049 (cit. 11/2020) (citované na strane 302).

[15] M. Nemec, M. Sys, P. Svenda, D. Klinec a V. Matyas. „The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli“. Publik.: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. CCS '17. ACM, 2017, s. 1631–1648. DOI: 10.1145/3133956.3133969 (citované na strane 302).

[16] *OWASP Application Security Verification Standard 4.0.2*. 2020. URL: https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project (cit. 11/2020) (citované na strane 305).

[17] D. Poddebniak, C. Dresen, J. Müller, F. Ising, S. Schinzel, S. Friedberger, J. Somorovsky a J. Schwenk. „Efail: Breaking S/MIME and OpenPGP Email Encryption using Exfiltration Channels“. Publik.: *27th USENIX Security Symposium (USENIX Security 18)*. USENIX Association, 2018, s. 549–566. URL: https://www.usenix.org/conference/usenixsecurity18/presentation/poddebniak (cit. 11/2020) (citované na strane 304).

[18] G. d. S. Faria a H. Y. Kim. „Identification of Pressed Keys by Acoustic Transfer Function“. Publik.: *2015 IEEE International Conference on Systems, Man, and Cybernetics*. 2015, s. 240–245. DOI: 10.1109/SMC.2015.54 (citované na strane 302).

[19] *Secure Hash Standard (SHS)*. FIPS PUB 180-4. National Institute of Standards and Technology, 2015. DOI: 10.6028/NIST.FIPS.180-4 (citované na strane 288).

[20] *SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash, and ParallelHash*. NIST Special Publication 800-185. National Institute of Standards and Technology, 2016. DOI: 10.6028/NIST.SP.800-185 (citované na strane 288).

[21] *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*. FIPS PUB 202. National Institute of Standards and Technology, 2015. DOI: 10.6028/NIST.FIPS.202 (citované na strane 288).

[22] I. Shumailov, L. Simon, J. Yan a R. Anderson. „Hearing your touch: A new acoustic side channel on smartphones“. Publik.: *ArXiv* abs/1903.11137 (2019). URL: https://arxiv.org/abs/1903.11137 (citované na strane 302).

[23] T. Tervoort. *Zerologon: Unauthenticated domain controller compromise by subverting Netlogon cryptography (CVE-2020-1472)*. Whitepaper, Secura Cryptology ePrint Archive, Report 2019/347. 2020. URL: https://www.secura.com/uploads/whitepapers/Zerologon.pdf (cit. 11/2020) (citované na strane 286).

[24] C. Thompson, M. Shelton, E. Stark, M. Walker, E. Schechter a A. P. Felt. „The Web's Identity Crisis: Understanding the Effectiveness of Website Identity Indicators“. Publik.: *28th USENIX Security Symposium (USENIX Security 19)*. USENIX Association, 2019, s. 1715–1732. URL: https://www.usenix.org/conference/usenixsecurity19/presentation/thompson (cit. 11/2020) (citované na strane 296).

[25] *Transitioning the Use of Cryptographic Algorithms and Key Lengths*. NIST Special Publication 800-131A Rev. 2. National Institute of Standards and Technology, 2019. DOI: 10.6028/NIST.SP.800-131Ar2 (citované na strane 284).

[26] M. Vanhoef a E. Ronen. „Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd“. Publik.: *IEEE Symposium on Security & Privacy (SP)*. IEEE, 2020. URL: https://wpa3.mathyvanhoef.com/ (cit. 11/2020) (citované na strane 303).

Príloha: ilustračné príklady

Ilustračné príklady využívajú program OpenSSL vo verzii 1.1.1.

RSA – generovanie inštancie

Generovanie inštancie RSA schémy (nerozlišujeme, či je určená na šifrovanie alebo pre podpisovú schému) s dĺžkou kľúča 2048 bitov:

```
$ openssl genrsa -out myrsa.pem 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....................................................+++++
.........................+++++
e is 65537 (0x010001)
```

Poznamenajme, že v našom príklade je kľúč uložený nešifrovane, hoci openssl umožňuje kľúč aj šifrovať s použitím hesla. V súbore myrsa.pem sú uložené jednotlivé parametre RSA inštancie (samotný súbor obsahuje dáta vo formáte PEM kódované v base64, ktoré sú v nasledujúcom výstupe zobrazené v časti „writing RSA key“). Vo výstupe sú pre skrátenie výstupu vynechané niektoré riadky. K významu jednotlivých hodnôt (pozri aj časť 11.2.1, pričom hodnoty exponent1, exponent2 a coefficient sú použité na urýchľovanie súkromnej RSA transformácie):

modulus	hodnota n
publicExponent	hodnota e
privateExponent	hodnota d
prime1, prime2	prvočísla p, q (bez ujmy na všeobecnosti v tomto poradí)
exponent1, exponent2	hodnoty $d \bmod (p-1)$ a $d \bmod (q-1)$
coefficient	hodnota $q^{-1} \bmod p$

```
$ openssl rsa -in myrsa.pem -text
RSA Private-Key: (2048 bit, 2 primes)
modulus:
    00:d0:71:30:bf:c0:be:64:25:00:9f:d6:3a:e4:e5:
    ... vynechaných 16 riadkov ...
    2c:03
publicExponent: 65537 (0x10001)
privateExponent:
    00:c8:9c:98:01:85:5c:f8:7f:50:69:85:42:eb:77:
    ... vynechaných 16 riadkov ...
    61:a9
prime1:
    00:f9:1e:03:4e:95:95:a4:5a:8e:91:c2:9e:cc:bd:
    ... vynechaných 7 riadkov ...
    26:ac:bb:7f:15:3f:d5:2d:15
prime2:
    00:d6:33:7c:59:43:d5:29:72:03:6f:8d:3b:e8:3a:
    ... vynechaných 7 riadkov ...
```

```
    a2:31:ca:e4:d8:39:a9:aa:b7
exponent1:
    00:be:2b:30:21:14:45:98:a2:5c:85:5e:c9:74:c7:
    ... vynechaných 7 riadkov ...
    7e:33:8c:2a:16:21:95:6d:85
exponent2:
    00:b5:93:71:6e:ae:1c:cd:84:53:bb:45:4b:2a:41:
    ... vynechaných 7 riadkov ...
    9a:d2:80:be:db:38:8e:46:23
coefficient:
    00:d3:4f:f4:76:27:8d:13:56:44:70:55:76:38:7a:
    ... vynechaných 7 riadkov ...
    2b:e5:49:95:1a:91:44:ee:f2
writing RSA key
-----BEGIN RSA PRIVATE KEY-----
MIIEpgIBAAKCAQEA0HEwv8C+ZCUAn9Y65OVOOdSLBeTqZxHWC7rISlJYP4r6Ldbu
UKLpF2XOsCbyqSKnANqInBspAfzswZhdQJ2HKdz8v//KpYJlQOOcfOQvjAEU7YXp
... vynechaných 22 riadkov ...
Yz+O7ZjgC5fFTYge/lrEAnNwUbCX3lnpCEBFsp53haMKK+VJlRqRRO7y
-----END RSA PRIVATE KEY-----
```

Extrakcia verejného kľúča a jeho súčasti:

```
$ openssl rsa -in myrsa.pem -pubout -out myrsa-pub.pem
writing RSA key
$ openssl rsa -pubin -in myrsa-pub.pem -text
RSA Public-Key: (2048 bit)
Modulus:
    00:d0:71:30:bf:c0:be:64:25:00:9f:d6:3a:e4:e5:
    ... vynechaných 16 riadkov ...
    2c:03
Exponent: 65537 (0x10001)
writing RSA key
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0HEwv8C+ZCUAn9Y65OVO
OdSLBeTqZxHWC7rISlJYP4r6LdbuUKLpF2XOsCbyqSKnANqInBspAfzswZhdQJ2H
... vynechané 4 riadky ...
AwIDAQAB
-----END PUBLIC KEY-----
```

RSA – šifrovanie a podpisovanie

Šifrovanie a dešifrovanie krátkeho textu pomocou RSA a výplne PKCS #1 v1.5. Výplňová schéma je explicitne zadaná pri šifrovaní (nie je to nutné, táto schéma je implicitná). Zašifrovaný text je v binárnom súbore cipher.bin. Za povšimnutie stojí fakt, že pri šifrovaní je jedným zo vstupov súbor s verejným kľúčom (myrsa-pub.pem) a pri dešifrovaní súbor so súkromným kľúčom (myrsa.pem).

```
$ echo 'Kryptologia II - pokusny text' | openssl pkeyutl -encrypt
  -pkeyopt rsa_padding_mode:pkcs1 -pubin -inkey myrsa-pub.pem
  -out cipher.bin
$ openssl pkeyutl -decrypt -inkey myrsa.pem -in cipher.bin
Kryptologia II - pokusny text
```

Podpísanie a následné overenie podpisu súboru text.txt pomocou RSA a výplne PKCS #1 v1.5 (implicitná voľba), pričom použijeme hašovaciu funkciu SHA-256. Podpis je uložený v binárnom súbore sig.bin. Pri podpisovaní sa použije súkromný kľúč a pri overovaní verejný kľúč RSA schémy.

```
$ cat text.txt | openssl dgst -sha256 -binary | openssl pkeyutl -sign
  -inkey myrsa.pem -out sig.bin -pkeyopt digest:sha256
$ cat text.txt | openssl dgst -sha256 -binary | openssl pkeyutl -verify
  -sigfile sig.bin -pubin -inkey myrsa-pub.pem -pkeyopt digest:sha256
Signature Verified Successfully
```

CSR a samopodpísaný certifikát

Vygenerovanie novej inštancie RSA schémy s dĺžkou kľúča 2048 bitov. Súkromný a verejný kľúč sú (nešifrované) uložené v súbore myrsa.pem. V súbore mycsr.csr je uložený CSR pre potenciálnu žiadosť o vydanie certifikátu certifikačnou autoritou.

```
$ openssl req -new -newkey rsa:2048 -keyout myrsa.pem -nodes -subj
  "/C=SK/L=Bratislava/O=Testovacia spolocnost/CN=www.test.xx" -out mycsr.csr
Generating a RSA private key
.....................................................+++++
.....................................................+++++
writing new private key to 'myrsa.pem'
-----
```

Pozrime sa na štruktúru informácií v CSR, pričom samotný súbor mycsr.csr obsahuje dáta vo formáte PEM kódované v base64, ktoré sú v nasledujúcom výstupe zobrazené v časti ohraničenej BEGIN/END CERTIFICATE REQUEST.

```
$ openssl req -in mycsr.csr -text
Certificate Request:
  Data:
    Version: 1 (0x0)
      Subject: C = SK, L = Bratislava, O = Testovacia spolocnost,
               CN = www.test.xx
      Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
          RSA Public-Key: (2048 bit)
          Modulus:
```

```
            00:d5:3c:4e:43:ff:96:3b:81:2a:bd:90:b7:9c:4d:
            ... vynechaných 16 riadkov ...
            18:97
          Exponent: 65537 (0x10001)
      Attributes:
        a0:00
  Signature Algorithm: sha256WithRSAEncryption
    83:77:ab:5c:ba:af:4d:85:4a:59:b1:25:40:e6:c7:12:e3:6b:
    ... vynechaných 13 riadkov ...
    16:c2:f2:28
-----BEGIN CERTIFICATE REQUEST-----
MIICnTCCAYUCAQAwWDELMAkGA1UEBhMCU0sxEzARBgNVBAcMCkJyYXRpc2xhdmEx
... vynechaných 13 riadkov ...
KA==
-----END CERTIFICATE REQUEST-----
```

Samopodpísaný certifikát získame (vrátane novej RSA inštancie) napríklad takto, pričom súkromný kľúč je uložený v súbore myrsa2.pem a certifikát v súbore mycer2.cer:

```
$ openssl req -new -newkey rsa:2048 -keyout myrsa2.pem -nodes -subj
  "/C=SK/L=Bratislava/O=Testovacia spolocnost/CN=www.test.xx" -x509
  -days 1000 -out mycer2.cer
```

Overenie certifikátu prostredníctvom OCSP

Overme platnosť certifikátu web servera Európskej komisie pomocou OCSP. Certifikát si uložíme do súboru ec.pem a následne z neho získame url, kam možno posielať OCSP požiadavky:

```
$ openssl s_client -connect ec.europa.eu:443 </dev/null 2>/dev/null |
  openssl x509 -outform PEM >ec.pem
$ openssl x509 -in ec.pem -ocsp_uri -noout
http://ocsp2.globalsign.com/gsorganizationvalsha2g2
```

Získame certifikát CA, ktorá vydala certifikát pre web server, vrátane konverzie z DER do PEM formátu. V tomto prípade je CA „GlobalSign Organization Validation CA - SHA256 - G2“. Výstup je v súbore gs.pem.

```
$ openssl x509 -in ec.pem -text -noout | grep "CA Issuer"
      CA Issuers - URI:http://secure.globalsign.com/cacert/
                   gsorganizationvalsha2g2r1.crt
$ wget -q  http://secure.globalsign.com/cacert/gsorganizationvalsha2g2r1.crt
$ openssl x509 -in gsorganizationvalsha2g2r1.crt -inform DER -out gs.pem
```

Informácie posielané a získané v odpovedi pri overovaní certifikátu ec.pem pomocou OCSP vidieť na nasledujúcom príklade. Sumár bez detailov je v posledných 4 riadkoch výpisu.

```
$ openssl ocsp -nonce -issuer gs.pem -cert ec.pem -url
  http://ocsp2.globalsign.com/gsorganizationvalsha2g2 -text
OCSP Request Data:
    Version: 1 (0x0)
    Requestor List:
        Certificate ID:
          Hash Algorithm: sha1
          Issuer Name Hash: 0C9E4D9C3DEDEF84D891E972C7CF8406BC197B07
          Issuer Key Hash: 96DE61F1BD1C1629531CC0CC7D3B830040E61A7C
          Serial Number: 34D7E3DA71A37D6F9627FA6D
    Request Extensions:
        OCSP Nonce:
            0410BA1B29B27389E35972466F9068E47D94
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: 9C4D0099000E8BB0018175A1BAF0D025D7A01C47
    Produced At: Jan 17 21:28:35 2021 GMT
    Responses:
    Certificate ID:
      Hash Algorithm: sha1
      Issuer Name Hash: 0C9E4D9C3DEDEF84D891E972C7CF8406BC197B07
      Issuer Key Hash: 96DE61F1BD1C1629531CC0CC7D3B830040E61A7C
      Serial Number: 34D7E3DA71A37D6F9627FA6D
    Cert Status: good
    This Update: Jan 17 21:28:35 2021 GMT
    Next Update: Jan 21 21:28:35 2021 GMT

    Response Extensions:
        OCSP Nonce:
            0410BA1B29B27389E35972466F9068E47D94
    Signature Algorithm: sha256WithRSAEncryption
         57:8d:3a:6f:f5:10:cd:9b:1b:20:6f:59:1d:cc:05:33:fb:2f:
         ... vynechaných 13 riadkov ...
         53:ca:72:e2

Certificate:
    ... vynechané riadky popisujúce certifikát OCSP Respondera ...

Response verify OK
ec.pem: good
        This Update: Jan 17 21:28:35 2021 GMT
        Next Update: Jan 21 21:28:35 2021 GMT
```

Kapitola 12

Riadenie kontinuity podnikania, procesov a činností

Lenka Gondová

12.1 Úvod

Cieľom tejto kapitoly je predstaviť základné princípy BCM[1]. Po prečítaní tejto kapitoly by ste mali rozumieť dôležitým pojmom z oblasti BCM, postupu ako dosiahnuť stav, ktorý je pre riadenie kontinuity považovaný za minimálny štandard, a vedieť, čo odporúčajú postupy najlepšej praxe[2].

Pojmy, ktorými sa kapitola zaoberá:

- BCM (Business Continuity Management)
- BIA (Business Impact Analysis)
- RTO (Recovery Time Objective)
- RPO (Recovery Point Objective)
- DRP (Disaster Recovery Plan)
- Riadenie incidentov
- Testovanie plánov obnovy

Koho by to mohlo zaujímať:

Študent/ absolvent pri nástupe do praxe má po prečítaní rozumieť aké podklady, z akých častí spoločnosti potrebuje získať aby naplánoval spracovanie plánu kontinuity, vedel ich skoordinovať aspoň ako projektový koordinátor ak už nie ako technický expert, ktorý rozumie aj

[1] v anglicky písanej literatúre používaná skratka pre Business Continuity Management = BCM, po slovensky riadenie kontinuity podnikania. O tom, že nejde jen o podnikanie, hovoríme ďalej v texte

[2] Porovnáme ISO normy a odporúčania najlepšej praxe vychádzajúce z rizík pre konkrétnu firmu/oblasť podnikania/veľkosť firmy

technickým náležitostiam zachovania prevádzky. Následne zorganizoval testovanie na overenie plánu kontinuity.

Manažér v riadiacej funkcii, ktorá vyžaduje zodpovednosť za kontinuitu spoločnosti by mal po prečítaní vedieť vyhodnotiť a prípadne schváliť stav opatrení a pochopiť potrebu ďalšieho zlepšovania.

Ľudia majú radi kontinuitu

Ľudia nemajú radi, ak na niečom pracujú a náhle sa stane niečo, čo im to prekazí. Znervózňuje ich už samotná predstava, že by k niečomu podobnému mohlo prísť. To platí rovnako pre tých, ktorí vykonávajú konkrétnu činnosť rovnako ako pre tých, ktorí sú na nej závislí - či už vo vnútri organizácie (zamestnanci, vedúci pracovníci) alebo mimo nej (zákazníci, používatelia produktov alebo služieb).

Lenže svet nie je ideálny

Bolo by asi príliš optimistické až naivné očakávať, že sa v živote alebo pri podnikaní v komerčnej firme alebo prevádzke akejkoľvek inštitúcie neprihodí nič nečakané alebo nepredvídateľné.

Média nám denne ukazujú správy o katastrofách veľkého rozsahu, ktoré majú dopady na životy a zdravie ľudí a na prevádzku organizácií.

Klimatické zmeny majú za následok veľké výkyvy počasia. Tornáda na územiach, kde sa doteraz nevyskytovali (napr. Február 2019 západná Európa), požiare zasahujúce veľké územia (Kalifornia, Austrália), záplavy, hurikány, silný mráz sú len príkladmi vplyvov, ktoré majú ničivé následky.

Pri analýze rizík obvykle takéto javy hodnotíme ako málo pravdepodobné a s veľmi vysokým dopadom, avšak ich výskyt je čoraz častejší. Pre všetkých nás môže byť nepredvídateľná udalosť označená ako katastrofa. Pod pojmom havária alebo katastrofa označujeme také udalosti, ktoré majú negatívny vplyv na činnosti organizácie vo veľkom rozsahu.

Nie len počasie môže byť príčinou nežiaducich javov s obrovskými následkami. Teroristické útoky, vojnové konflikty, epidémie infekčných chorôb žiaľ nie sú až takými málo pravdepodobnými ako by sme si asi všetci priali.

Príklad Taiwanu pri reakcii na Korona krízu ukázala rozdiely v pripravenosti krajín na pandémiu

Pandémia COVID-19 ukázala medzery v pandemických plánoch väčšiny krajín. Málokto bol pripravený na priebeh katastrofy v špecifických podmienkach daných vysoko infekčným ochorením, ktorého príznaky sa prejavili často až po tom, čo prenášač nakazil veľké množstvo ďalších ľudí. Príklad Taiwanu je peknou ilustráciou toho, ako šťastie praje pripraveným.

Taiwan sa poučil z epidémie SARSu v rokoch 2003 a v čase, kedy vypukla epidémia COVID-19 v čínskom Wuhane, okamžite aktivoval preventívne plány národnej agentúry pripravené po skúsenostiach so SARSom hneď po publikovaní prvých prípadov na pevninskej Číne, s ktorou má Taiwan intenzívnu obchodnú spoluprácu[3]. Opatrenia vyvolané aktiváciou tohoto

[3] https://edition.cnn.com/2020/04/04/asia/taiwan-coronavirus-response-who-intl-hnk/index.html

plánu mali za následok významne lepšie výsledky v mortalite a pri šírení pandémie oproti krajinám s inou stratégiou. Zároveň tieto opatrenia neochromili ekonomiku, ako tomu bolo v krajinách, ktoré aktivovali svoje národné stratégie neskôr, často až po tom, čo príval chorých ochromil zdravotný systém a zároveň jedinou prevenciu pre komunitné šírenie nákazy bol zákaz vychádzania a vyhlásenie výnimočných stavu. Na vyhodnotenie ekonomických následkov týchto opatrení si ešte musíme počkať, keďže sa očakávajú dopady počas nasledovných mesiacov a rokov. Na priebehu Korona krízy v jednotlivých krajinách ale môžeme už teraz vidieť, že včasnosť a premyslenosť koordinácie opatrení pri vypuknutí epidémie má priamu súvislosť s účinnosťou opatrení a ich dopadom na zdravotné systémy a ekonomiku krajín. Na príklade Talianska, Španielska, USA môžeme vidieť, že podcenenie situácie malo za následky nečakanú mortalitu a ochromenie zdravotných systémov. Na druhej strane nepripravenosť pandemických plánov, absencia ochranných pomôcok, neskoré zabezpečenie testovania obyvateľstva predĺžili v mnohých krajinách potrebu karanténnych opatrení s drastickým dopadom na ekonomiku, ktoré sa ešte bude prejavovať v nasledujúcich obdobiach.

Hackerské útoky ohrozujú nás všetkých novou formou kriminality.

Jednou z najväčších hrozieb vnímaných v súčasnosti[4] pre organizácie aj jednotlivcov je počítačová kriminalita. Pre útoky, ktoré využívajú prepojenie s internetom sa používa aj označenie kybernetické útoky.

Za posledných 10 rokov sa táto hrozba rozvinula do rozmerov, ktoré prinútili štáty prijímať legislatívu adresujúcu ochranu kontinuity kľúčových činností služieb pre svojich občanov (vrátime sa k tomu v kapitole Riadenie kontinuity v legislatíve). Jedným z prvých významnejších dokumentovaných prípadov v tejto oblasti je útok z Číny v roku 2010 na spoločnosť Google, konkrétne jej Gmailové účty, kde cieľom boli emailové účty čínskych aktivistov za ľudské práva[5]. Tento útok dokresľuje situáciu, kedy sa začali kybernetické útoky používať v medzinárodnom meradle a v rozsahu, ktorý dal vznik pojmu označujúcemu pokročilé vytrvalé hrozby – Advanced Persistent Threat skrátene APT.

Na to je tu BCM

Organizácie sa týmto udalostiam snažia zabrániť a pokiaľ sa im to nepodarí, aspoň mať pripravený súbor krokov, ktorými minimalizujú nežiaduce dopady takýchto udalostí. Všetkým týmto opatreniam sa hovorí jednoducho Business Continuity Management skrátene BCM v preklade riadenie kontinuity podnikania. Je dôležité si uvedomiť, že pod pojmom Business v preklade podnikanie sa nechápu len komerčné spoločnosti ale akékoľvek činnosti spravidla v organizáciách. Môže ísť o akúkoľvek organizáciu, nie len komerčnú ale napríklad o nemocnicu, školu, ministerstvo alebo rodinu. Preto synonymom pre BCM je pojem riadenie kontinuity činností.

Pojem *riadenie* vyvoláva predstavu cieľavedomej, systematickej činnosti, ktorú má niekto pod kontrolou. Kontinuita je iste zaujímavá pre zainteresovaných na spoločnosti: znamená istotu dodávok tovarov alebo služieb pre zákazníkov, ktorých dôveru potrebujete na ich udržanie.

Pre zamestnancov je dobré veriť v budúcnosť svojej kariéry a istotu zamestnania. Investori

[4] Prieskum Verizone https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf založený na analýze 41,686 incidentov, z toho 2013 narušení bezpečnosti dát

[5] Responding to Targeted Cyberattacks, ISACA and ITGI, 2013, s.15

veria v návratnosť svojich investícií, načo je potrebné, aby spoločnosť vykonávala svoje kľúčové činnosti aj v budúcnosti. Tieto vzťahy sú postavené na dôvere. Kontinuita podnikania je teda zárukou a zároveň i predpokladom, že dôvera nebude sklamaná.

A ako už je pri zárukách a poistiek zvykom, zainteresované strany, v podnikaní predovšetkým zákazníci, začali od organizácií, hlavne dodávateľov, vyžadovať dôkazy o kontinuite podnikania formou certifikácie[6] .

Realita často zaostáva

Jedna vec je o BCM vedieť, prípadne hovoriť, druhá je vykonávať ho a ešte aj správne. Že to tak v praxi vždy nie je a aké to môže mať následky, si poďme názorne ukázať na príkladoch z praxe.

S čím zápasia spoločnosti pri riadení kontinuity?

Prieskum[7] od Continuity Central poukazuje posledných 5 rokov na najčastejšie problémy pri riadení kontinuity. Respondenti prieskumu[8] uvádzajú najväčšie výzvy pri riadení kontinuity:

- nedostatok zdrojov
- nedostatočnú podporu a apatiu v organizácii
- nedostatočnú podporu od vrcholového vedenia organizácie
- veľké zmeny v organizácii
- iné priority než je riadenie kontinuity

Pri riadení kontinuity je podstatná rýchlosť reakcie na incident

Každá katastrofa môže začať ako bežný incident. Včasná reakcia na incident a zabránenie rozšírenia jeho následkov do rozsahu katastrofy môže byť rozhodujúca pre organizáciu. Pri dobrej reakcii na incident sa môže vyriešiť situácia v zárodku, kým ešte kaskáda následkov neprerastie do veľkých rozmerov. Preto je podstatné, ako dobre je implementované riadenie incidentov.

V ďalšej časti sa preto pozrieme na to, čo to je incident, ako môže vyzerať v praxi riadenie incidentov, čiže detekcia, reakcia na incidenty, ich riešenie a následná spätná väzba pri zlepšovaní riadenia incidentov.

Čo to je incident

Pojmom *incident* označujeme udalosť alebo situáciu, ktorá spôsobí alebo môže spôsobiť nezžiaduúce prerušenie činnosti, stratu, núdzový stav alebo krízu v nejakej organizácii, alebo v systéme[9].

[6] ISO/IEC 22301:2019 Systémy manažérstva kontinuity podnikania. Požiadavky

[7] https://www.continuitycentral.com/index.php/news/business-continuity-news/3643-business-continuity-trends-and-challenges-2019-survey-results

[8] Prieskumu sa zúčastnilo 134 spoločností, prevažne z firiem nad 250 zamestnancov

[9] D. Olejár a kol. Výkladový slovník pojmov informačnej bezpečnosti

Typický životný cyklus riadenia incidentu od jeho vzniku až po činnosti po jeho uzavretí vysvetľujú svetovo uznávané štandardy ISO[10] a NIST[11].

Aký je teda rozdiel medzi incidentom a haváriou?

Každá havária spočiatku znamená incident. Rozdiel medzi incidentom a haváriou je spravidla v rozsahu, avšak rozlíšenie medzi tým, kedy ešte v organizácii platí bežná prevádzka, počas ktorej sa rieši nejaký incident a kedy už je potrebné aplikovať naplánovaný stav riešenia krízy alebo havárie, môže byť kľúčové pre neskoršie následky a priebeh riešenia obnovy po havárii.

Riadenie kontinuity v legislatíve

Povedali sme, že riadenie kontinuity stojí zdroje. Možno sa nájdu organizácie, ktoré si povedia, že im to za to nestojí. To je samozrejme jedna z možností. Už dávno povedal slávny zakladateľ riadenia kvality Edward W. Deming[12], že „prežitie nie je povinné“. Nuž a podobne je to aj s riadením kontinuity. Avšak v niektorých prípadoch organizáciám štát túto voľbu neumožňuje (teda pri dodržiavaní zákonov, čo je opäť voľba každej organizácie): postupne pribúdajú zákony, kde riadenie kontinuity zákon priamo predpisuje.

Napr. pre podniky, ktoré tvoria tzv. kritickú infraštruktúru štátu[13], povinnosti pre všetky organizácie spracúvajúce osobné údaje priamo nariadenie EÚ GDPR[14] vyžaduje zabezpečiť, že ani v prípade nepredvídateľných udalostí nebudú mať osobné údaje horšiu ochranu než počas bežnej prevádzky.

Jednou z najnovších a zároveň najzásadnejších zákonných úprav súvisiacich s povinnými bezpečnostnými opatreniam, ktoré zahŕňajú aj riadenie kontinuity je európska smernica o ochrane informačných systémov a sietí[15], ktorú slovenská legislatíva implementovala zákonom o kybernetickej bezpečnosti č. 69/2019 Z.z. a súvisiacimi vyhláškami [16], predovšetkým vyhláškou o bezpečnostných opatreniach.

Čo zahŕňa oblasť riadenia kontinuity podnikania pre riadenie sietí a informačných systémov voči kybernetickým hrozbám[17]

„Riadenie kontinuity pozostáva najmenej z

a) vypracovania stratégie a krízových plánov na zabezpečenie dostupnosti siete a informačného systému po narušení alebo zlyhaní v dôsledku kybernetického bezpečnostného inci-

[10] Napr. Annex časť 16 normy ISO 27001:2013, ISO 22320:2018 Security and resilience - Emergency management - Guidelines for incident management, ISO 22313:2020 Security and resilience - Business continuity management systems - Guidance on the use of ISO 22301

[11] NIST 800-61 Computer Security Incident Handling Guide, Recommendations of the National Institute of Standards and Technology http://dx.doi.org/10.6028/NIST.SP.800-61r2

[12] https://www.brainyquote.com/quotes/w_edwards_deming_377112

[13] https://www.zakonypreludi.sk/zz/2011-45#p9 Zákon č.45/2011 Z.z. § 9 určuje povinnosť spracovať bezpečnostný plán pre prvky kritickej infraštruktúry a precvičiť podľa bezpečnostného plánu aspoň raz za tri roky modelovú situáciu hrozby narušenia alebo zničenia prvku

[14] Vložím odkaz na zákon a presne čo chce

[15] EU 1148/2016 SMERNICA EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii

[16] vymenovať vyhlášky, každú ešte rozoberieme neskôr

[17] Vyhláška NBÚ č.362/2018 Z.z. ktorou sa ustanovuje obsah bezpečnostných opatrení podľa § 20 ods. 3 písm. m) zákona o kybernetickej bezpečnosti č.69/2018 Z.z.

dentu na základe vykonania analýzy dopadov kybernetického bezpečnostného incidentu na základnú službu,

1. b) vyčlenenia adekvátnych finančných, materiálno-technických a personálnych zdrojov na zabezpečenie riadenia kontinuity činností,
2. c) určenia komunikačného plánu na plnenie havarijných plánov a plánov obnovy spolu s kontaktnými údajmi, určeniami rolí a zodpovednosti na plnenie havarijných plánov a plánov obnovy po kybernetickom bezpečnostnom incidente,
3. d) určenia cieľovej doby obnovy jednotlivých procesov, siete a informačných systémov a aplikácií, a to najmä určením doby obnovy prevádzky, po uplynutí ktorej je po kybernetickom bezpečnostnom incidente obnovená najnižšia úroveň poskytovania základných služieb,
4. e) určenia cieľového bodu obnovy jednotlivých procesov, siete a informačných systémov základnej služby a aplikácií, a to najmä určením najnižšej úrovne poskytovania služieb, ktorá je dostatočná na používanie, prevádzku a správu siete a informačného systému a zachovanie kontinuity základnej služby,
5. f) testovania a vyhodnocovania jednotlivých procesov riadenia kontinuity činností a realizácie opatrení na zvýšenie odolnosti sietí a informačných systémov základnej služby,
6. g) určenia plánov havarijnej obnovy a postupov zálohovania na obnovu siete a informačného systému po jeho narušení alebo zlyhaní v dôsledku kybernetického bezpečnostného incidentu.

“

Poďme si hlbšie rozobrať, z čoho sa teda riadenie kontinuity skladá

Je pravdepodobne jasné, že pokiaľ nastane nežiadúca situácia, ktorá má negatívny vplyv na činnosť organizácie, vtedy je už neskoro začať rozmýšľať, čo robiť. Ideálne je, ak sme si dopredu pripravili nejaké možnosti reakcie, čiže plánovali stratégiu pre prípad havárií.

Aby bolo BCM úspešné, musia byť zmysluplne pripravené a realizované všetky etapy, ktoré sa pri riadenom priebehu havárie môžu vyskytnúť vrátane:

- identifikácie rizík,
- prevencie výskytu havárie formou implementácie preventívnych bezpečnostných opatrení
- detekcie, že nastala nežiaduca udalosť implementáciou opatrení pre detekciu, vyhodnotenie udalostí a eskalačných mechanizmov pri riadení incidentov
- vyhlásenia, že došlo k havárii
- reakcie na haváriu v súlade s plánom
- obnovy kritických procesov a ich podporných systémov
- návrat do pôvodného stavu

Z pohľadu systematickej prípravy v súlade s ISO normami rozpoznávame činnosti v rámci tzv. PDCA (Plan - Do - Check - Act) cyklu, čo v prípade noriem na riadenie kontinuity pozostáva z nasledovných etáp.

12.2 Etapy riadenie kontinuity v praxi

Riadenie kontinuity je proces, ktorý sa v organizáciách, ktoré k téme pristupujú systematicky, vo všeobecnosti skladá z týchto etáp:

- Plánovanie kontinuity (BCP)
- Analýza dopadov (BIA)
- Príprava plánov obnovy po havárii[18] (DRP)
- Testovanie

12.2.1 Plánovanie kontinuity

V etape plánovania kontinuity (BCP[19]) si každá organizácia potrebuje uvedomiť, aké činnosti alebo procesy[20] sú pre ňu rozhodujúce a ak by bola zásadne narušená ich prevádzka, v akom poradí je potrebné sa zaoberať ich obnovou.

Štandardne je výstupom etapy plánovania tzv. Plán kontinuity - Business Continuity Plan, skrátene sa používa v anglických textoch skratka BCP. Súčasťou plánu kontinuity je súbor zdokumentovaných rozhodnutí, stratégia obnovy organizácie, postup vyhlásenia krízy, komunikačné plány, kontakty na dôležité tímy obnovy vrátane dodávateľov, od ktorých procesy organizácie závisia. Plány kontinuity sú vyžadované v písomnej forme pri certifikácii systémov podľa noriem ISO, formálnymi požiadavkami týchto noriem na BCP sa budeme zaoberať v časti zaoberajúcej sa auditom riadenia kontinuity[21].

Kľúčovým výstupom etapy plánovania a zároveň vstupom pre ďalšiu etapu je práve súbor informácií o procesoch organizácie. V prípade, že je organizácia riadená systematicky - napr. v súlade s požiadavkami normy na riadenie kvality ISO 9001, existuje v organizácii spracovaný dokument, popisujúci kľúčové procesy minimálne v rozsahu[22]:

- Účel procesu
- Vlastník procesu
- Vstupy potrebné pre proces
- Výstupy procesu

[18] Disaster recovery plans, ďalej DRP

[19] Business Continuity Planning, ďalej BCP

[20] Pojmom proces označujeme zreťazenie činností, ktoré transformujú vstupy na výstupy s cieľom dosiahnuť želané výsledky organizácie. Procesným prístupom k riadeniu sa zaoberá norma ISO 9001.

[21] pozri kapitolu Audit

[22] Minimálnym rozsahom informácií pri popisovaní procesov sa zaoberá aj norma ISO ISO/IEC TR 24774:2010 Softvérové a systémové inžinierstvo. Riadenie životného cyklu. Návod na popis procesov

- Kritériá pre riadenie procesu (napr. KPI[23] alebo ciele, parametre)
- Ďalšia dokumentácia procesu ak je to vhodné
- Popis aktivít a tzv. RACI[24] matica alebo iné zachytenie zodpovedností a právomocí pracovných pozícií a činností
- Zdroje potrebné pre proces

Pri príprave stratégie odozvy sú tieto podklady dôležitým vstupom pre rozhodnutia, ktoré procesy sú pre organizáciu dôležité, a určenie, ako dlho vie organizácia znášať následky incidentov bez podstatných dopadov na jej existenciu, tzv. RTO[25], a od čoho je to závislé. Tieto informácie sú kľúčové v ďalšej etape – analýze dopadov tzv. BIA (Business Impact Analysys).

12.2.2 Čo ak? Analýza dopadov na kľúčové procesy organizácie

Pre každú nečakanú udalosť je dobré pripraviť si dopredu, kto má čo robiť, pretože v čase nepredvídateľných udalostí je to rýchlejšie, lacnejšie, pravdepodobne to dopadne lepšie než náhodné chaotické riešenie situácie. Hovoríme tomu stratégia obnovy.

Keďže však v čase plánovania netušíme, čo sa stane, rozmýšľame o možných rizikách. Na to aby sme mohli byť pripravení na rôznorodé nepriaznivé situácie sa vykonáva tzv. analýza dopadov (BIA = Business Impact Analysis).

Základnou úvahou v rámci analýzy dopadov je otázka, aký následok bude mať nežiaduca situácia na výpadok činností (procesov) organizácie.

Vo väčších organizáciách na túto otázku spravidla nedokáže odpovedať jeden človek, je potrebné získať informácie zo všetkých kľúčových oblastí organizácie. Preto je nutné poznať rozdelenie právomocí a zodpovednosti v organizácii a zorganizovať zapojenie všetkých kľúčových rolí. Rozdelenie zodpovedností a právomocí (môžete sa stretnúť aj s používaním skratky RACI[26]) je kľúčovou pri všetkých oblastiach efektívneho riadenia organizácie, nie len pri riadení kontinuity.

Pokiaľ nevieme, čo sú kľúčové procesy a čo je potrebné pre ich prevádzku, bude ťažké pokračovať. Preto je prvým krokom analýzy dopadov súpis a priorizácia procesov organizácie a inventarizácia aktív potrebných pre chod týchto kľúčových procesov.

Na ako dlho by mohli činnosti kľúčových procesov vypadnúť aby to nemalo negatívny vplyv na organizáciu? Keď vypadnú na dlhšie, čo to spôsobí? Rovnaká otázka patrí pri skúmaní výpadku jednotlivých aktív, ktoré sú kľúčové pre chod každého kľúčového procesu.

Niektorí ľudia môžu mať pocit, že takúto analýzu spravia od stola. Opak je pravdou. Je potrebné sa spýtať tých, ktorí za jednotlivé kľúčové procesy zodpovedajú (označovaní aj ako vlastníci procesov).

[23] Key Performance Indicators - kľúčové indikátory výkonnosti

[24] RACI – prvé písmená anglického označenia rôznych možných vzťahov pracovnej pozície a činnosti: Responsible, Accountable, Consulted, Informed.

[25] Recovery Time Objective – plánovaný čas obnovy

[26] Responsible, Accountable, Consulted, Informed – označovanie pre typické vzťahy voči zodpovednosti jednotlivých pozícií v organizáciách

Dokument analýza dopadov (BIA)

Výstupom analýzy dopadov spravidla dokument, kde BIA vyzerá tak, že poznáme kľúčové procesy organizácie, prípustné akceptovateľné doby výpadku pre každý proces (RTO), rozpracovanie do detailu, kde je zrejmé, ktoré aktíva teda smú vypadnúť na maximálne prípustnú dobu akceptovateľného RTO pre proces a máme plán opatrení, ktoré sa musia realizovať, aby toto bolo možné.

Dopady nepredvídateľných udalostí sa spravidla ohodnocujú vo finančnom vyjadrení alebo v bodoch podľa dohodnutej stupnice dopadov. Metodika vyhodnocovania môže byť kvalitatívna (napr. nízky, stredný, vysoký dopad) alebo kvantitatívna (vyjadrená vo finančnom vyjadrení), rozhodnutie o výbere metodiky je na organizácii. Čo je možno v praxi oveľa dôležitejšie, je aby sa na úvahách zúčastnili zástupcovia rôznych častí organizácie a vzali do úvahy pokiaľ možno čo najviac hľadísk aby sa na nič dôležité nezabudlo.

Vzťah analýzy rizík a analýzy dopadov

Povedali sme si, že je potrebné plánovať. Ale čo teda ideme plánovať? Na to aby sme naplánovali a pripravili nejaké opatrenia si potrebujeme predstaviť rizikové scenáre.

Pri analýze dopadov na činnosti organizácie sa berú do úvahy jednotlivé scenáre udalostí, ktorých dopad by bol pre organizáciu zásadný. Jednotlivé scenáre udalostí môžu vychádzať z tzv. analýzy rizík[27], ak je v organizácii k dispozícii[28] .

Pri analýze rizík sa zvažujú potenciálne hrozby, ktoré môžu mať nežiaduci vplyv na aktíva s nejakou odhadovanou pravdepodobnosťou. Výsledkom bude vyhodnotenie rizík.

Na rozdiel od úplnej analýzy rizík, (ktorá nám pri plánovaní kontinuity samozrejme pomôže[29]) neuvažujeme o pravdepodobnostiach výskytu a dopadoch jednotlivých hrozieb s cieľom vypočítať výšku rizika, ale zameriavame sa na praktický dopad na chod organizácie v prípade výpadku činnosti, technológie, ľudí (inými slovami čohokoľvek, čo je pre chod organizácie kľúčové, zvykne sa to označovať aj pojmom aktíva) vplyvom nepredvídateľnej udalosti čiže havárie alebo katastrofy.

Analýza dopadov sa teda primárne zameriava na následky udalosti na činnosť, t.j. jednotlivé procesy organizácie. Ako uvidíte v ďalších príkladoch, ide o úplne logický proces.

Pri určovaní dopadov sa tiež analyzujú tzv. závislosti na aktívach, inak povedané, čo potrebujú procesy v organizácii pre svoje hladké fungovanie. Tieto informácie sú podstatné pre ďalšiu etapu, v ktorej sa spracovávajú plány obnovy týchto dôležitých aktív a zároveň sa analyzujú opatrenia, ktoré sú pre úspešnú obnovu nevyhnutné, čomu sa budeme venovať neskôr.

Pretože nie sú procesy ako procesy, je dôležitým výstupom v tejto etape určenie ich citlivosti s cieľom vyhodnotiť, ktoré z nich je nevyhnutné obnoviť ako prvé a ktoré môžu počkať a ako dlho. Ak by sme mali použiť analógiu s ľudským organizmom, v prípade havárie musíme obnoviť

[27] Prístup založený na riziku je veľmi dôležitou súčasťou systematického riadenia, postup analýzy rizík bol predstavený v úvodnej kapitole a kapitole Manažment informačnej bezpe4nosti

[28] Príklady hrozieb boli uvedené aj v úvodnej kapitole. Pre lepšiu predstavu hrozieb, ktoré môžu mať katastrofický dopad na kontinuitu činností organizácie uvádzame niekoľko príkladov v prílohe

[29] O analýze rizík sa dočítate v kapitole Manažment informačnej bezpe4nosti

Kľúčový proces	**Aktívum**	**RTO**	**DRP**
Krvný obeh	Srdce	4 minúty	Masáž srdca
Dýchanie	Pľúca	4 minúty	Uvoľnenie dýchacích ciest, umelé dýchanie
Metabolizmus	Tráviaci systém, jedlo, nápoje	24 hodín	Umelá výživa

Tabuľka 12.1: Kritické procesy a RTO

kľúčové životné procesy tak, aby sme zachránili organizmus a zabránili trvalým následkom na zdraví, a až potom sa môžeme venovať napríklad zlomeninám.

V prípade ľudského tela by určenie kritických procesov, ich prípustná doba výpadku (RTO) a potrebné aktíva na príklade ľudského organizmu vyzerali takto:

Na uvedenom príklade ilustrujeme, že najprv potrebujeme obnoviť kľúčové životné funkcie a zachraňovať dôležité orgány, ktoré sú predpokladom pre tieto životné procesy. V prípade mozgu dochádza k nenávratným poškodeniam v prípade straty zásobovania kyslíkom už po niekoľkých minútach. Preto je pre návrat do bežného života po havárií kľúčové, aby sme venovali všetky zdroje najprv obnove takých procesov, ktoré by návratu do bežného života mohli navždy zabrániť. Pravdepodobne budeme teda najprv obnovovať krvný obeh a dýchanie a až potom budeme podávať nápoje a jedlo formou umelej výživy. Samozrejme ale pokiaľ trvá výpadok pridlho, pribúdajú ďalšie a ďalšie nutné kroky, napr. dehydratácia alebo hlad môžu rovnako spôsobiť vážne následky na zdraví ak trvajú pridlho.

Rovnako je potrebné zvažovať následky výpadkov aktív, od ktorých sú závislé kľúčové procesy v organizácii. Nie je vždy samozrejmé, že si v každej organizácii uvedomujú, ktoré aktíva to sú. V prípade, že organizácia má systematicky riadenú informačnú bezpečnosť[30], je jednou z riadených oblastí aj riadenie aktív.

Výsledkom systematického riadenia aktív je tzv. zoznam aktív, v ktorom organizácia identifikuje tzv. vlastníkov aktív, tj. názvy pracovných pozícií alebo mená pracovníkov, ktorí aktíva používajú alebo spravujú. Práve títo pracovníci dokážu identifikovať mieru dopadov výpadkov aktív, spravidla majú vedomosť o závislosti medzi aktívami a závislosťami kľúčových procesov organizácie na týchto aktívach.

Pri systematickom riadení aktív musí byť tiež identifikovaná citlivosť aktíva z pohľadu informačnej bezpečnosti, čiže z pohľadu dostupnosti, dôvernosti a integrity dát[31]. Táto identifikácia slúži v etape BIA k tomu, aby boli zohľadnené napr. požiadavky na zachovanie dôvernosti osobných údajov alebo utajovaných skutočností aj v prípade havárie, k čomu organizáciu zaväzujú zákonné predpisy.

Ako sme už uviedli, je výsledkom BIA zváženie citlivosti organizácie vplyvom výpadku procesu. V praxi to znamená, že touto analýzou zistíme poradie, v akom sa procesom venuje pozornosť pri obnove činností v prípade katastrofy. Pri analýze závislostí procesov od aktív ale okrem toho nepriamo zisťujeme aj informáciu o dôležitosti aktíva, čo je informácia potrebná v ďalšej etape, pri príprave plánov obnovy po havárii.

[30]Napríklad v súlade s normou na riadenie systému informačnej bezpečnosti ISO 27001
[31]Kľúčové oblasti riadenia informačnej bezpečnosti boli predstavené v úvodnej kapitole

Ak sa napríklad zistí, že jeden proces je dôležité obnoviť do 2 hodín a iný stačí do 24 hodín a oba sú závislé od rovnakého aktíva, je potrebné toto aktívum obnoviť do 2 hodín.

Ako sa pozerať na cieľový čas obnovy (RTO)

Poďme na chvíľu do reálneho prostredia bežných organizácií a predstavme si rôzne požiadavky na cieľový čas obnovy (RTO) pri systémoch nemocnice. Jednou z kľúčových otázok pre kritický proces vykonávania chirurgických operácií môže byť otázka, ako dlho pacient v narkóze pri operácii vydrží bez podporných systémov, akým je napríklad dýchanie? Tieto systémy môžu byť závislé od dodávok elektrickej energie, vzduchovej ventilácie, dodávok vody a pod. Preto RTO pre dodávku elektriny pri plánovaní kontinuity činností nemocnice bude určené maximálne v minútach, po ktorých pri výpadku elektriny majú spustiť používanie záložných zdrojov napájania nemocnice.

Plánovanie kapacít v tej súvislosti otvára ďalšie špecifické otázky pre prostredie konkrétnej inštitúcie a znalosť potrebných postupov. Pri operácii si vieme predstaviť, že by sa pri plánovaní záložného napájania malo myslieť aj na svetlo aj sterilizáciu. Pri plánovaní je veľmi podstatné ako dlho trvá výpadok primárneho systému, počas ktorého dokáže záložný systém zabezpečiť náhradné riešenie. Pri pretrvávajúcom výpadku je dôležité naplánovať napr. postupné vypínanie menej dôležitých systémov. Na to je potrebné poznať dôležitosť týchto systémov, kde spravidla vystupuje do popredia kritérium, že zdravie a životy ľudí majú prednosť pred ekonomickými škodami.

Čo to je RPO

Pri riadení kontinuity sa môžeme v odbornej literatúre okrem pojmu RTO stretnúť s ešte jednou podobnou skratkou a to je RPO. RPO (angl. Recovery Point Objective) znamená, ako staré dáta mi slúžia na obnovu pri stanovenom čase obnovy RTO. Ak na obnovu dát zo zálohy použijem dáta z včerajšieho večera, tak mám RPO napr. 12 hod. Platí, že čím čerstvejšie dáta používam na obnovu, tým menšia hodnota RPO v čase. Rovnako spravidla platí, že rastúce nároky na RPO sa prejavujú rastúcimi nárokmi na investície do riadenia kontinuity.

V etape plánovania kontinuity je dôležitá príprava stratégií v prípade realizácie niektorého zo scenárov identifikovaných pri BIA. Súčasťou je aj príprava v podobe dobrých plánov na obnovu po haváriách.

12.2.3 Príprava plánov obnovy po havárii

Plány obnovy po havárii[32] (DRP) sú dokumenty, ktoré poskytujú návod na obnovu kľúčových aktív identifikovaných v rámci BIA. Na obsah plánov obnovy neexistuje žiadny univerzálny návod. Plány obnovy po haváriách pre jednotlivé aktíva sú závislé od požívaných technológií, charakteru činností organizácie, jej závislosti od rôznych typov aktív ako sú internetové pripojenie, sieťová prevádzka interných sietí, budovy a kancelárie, dátové centrá alebo dodávateľské služby.

Plány obnovy sa spravidla píšu pre pracovníkov s vedomosťami o daných technológiách, avšak dôležitou časťou prípravy reakcie na incidenty sú úvahy o nedostupnosti týchto pracov-

[32]Disaster recovery plans = DRP

níkov a následnej prípravy dokumentov plánov obnovy tak, aby boli použiteľné aj v prípade neprítomnosti expertov.

Keďže hranica medzi riadením incidentov a riadením kontinuity činností je daná len strategickým rozhodnutím vedenia, kedy budú aktivované procedúry riadenia kontinuity, môžu byť DRP významnou mierou totožné s bežnými postupmi na riadenie incidentov a tak sú v praxi často totožné i činnosti reakcie na incident a činnosti obnovy aktíva[33] .

Plány obnovy sa napr. môžu zaoberať:

- Obnovou sieťovej prevádzky internej siete
- Obnovou funkčnosti centrálneho databázového servera
- Obnovením dát zo zálohy
- Presťahovaním do náhradných priestorov
- Obnovením napájania elektrickou energiou z naftového generátora
- Aplikovaním záložného zdroja napájania (UPS[34]) pri krátkodobom výpadku elektrickej energie
- Presmerovaním pripojenia na internet na náhradného poskytovateľa služby
- Presmerovaním spracovania dát do dátového centra v cloude
- Privolaním pomoci jednotky CSIRT[35] v prípade kybernetického útoku

Oblasti plánov obnovy v rámci vyššie uvedených príkladov môžu byť aplikované jednotlivo alebo súčasne, podľa rozsahu incidentov, ktoré sú prípadne neskôr klasifikované ako katastrofa.

Podľa logiky obnovy a konkrétnych podmienok organizácie sú jednotlivé kroky aplikované v určitom poradí.

Napr. pri výpadku elektrickej energie je potrebné najprv naštartovať naftový generátor ako náhradný zdroj napájania, až potom je možné obnovovať prevádzku servera alebo aplikovať dáta zo zálohy. Ak by sme tieto činnosti robili počas napájania cez UPS, ktoré má časové obmedzenie (toto zistíme napr. pri testovaní obnovy, ktorým sa budeme zaoberať v ďalšej časti), je možné, že tieto činnosti budú prerušené výpadkom UPS s následnou možnou stratou alebo poškodením dát.

Komunikačné plány

Súčasťou pripravovaných dokumentov sú aj tzv. komunikačné plány. Pri vyhlásení krízy je kľúčová koordinácia aktivít obnovy, je potrebné informovať rôzne časti organizácie alebo zainteresované strany ako sú zákazníci či dodávatelia. V mnohých prípadoch podlieha organizácia zákonným povinnostiam voči hláseniu narušenia bezpečnosti alebo súkromia. Preto je praktické pripraviť postupy komunikácie a koordinácie dopredu formou určenia tímov, ich úloh a

[33]Odkaz na riadenie incidentov niekde v inej kapitole
[34]UPS Uninterruptible Power Supply
[35]CSIRT - Computer Security Incident Response Team - jednotka na pre riešenie počítačových incidentov

uvedenia kontaktných údajov na členov tímov. Tak ako sú veľmi rôznorodé plány obnovy, sú rôznorodé aj potreby komunikácie a koordinácie rôznych organizácií pri kríze.

Príkladmi tímov dôležitých pri plánovaní obnovy môžu byť:

- Tím na reakciu na incidenty
- Tlačové oddelenie spoločnosti
- Tím na obnovu dát
- Tím na obnovu sieťovej prevádzky
- Tím na obnovu serverov
- Evakuačný tím

12.2.4 Testovanie

Dobrým spôsobom ako prísť na to, načo sme v predchádzajúcich etapách nepamätali, je testovanie, a to jak plánov kontinuity aj plánov na obnovu činnosti. Skúsenosti z auditov riadenia kontinuity činností[36] ukazujú, že často až testy plánov ukážu slepé miesta, ktoré je potrebné zlepšiť, ak má byť obnova úspešná.

Pre úplnosť si povedzme, že ďalšími možnosťami, ako zistiť, na čo sme nepomysleli, sú samozrejme samotné incidenty, ktoré v praxi ukážu našu pripravenosť, alebo incidenty, ktorých rozsah považujeme za katastrofu, a teda poučenie na svojich vlastných chybách. Je to jedna z možností. Môže sa ale stať, že incident nie je uspokojivo vyriešený a v extrémnom prípade vedie k zániku organizácie.

Tetovanie plánov obnovy by malo pokrývať všetky časti plánovania kontinuity. Neznamená to, že sa má ochromiť prevádzka, aby sa otestovalo, či boli plány kontinuity spracované správne. K tomu, ako dôsledne a relatívne bezbolestne zistiť kvalitu BCP testovaním, existuje viacero prístupov:

Tzv. testovanie od stola, kedy sa plány prechádzajú ako teoretické cvičenie s tímami obnovy. Už pri tejto forme testovania je možné prísť na nelogické časti plánovania kontinuity, predovšetkým tak, že sa za stôl posadia zástupcovia rôznych častí organizácie, ktorí môžu postrehnúť nedostatky z rôznych uhlov pohľadu vyplývajúcich z diverzity znalostí a skúseností.

Čiastočné testovanie plánov: testujú sa jednotlivé výpadky čiastkových komponentov napr. v čase ich bežnej údržby a zároveň sa pretestuje procedúra obnovy formou kontroly správnosti postupu, správnosti a aktuálnosti dokumentácie, ale tiež niekedy prehliadané nebo automaticky predpokladané schopnosti personálu aplikovať dokument v prípade potreby vzhľadom na svoje vedomosti a pod. Napr. pri výmene pokazeného routera sa v sieti otestuje správnosť redundantného zapojenia náhradného smerovania sieťovej prevádzky.

[36] kapitola Audit

Alebo pri inštalácii novej technológie sa preskúša správnosť a úplnosť zaškolenia personálu do údržby tak, že inštaláciu vykoná školený pracovník pod dohľadom špecialistu od dodávateľa.

Úplné testovanie plánu kontinuity — maximálne možné otestovanie v plnom rozsahu, pričom je vhodné brať ohľad na možné narušenie skutočnej prevádzky spoločnosti, aby sa samotné pripravovanie na katastrofu nestalo katastrofou.

12.2.5 Príklady z praxe

V predchádzajúcich častiach sme ilustrovali všeobecné etapy plánovania kontinuity činností. Napriek tomu, že vo všeobecnej rovine sú tieto etapy rovnaké, v praxi je potrebné riadenie kontinuity významne prispôsobiť procesom organizácie, výsledkom veľmi dôslednej analýzy dopadov, teda BIA, a plány obnovy po haváriách, teda DRP, je potrebné tiež veľmi individuálne prispôsobovať konkrétnym okolnostiam organizácie.

Z toho vyplýva, že k rôznym šablónam a schematickým aplikáciám riadenia kontinuity prevzatým z teoretických návodov je vhodné pristupovať veľmi triezvo. Ako veľmi rôzne môžu byť procesy rôznych organizácií, ako majú rovnaké negatívne udalosti veľmi rôzny dopad na kontinuitu činností organizácie a ako rôzne môžu byť plány a opatrenia pri obnove bežnej prevádzky, si v tejto časti ukážeme na príkladoch troch rôznych organizácií.

Organizácia A

sa zaoberá spracovaním údajov o nákupnom správaní zákazníkov spoločností v oblasti predaja formou elektronického obchodu. Produkt spoločnosti je postavený na moderných technológiách s podporou strojového učenia a umelej inteligencie a prevádzkovaný formou Cloud Computingu. Spoločnosť nevlastní žiadne dátové centrá, IT infraštruktúru ani budovy alebo kancelárie. Pracovníci spoločnosti môžu teoreticky pracovať odkiaľkoľvek na svete a s kolegami komunikujú formou video konferencií a IT technológií podporujúcimi spoluprácu. Spoločnosť poskytuje svojim zákazníkom služby okamžitého spracovania dát v reálnom čase, a preto sú dohody o úrovni poskytovaní služieb (ďalej SLA[37]) uzatvorené so zákazníkmi veľmi prísne. V prípade otázok alebo problémov majú používatelia produktu A k dispozícii služby podpory formou dialógového okna priamo v používateľskom rozhraní produktu organizácie A.

Organizácia B

je sieť maloobchodných prevádzok s centrálnym skladom a kanceláriami sídla spoločnosti. Zásobovanie predajní je závislé od dopravy tovaru, dostupnosti tovaru u dodávateľov a služieb centrálneho skladu. Predajne sú pripojené do internej siete a pre potreby predaja používajú softvérovú aplikáciu pripojenú do centrálnej databázy v reálnom čase. Zároveň sú predajne napojené na systém evidencie elektronických registračných pokladní. Predajne sú prevádzkované na 2 pracovné smeny aby pokryli otváracie hodiny v rozsahu otváracích hodín veľkých obchodných centier. Typickým zákazníkom organizácie B je návštevník obchodného centra.

[37] Service Level Agreements

Organizácia C

poskytuje služby externej správy registratúry pozostávajúce z uskladnenia písomností, ich evidencie, ochrany a sprístupnenia na základe žiadanky pracovníkov klientov organizácie C. Organizácia svojim klientom umožňuje, že nemusia disponovať skladovacími priestormi a pracovníkmi, ktorí sa o písomnosti starajú, pritom ale stále majú písomnosti k dispozícii do 24 hod od žiadanky. Písomnosti sú uskladnené v centrálnom sklade, ktorý je zabezpečený protipožiarnymi a bezpečnostnými prvkami a vybavený čítačkami čiarových kódov pre rýchlu identifikáciu písomností a ich umiestnenia. Evidencia písomností je v centrálnej databázovej aplikácií, ktorá v reálnom čase umožňuje pracovníkom klientskych organizácií prehľadávanie písomností a podávanie žiadostí o ich sprístupnenie. Sprístupnenie písomností na základe žiadaniek prebieha do 24 hodín dovozom kuriérom na základe SLA s prísnymi postihmi v prípade nedodržania termínu.

Organizácia D

je banka. Sektor bankovníctva podlieha prísnej regulácii, takže informačná bezpečnosť a systematické riadenie kontinuity je tradičnou súčasťou procesov. Banka má spracované podrobné smernice, stabilizované sieťové a počítačové vybavenie, dostatok zdrojov a dbá na aktualizáciu dokumentácie, dôsledné preškolenie personálu a rozsiahle pravidelné testy obnovy.

Organizácia E

je nemocnica. Evidencia centrálneho príjmu a karty pacientov sú uložené v centrálnom databázovom informačnom systéme s prístupom z počítačov lekárov a sestier v architecture klient-server. Informačný systém je spravovaný externým dodávateľom, ktorý sa pripája vzdialeným pripojením.

Identifikácia kľúčových procesov organizácií v príkladoch

Už pri identifikácii kľúčových procesov vidíme ako veľmi sa líšia výsledky podľa konkrétnej organizácie, potrieb jej klientov, stavu ich technologického vybavenia a potrebných aktív. Samozrejme pre potreby príkladov v tejto kapitole sme príklady v porovnaní s praxou značne zjednodušili.

Procesy identifikované ako kľúčové v organizácii A

- Spracovanie dát
- Zákaznícka podpora
- Vývoj a údržba aplikácie

Procesy identifikované ako kľúčové v organizácii B

- Prevádzka predajne
- Zásobovanie tovarom
- SW aplikácia predajne

Procesy identifikované ako kľúčové v organizácii C

- Aplikácia žiadaniek
- Prevádzka skladu
- Služby kuriéra

Procesy identifikované ako kľúčové v organizácii D

- Prevádzka pobočky
- Internetové bankovníctvo
- Spojenie s clearingovým centrom a spracovanie platieb kartami

Procesy identifikované ako kľúčové v organizácii E

- Centrálny príjem
- Lôžkové oddelenie
- Výkon operácií

Úvahy pri BIA vyplývajúce z rôznosti okolností týchto procesov a výsledné RTO:

	Proces (RTO)	Negatívny vplyv nejakej udalosti	Dopady na organizáciu
A	Spracovanie dát (1 minúta)	Nedostupnosť komponentov cloudovej architektúry alebo sieťovej konektivity Dáta sú spracované nesprávne Dáta nie sú spracované včas	Pokuty za nedodržanie SLA, strata tržieb, odchod zákazníkov ku konkurencii, strata dôvery investorov, zníženie hodnoty organizácie, bankrot
	Zákaznícka podpora (1 minúta)	Zákaznícka podpora neodpovedá (napr. výpadok personálu vplyvom pandémie, neznalosť)	Pokuty za nedodržanie SLA, strata dôvery a nespokojnosť používateľov aplikácie
	Vývoj a údržba SW (24 hod)	Chyby v aplikácii nie sú opravené	Strata postavenia na trhu, strata dobrého mena, odchod zákazníkov ku konkurencii, bankrot

	Proces (RTO)	**Negatívny vplyv nejakej udalosti**	**Dopady na organizáciu**
B	Prevádzka predajne (3 dni)	Nie je kde predávať (priestory predajne) Nie je komu predávať (pandémia) Nemá kto predávať (štrajk, pandémia)	Výpadok tržieb, bankrot
	Zásobovanie tovarom (14 dní)	Nie je čo predávať	Čiastkový výpadok tržieb, strata sa zvyšuje s postupným vypredávaním zásob na predajni, ktorá má typicky priemernú mesačnú zásobu na sklade.
	SW aplikácia predajne (3 dni)	Nie je na čom predávať (chyba aplikácie, výpadok internetu, výpadok sieťového spojenia s databázou)	Predaj cez náhradné postupy, strata informácie o stave zásob, zdržiavanie pri ručnom vypisovaní dokladov o predaji, nepresnosti v evidencii, pokuta za chyby v účtovníctve

	Proces (RTO)	**Negatívny vplyv nejakej udalosti**	**Dopady na organizáciu**
C	Aplikácia žiadaniek (4 hod)	Písomnosti sa nedajú dohľadať, sú nedostupné pre pracovníkov klientov	Pokuty za porušenie SLA, odchod zákazníkov ku konkurencii, strata dôvery investorov, bankrot
	Prevádzka skladu (24 hod)	Poškodenie, zničenie alebo nedostupnosť priestorov s dopadom na písomnosti	Pokuty za porušenie SLA, súdne spory, vymáhanie škody za pokuty za porušenie daňových a účtovných predpisov klientov pri strate registratúry, bankrot
	Služby kuriéra (24 hod)	Písomnosti sa nedopravia včas ku klientom	Pokuty za porušenie SLA, nespokojnosť zákazníkov

	Proces (RTO)	**Negatívny vplyv nejakej udalosti**	**Dopady na organizáciu**
D	Prevádzka pobočky	Prevádzka pobočky nie je dostupná	Nepohodlie a nespokojnosť zákazníkov, použitie internetového bankovníctva alebo inej pobočky, pri veľkom rozsahu odchod klientov banky ku konkurencii
	Internetové bankovníctvo	Nedostupnosť služby. Pri hackerskom útoku možno narušenie bezpečnosti a okradnutie klientov.	Súdne spory s klientami, pokuty zo strany regulátorov. V extrémnom prípade zrušenie bankovej licencie alebo bankrot.
	Spojenie s clearingovým centrom a spracovanie platieb kartami	Neskoré alebo nesprávne zrealizovanie operácií.	Súdne spory s klientami, pokuty zo strany regulátorov. V extrémnom prípade zrušenie bankovej licencie alebo bankrot.

	Proces (RTO)	**Negatívny vplyv nejakej udalosti**	**Dopady na organizáciu**
E	Centrálny príjem	Elektronická evidencia je nefunkčná, prechod na manuálnu.	Predlžovanie čakacích dôb, ohrozenie zdravia a života pacientov, nutnosť prevozu do iných nemocníc
	Lôžkové oddelenie	Nedostupnosť evidencie k výkonom a sledovanie pacientov	Prechod na manuálne sledovanie, nutnosť prevozu.
	Výkon operácií a ambulantná starostlivosť	Znemožnenie výkonu operácií, bez kariet pacienta nie je možné poskytovať starostlivosť	Paralýza prevádzky, zastavená činnosť

Príkladmi z praxe sme chceli poukázať na to, že dôvody výpadkov kľúčových procesov rôznych organizácií sú veľmi rôznorodé, rovnako budú rôznorodé aj plány obnovy týchto organizácií, avšak pre všetky organizácie platí, že pokiaľ nebudú na nepriaznivé udalosti reagovať včas a profesionálne, môžu mať výpadky veľmi negatívne následky pre existenciu a budúcnosť organizácií.

Spravidla ak zákazníci, klienti alebo používatelia produktov a služieb organizácií považujú služby za dostatočne dôležité, aby za nich boli ochotní platiť, je vysoko pravdepodobné, že tiež očakávajú, že budú za všetkých okolností k dispozícii neboli že organizácia zabezpečí svoju kontinuitu.

Aj v prípade, že organizácia prvotné následky závažného incidentu nejako prežije, neskorá reakcia, zlá komunikácia alebo iným spôsobom nevhodný priebeh obnovy môžu zákazníkom naznačiť, aby v dlhodobom meradle vyhľadali na trhu spoľahlivejšiu alternatívu.

12.2.6 Nastavenie postupov na dosiahnutie cieľového času obnovy

Pri určovaní postupu krokov v rámci obnovy konkrétnych aktív, ktorých výpadok ohrozuje proces organizácie, musíme vychádzať z cieľového času obnovy, teda maximálne možného času, ktorý môže uplynúť, kým obnovíme funkčnosť aktív, čo sme identifikovali v rámci analýzy dopadov.

Často až systematická analýza dopadov a následné snahy o spracovanie postupu obnovy poukážu na nerealistické očakávania a absenciu súladu medzi potrebami zachovania kontinuity procesov a pripravenosti organizácie realizovať tieto opatrenia.

Dôvody môžu byť rôzne:

- Nedostatok zdrojov (peniaze, ľudia, technológia)
- Slabá informovanosť o postupoch a nákladov na opatrenia
- Nedostatok vedomostí personálu na obnovu prevádzkovaných technológií

Príklad z praxe pri príprave organizácie na certifikáciu systému riadenia kontinuity činnosti podľa ISO 22301. Pri otázke, ako dlho môže trvať v spoločnosti výpadok emailovej komunikácie, generálny riaditeľ okamžite odpovedal, že maximálne 5 minút. Po predložení kalkulácie technického riešenia zabezpečenia RTO 5 min bolo toto očakávanie s veľkou nevôľou prehodnotené na 3 dni. RTO 5 min predpokladalo redundanciu emailového servera zapojeného v clustri s vysokou dostupnosťou a drahou službou okamžitej podpory pri výpadku akéhokoľvek komponentu.

Pred rozšírením služieb cloudových technológií znamenalo aj zabezpečenie RTO na 3 dni významné investície pri dohodách s dodávateľmi, ktorí zabezpečovali tzv. cold sites alebo hot sites, prípadne skladovanie náhradných dielov alebo celých zostáv technologických prvkov, ktoré organizácia používa. Dnešné možnosti cloudových technológií umožňujú úplne iné prístupy organizácií pri riadení kontinuity.

Tieto výhody je možné aplikovať za predpokladov zásadných organizačných zmien, ktoré v súčasnosti vo svete označuje ako "digitalizácia". Výhodu v tomto smere majú relatívne nové organizácie, ktoré sa "narodili digitálne", napr. tzv. startupy[38] , ktoré vytvárajú svoje softvérové produkty priamo v cloude a ponúkajú formou predplatného (Software as a Service, SaaS).

12.2.7 Cloud computing a jeho využitie pri riadení kontinuity

Cloud computing v súčasnosti prináša veľmi zaujímavé možnosti použiteľné aj pri riadení kontinuity. Miesto zabezpečovania investične náročných náhradných priestorov pre prípad zničenia budovy organizácie alebo celých záložných dátových centier, je možné zvážiť pre a proti využívania služieb poskytovateľov cloudových riešení.

[38]Startup - označenie začínajúcich firiem, spravidla takých, ktoré sa snažia nájsť obchodný model rýchleho rastu. Idealizovaná predstava začínajúcich startupov je snaha stať sa tzv. Jednorožcom. Ako jednorožec (angl. Unicorn) sú označované startupy, ktoré prekročili rýchlym rastom 1 miliardu dolárov ako hodnotu spoločnosti

Cloud computing, samozrejme ako všetko na svete, popri výhodách prináša aj riziká. Prehľad výhod a nevýhod pri používaní cloudových služieb najdeme napr. v analýze rizík pri používaní cloudových služieb, ktorú spracovala ENISA.[39]

Ošetrenia rizík, ktorými sa zaoberáme v časti o audite cloudových technológií[40] , umožnia organizácii využívať predovšetkým výhody z úspory z rozsahu, ktoré okrem ekonomických výhod môžu mať aj priaznivý dopad z hľadiska rozsahu implementovaných bezpečnostných opatrení.

Vráťme sa ešte k našim príkladom pri riadení kontinuity organizácií a tomu, ako sme pri nich stanovili RTO a RPO a ako vyzerajú príklady postupov z ich plánov obnovy.

Ako dokáže organizácia A dosahovať RTO v rozsahu 1 minúty

Pre spoločnosť A je prípustný RTO do 1 minúty, vzhľadom na to, že najväčší prínos z používania aplikácie majú zákazníci spoločnosti vtedy, keď sú dáta spracúvané v reálnom čase.

V prípade oneskorenia alebo zlého spracovania časti dát prudko klesá prínos pri používaní softvérovej aplikácie, čo je hlavný prínos existencie firmy na trhu.

Túto reakčnú schopnosť umožňuje spoločnosti A využívanie cloudových technológií a architektúra orientovaná na spracovanie petabytov údajov v reálnom čase.

V praxi predstavujú postupy v DRP tejto spoločnosti sústavu automatizovaných procesov a zreťazenie používaných technológií do asynchrónneho toku operácií nad dátami[41], kedy sú nasadením obrovskej výpočtovej sily v cloude dáta okamžite spracované do podoby, v akej sú dostupné používateľovi cez používateľský interface (tzv. frontend).

Zároveň dáta ešte existujú po nejaký čas (napr. 7 dní alebo 30 dní, podľa nastavenej exspirácie) v technológiách použitých v postupných krokoch asynchrónneho spracovania, čiže pri výpadku ktoréhokoľvek prvku spracovania dát je možné obnovou jeho funkčnosti dáta spracovať na základe opätovného spracovania dát z predchádzajúcej operácie.

RPO je v tomto prípade nastavené na 0. V rámci SLA a podmienok používania aplikácie je podstatné, aby všetky dáta boli spracované bez strát.

Zároveň sú kvôli vysokému nároku na kapacitu spracovania nasadené technológie redundantne, čo má priaznivý vplyv na získavanie vysokej dostupnosti. Síce sa pri výpadku niektorého z paralelne zapojených komponentov spomalí spracovanie dát, avšak nakoľko sú dáta z pohľadu koncového používateľa aplikácie spracúvané stále, nie je to často ani možné spozorovať.

Vznikajúce oneskorenie spracovania dát je zároveň sledované komplexným systémom monitoringu, čo umožní personálu technickej podpory vykonať zásah skôr, než príde k spozorovateľnej degradácii výpočtových služieb v architektúre, a dodržať tak prísne SLA.

Týmto prístupom sa dá za relatívne prístupných finančných podmienok (na strane používateľov aplikácie) zabezpečiť obrovská výpočtová sila s vysokou mierou odolnosti voči výpadkom,

[39]Cloud Computing Security Risk Assessment - Benefits, risks and recommendations for information security, ENISA November 2009 https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security/view

[40]kapitola Audit

[41]Napr. https://cloud.google.com/solutions/mobile/mobile-gaming-analysis-telemetry

čo by bez vhodného zreťazenia všetkých prvkov architektúry v cloude, zapojení redundantnej architektúry, nasadení monitorovacích nástrojov a služby technickej podpory zaškoleným personálom nebolo možné. Významnou úlohu v prípade organizácie A zohráva tiež využívanie nakupovanej technológie PaaS (Platform as a Service), kedy sa pracovníci technickej podpory a softvéroví inžinieri spoliehajú na služby platformy pri prevádzke siete, riadenia prístupov, správy databázových riešení, monitoringu a iných služieb a môžu sa venovať špecifickým nastaveniam funkcionality spracovania dát pre konkrétnu aplikáciu.

Prečo organizácii B postačuje RTO v rozsahu 3 dní

V prípade organizácie B bolo pri analýze určené RTO na 3 dni na základe zložitosti a nákladov na opätovné vrátenie do prevádzky pri ručnom nahrávaní predajov vykonaných v čase výpadku SW aplikácie.

Ošetrenie výpadkov priestorov predajní je vyriešené zmluvnými podmienkami s prenajímateľmi v nákupných centrách. Zabezpečenie personálu je v DRP zachytené formou rotácie z iných predajní. V extrémnom prípade nedostupnosti predajní aj personálu, ako sme tomu boli svedkami v čase Corona krízy, jednoducho neexistoval počas vyhláseného núdzového stavu alternatívny postup pre maloobchodný predaj a spoločnosť predávala len formou elektronického obchodu.

RPO nie je v tomto prípade podstatné, nakoľko dáta zo záloh nepomôžu riešiť chýbajúce dáta z predajov „na paragony[42]“ počas výpadku, ktoré je potrebné nahrať po opätovnom spustení SW aplikácie do prevádzky, kvôli správnosti skladovej evidencie a z dôvodu povinností vyplývajúcich z daňových a účtovných predpisov.

Doba RTO je stanovená na 3 dni jednoducho empiricky, kedy nároky na ručné nahratie 3 dní tržieb presahujú kapacity personálu a znamenajú dodatočné náklady (napr. nadčasy, brigádnici).

Zároveň náklady na opatrenia, ktoré znamenajú zabezpečenie funkčnej prevádzky do doby 3 dní nepredstavujú neriešiteľné náklady.

Obnova internetového pripojenia je riešená formou SLA s dodávateľmi a alternatívnymi možnosťami pripojenia cez dátové mobilné služby.

Obnova výpadku centrálnej serverovej infraštruktúry do 3 dní je realizovateľná s veľkou rezervou formou náhradného servera zálohovaného v reálnom čase.

Zásobovanie tovarom z centrálneho skladu je alternatívne riešené dohodami o rozvoze tovaru priamo od dodávateľov do jednotlivých predajní v prípade potreby.

Predaj cez webovú stránku eShopu spoločnosti B predstavoval čiastočnú náhradu výpadku tržieb predajní v čase uzatvorených nákupných centier v čase Corona krízy aj keď osobný kontakt so zákazníkom a možnosť si tovar chytiť pred nákupom do ruky znamená nepochybne výhodu osobného kontaktu v predajni.

[42] Označenie tlačiva, ktoré sa používalo ako doklad o predaji pred zavedením elektronických registračných pokladní

Test kontinuity v organizácii C rozhodol o rozšírení ponuky služieb

Ilustrácia systému riadenia kontinuity organizácie C vychádza z reálneho príkladu spoločnosti, ktorá má certifikovaný systém riadenia kontinuity činností a v praxi dôsledne realizovala všetky výhody, ktoré systémový prístup prináša.

RTO organizácie C vychádzalo z SLA, ktoré boli zákazníkmi podmienkou pre uzatvorenie zmluvného vzťahu. Bez toho, aby bola organizácia C schopná sľúbiť, že privezie dokumentáciu do 4 hodín alebo najneskôr ďalší pracovný deň späť k zákazníkovi, ak ju jeho pracovník potrebuje, znamenala zásahy do schopnosti rýchlo vyhľadať záznam (implementovaním označovania a snímania písomností a ich umiestnenia cez čiarové kódy). To predpokladá prebratie a označenie písomností pri dodávke nových registratúrnych záznamov od zákazníka. Veľké obavy zákazníkov z rizika poškodenia písomností požiarom, vodou či narušením priestorov v dôsledku vlámania viedli k rozsiahlym opatreniam na strane budovy. Zároveň bola prenajatá ďalšia budova, ktorá bola pripravená na presťahovanie v prípade krízy (náklady na prenájom).

Pracovníci pravidelne absolvovali cvičenia, ktoré testovali schopnosť presťahovať celý sklad registratúry do náhradných priestorov v priebehu 24 hodín. V prípade výpadku databázy registratúry cez ktorú si zákazníci žiadajú o záznamy, bol vybudovaný systém vysielačkovej komunikácie v rámci skladu na základe komunikácie dispečera so zákazníkom a okamžitého dohľadania záznamov v sklade (mobilné telefóny sú v sklade spolu s akýmikoľvek technológiami umožňujúcimi robiť záznam z registratúrnych dokumentov zakázané). Napriek tomu bolo vyhodnotené pri testovaní kontinuity zvyškové riziko straty záznamov pre zákazníkov ako neakceptovateľné.

Aplikácia postupov v súlade s certifikačnou normou ISO 22301 priniesla rozhodnutie, že spoločnosť zaviedla službu digitalizácie registratúrnych záznamov, ktorú uvítali aj zákazníci C a stala sa významným zdrojom nárastu tržieb spoločnosti. Záznamy, ktoré sú dnes plne digitalizované, prestali mať v prípade výpadku ich dostupnosti neakceptovateľný dopad. Na druhej strane digitalizácia priniesla zvýšené nároky na ochranu dôvernosti záznamov, čo vyvolalo dodatočné opatrenia v oblasti riadenia prístupových práv, potrebu penetračného testovania, zavedenie šifrovej ochrany a pod. v rámci aktualizácie plánov kontinuity.

V organizácii D znamená riadenie kontinuity a testovanie obnovy už nudnú rutinu

Banka má v praxi implementované smernice, ktoré zabezpečujú aktualizácie plánov obnovy a preškolenie personálu ako súčasť zmenového riadenia pri zmenách organizácie vrátane presunov personálu, úprav softvérového vybavenia alebo pri pravidelnej obnove hardvérového vybavenia, stabilizované sieťové a počítačové vybavenie. Je nutné podotknúť, že na toto všetko má aj dostatok zdrojov a dbá na aktualizáciu dokumentácie. Cenou za to je však veľmi komplexný sled krokov pri schvaľovaní každej zmeny a relatívne zdĺhavá implementácie zmien do praxe. Rozsiahle pravidelné testy obnovy spravidla neprinášajú veľké prekvapenia a banka výsledkami testovania dokladá plnenie dodržiavania regulačných požiadaviek.

V organizácii E sa pri kybernetickom útoku obnova prevádzky nepodarila

Nemocnica je veľmi citlivý a zraniteľný cieľ kybernetického útoku. Zraniteľnosť má niekoľko príčin, ktoré sú niekde spoločné s inými organizáciami, ale aj špecifické, ktoré vychádzajú z

prostredia danej nemocnice. V konkrétnom prípade boli identifikované problémy s aktualizáciou hesiel, znalosťami a preškoľovaním personálu, bezpečnou prácou s e-mailom, ale aj používaním vzdialeného prístupu bez patričného zabezpečenia (VPN). Používanie externých komponentov na pripájanie k terminálom nemala organizácia vyriešené, keď si mohol užívateľ pripojiť k svojmu počítaču ľubovoľné zariadenie bez patričnej kontroly.

Argumentom organizácie bolo, že vzhľadom na nedostatok a vyťaženie personálu, nie je dostatočný priestor na riešenie a dodržiavanie elementárnych bezpečnostných požiadaviek. Cesta ku kybernetickému útoku bola potom jednoduchá. Útočník použil škodlivý kód „ramsovér“ na zašifrovanie databáz. Nakoľko organizácia nemala správne nastavené zálohovanie, zašifrované boli aj zálohy a nebola možná obnova systému zo záloh.

V tom momente prestali fungovať systémy a nemocnica bola paralyzovaná. Bez prístupu do systému musela zrušiť všetky plánované zákroky a prejsť v akútnych prípadoch na manuálnu prevádzku. Prevádzka bola zastavená a nebola obnoviteľná. Inštitúcia v tom momente prestala vykonávať činnosť na ktorú bola zriadená, s akútnym a priamym dopadom na zdravie svojich pacientov.

Po vyčerpaní všetkých dostupných prostriedkov, bola nemocnica nútená pristúpiť k zaplateniu požadovanej čiastky útočníkom, aby jej poskytol heslo na otvorenie zašifrovaných databáz.

12.3 Systém hlásenia incidentov ako súčasť povinností pri riadení kontinuity činností

Incidenty môžu mať za následok škody veľkého rozsahu v organizácii, ale aj na úrovni globálnych dopadov na bezpečnosť a ekonomiku, preto vznikli národné a medzinárodné regulácie, ktoré vynucujú hlásenie incidentov s cieľom koordinácie pri ich prevencii a eliminácii.

Jednou z takýchto regulácií v Európe je NISD[43], ktorá ukladá národným regulátorom prijať opatrenia s cieľom vybudovať systém hlásení incidentov.

Na Slovensku je implementáciou smernice NIS zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti, ktorý ukladá pre organizácie povinnosti pri riešení a hlásení incidentov. Zákon sa týka tzv. poskytovateľov základných služieb a poskytovateľov digitálnych služieb. Základné služby vymedzuje zákon výpočtom dôležitých oblastí hospodárstva, ktorých narušenie by malo dopad na bezpečnosť, životy, zdravie a finančnú situáciu obyvateľstva.

Rozsah odvetví, ktoré podliehajú zákonu o kybernetickej bezpečnosti vymenúva príloha zákona, pre ilustráciu sú to sektory: bankovníctvo, doprava, digitálna infraštruktúra (prevádzka doménových mien na internete, register domén, uzly internetu), elektronické komunikácie, energetika, infraštruktúra finančných trhov, pošta, priemysel, meteorologické služby, vodné stavby a zabezpečenie pitnej vody, verejná správa (obrana, bezpečnosť, spravodajské služby a utajované skutočnosti) a zdravotníctvo. Pri stanovení, či sa povinnosti vzťahujú na jednotlivé pre organizácie z uvedených sektorov, je rozhodujúce, či spĺňajú tzv. sektorové a dopadové kritéria,

[43]Smernica NIS (NIS Directive, ďalej len NISD): Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6.júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii

ktoré stanovuje vyhláška č. 165/2018 Z.z., ktorou sa určujú identifikačné kritériá prevádzkovanej služby.

Digitálne služby predstavujú: Cloud Computing, online trhovisko a internetový vyhľadávač.

Keďže NISD má za cieľ predovšetkým zabezpečiť implementáciu opatrení pre kľúčové organizácie, ktorých výpadky služieb by mali zásadné následky pre život krajiny, oslobodzuje z povinností poskytovateľov digitálnych služieb tzv. malé a stredné podniky. Do tejto kategórie spadajú organizácie, ktoré neprekračujú kritéria 50 zamestnancov a ročný obrat alebo celkovú ročnú bilanciu viac ako 10 000 000 eur.

Pri hlásení bezpečnostných incidentov na základe povinností zo zákona o kybernetickej bezpečnosti je potrebné uviesť nasledovné údaje:

Typ hlásenia: Prvotné alebo doplňujúce Druh údajov potencionálne zasiahnutých bezpečnostným incidentom

- Sektor
- Informácie o tom, kto hlási závažný kybernetický bezpečnostný incident
  - Názov a sídlo prevádzkovateľa základnej služby alebo poskytovateľa digitálnej služby
  - Názov poskytovanej základnej služby
  - Kontaktné údaje osoby oprávnenej riešiť hlásený závažný kybernetický bezpečnostný incident - Menný zoznam s emailom a telefónnym číslom
- Informácie o závažnom kybernetickom bezpečnostnom incidente v rozsahu potrebnom na jeho riadnu identifikáciu
  - Kategória závažného kybernetického bezpečnostného incidentu (Stupeň I, II alebo III)
  - Typ závažného kybernetického bezpečnostného incidentu
  - Časové údaje zistenia a vzniku závažného kybernetického bezpečnostného incidentu
  - Detailný opis priebehu závažného kybernetického bezpečnostného incidentu a jeho prvotná príčina
  - Popis rozsahu škôd
  - Odhad závažnosti dopadu závažného kybernetického bezpečnostného incidentu na užívateľov základnej služby alebo digitálnej služby
- Informácie o službe zasiahnutej závažným kybernetickým bezpečnostným incidentom
  - Prvotne zasiahnuté aktíva (Host/IP, vrátane identifikácie informačného systému a prevádzkových parametrov služby
  - Informácia, či ide o kritické aktíva z pohľadu zabezpečenia kontinuity služby alebo činnosti, a či je zariadenie v čase podávania hlásenia v prevádzke
- Informácie o riešení závažného kybernetického bezpečnostného incidentu
  - Stav riešenia závažného kybernetického bezpečnostného incidentu

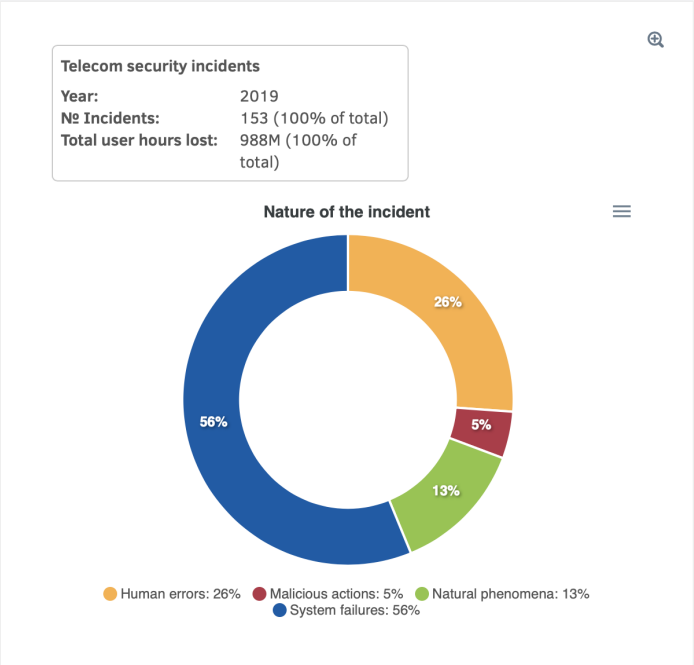
- Informácia o vykonaní nápravných opatrení smerujúcich k riešeniu hláseného závažného kybernetického bezpečnostného incidentu
- Opatrenia na zamedzenie opakovania závažného kybernetického bezpečnostného incidentu
- Popis možných negatívnych dopadov, opatrení a možných dôsledkov závažného kybernetického bezpečnostného incidentu
- Výsledok opatrení
- Dátum a čas realizácie opatrení

Hlásenie sa podáva buď odoslaním šifrovaného e-mailu na adresu sk-cert@nbu.gov.sk alebo nahlásením pomocou web formulára https://www.sk-cert.sk/sk/rady-a-navody/nahlasit-incident/index.html. Organizácia si môže dohodnúť aj inú formu hlásenia formou zmluvy s Národným bezpečnostným úradom.

Cieľom hlásení je získať prehľad o možných útokoch na dôležité organizácie v Slovenskej republike a umožniť tak varovania, ktoré NBÚ vydáva na základe hlásení.

12.3.1 Hlásenia národných incidentov do ENISA

Vzhľadom na dôležitosť telekomunikačných technológií a internetu sa zaviedli v tejto oblasti povinnosti sledovať a hlásiť incidenty ešte pred platnosťou NISD. Telekomunikační operátori a poskytovatelia služieb poskytujúcich dôveru[44] majú povinnosť poskytovať národným regulátorom hlásenia o incidentoch. Tieto hlásenia sa zhromažďujú



[44] Tzv. Trusted services providers

v ENISA[45], ktorá ich zverejňuje na svojej stránke. Zdroj týchto informácií môže byť užitočný pri určovaní priorít, na ktoré potenciálne príčiny incidentov sa zamerať pri plánovaní kontinuity.

ENISA spracúva tieto hlásenia do prehľadného vizuálneho zobrazenia[46]. V rokoch 2018-2019 viedli v zozname príčin výpadkov služieb zlyhania systémov, ľudské chyby a prírodné živly. Pozri nasledujúci obrázok[47].

[45] Agentúra Európskej únie pre kybernetickú bezpečnosť ENISA (European Union Agency for Cybersecurity)
[46] Dostupné na adrese |https://www.enisa.europa.eu/topics/incident-reporting/for-telcos/visual-tool
[47] ibid

Kapitola 13

Audit

Lenka Gondová

13.1 Úvod

V živote každého manažéra sa nájde chvíľa, kedy si hovorí, či vlastne vie, čo sa mu vo firme odohráva. Ak je organizácia ešte malá, je jednoduché rozumieť všetkým činnostiam, mať čas sa občas porozprávať so všetkými pracovníkmi a mať jasno v tom, čo sa v organizácii robí, ako sa to robí a či smeruje, kam chceme.

Ako však ide čas, firmy sa rozrastajú, procesy sú čoraz zložitejšie a situáciu paradoxne neuľahčuje ani to, že sa v organizáciách spoliehame čoraz viac na rôzne technológie.

Vedenie spoločnosti napriek tomu nesie zodpovednosť voči zainteresovaným stranám. Ako je teda možné nevedieť, ale zároveň zodpovedať?

Na to je tu audit. Audit je možné jednoducho charakterizovať ako porovnanie voči požiadavkám.

13.1.1 Druhy auditu

Na základe zdrojov požiadaviek poznáme rôzne druhy auditu.

Finančný audit vychádza napr. zo zákonov o účtovníctve a daniach s cieľom získať uistenie, že údaje v účtovných systémoch organizácie zodpovedajú skutočnosti.

Keďže historicky začali byť informačné systémy čoraz viac zapájané do všetkých činností vrátane podpory spracovania účtovníctva, vznikla potreba uistiť sa o správnom spracovaní dát v informačný systémoch, čo prinieslo audity informačných systémov.

Vzhľadom na narastajúcu dôležitosť ochrany dát sa určitá časť auditov informačných systémov začala zaoberať špecificky overením požiadaviek bezpečnostných opatrení v informačných systémoch.

Keďže množstvo okolností má dopad na bezpečnosť dát v informačných systémoch, vznikli audity, ktoré pri riadení bezpečnosti nekontrolujú len informačný systém samotný, ale aj spôsob používania, riadenie používateľov, riadenie všetkých aspektov organizácie, ktoré majú vplyv

na bezpečnosť - inými slovami audit bezpečnosti systémov riadenia[1]. Než sa pozrieme na rôzne druhy auditu z pohľadu požiadaviek rôznych noriem, zákonov alebo interných predpisov v organizáciách, ukážeme si najprv, aký má byť audit vo všeobecnosti.

Aký má byť audit

Bez ohľadu na druh auditu, vo všetkých prípadoch má byť audit objektívny, nezávislý a postavený na dôkazoch.

Aký má byť audítor

Ak majú výsledky auditu poskytnúť neskreslený, odborný, objektívny pohľad na organizáciu v rozsahu auditu, kladie to veľké nároky na vlastnosti audítorov. Objektívnosť a etické správanie audítora sú základným predpokladom dôveryhodnosti výsledkov auditu, preto sú veľmi prísne kontrolované a vynucované. V prípade audítorov certifikovaných ako CISA od spoločnosti ISACA je každý audítor povinný dodržiavať etický kódex s rizikom odobratia certifikátu pri neuspokojivom vyšetrovaní porušenia.

Profesionálny etický kódex ISACA

ISACA sformovala tento Profesionálny etický kódex s cieľom viesť členov ISACA a držiteľov certifikátov pri výkone ich profesionálnych a osobných aktivít.

Členovia ISACA a držitelia certifikátov majú:

1. Podporovať implementáciu a odporúčať zhodu s vhodnými štandardmi, postupmi a kontrolnými opatreniami pre informačné systémy.
2. Vykonávať svoje povinnosti objektívne, s primeranou osobnou a profesionálnou starostlivosťou v súlade s profesijnými štandardmi a najlepšími postupmi.
3. Slúžiť zákonnými a čestným spôsobom záujmom vlastníkov a udržiavať vysokú úroveň správania sa a konania a nezapojiť sa do činností, ktoré môžu diskreditovať profesiu.
4. Dodržiavať súkromie a dôvernosť informácií získaných pri plnení povinností pokiaľ nie je ich poskytnutie požadované v súlade legislatívou. Nepoužiť získané informácie vo vlastný prospech a ani ich neposkytnúť iným osobám či subjektom.
5. Udržiavať kvalifikáciu vo svojom odbore a zaviazať sa len k takým aktivitám, o ktorých predpokladajú, že sú dostatočne odborne kompetentný pre ich dokončenie.
6. Informovať príslušné skupiny o výsledkoch práce, oboznámiť ich so všetkými dôležitými informáciami.
7. Podporovať vzdelávanie vlastníkov, manažmentu, klientov a verejnosti pri rozširovaní ich znalostí v oblasti bezpečnosti a riadenia informačných systémov.

Nesplnenie požiadaviek tohto profesionálneho kódexu môže vyústiť do vyšetrovania činností člena alebo držiteľa certifikátu a napokon do disciplinárnych opatrení.[2]

[1] Napr. podľa medzinárodného certifikačného štandardu ISO/IEC 27001

[2] Zdroj: www.isaca.sk

Objektívnosť auditov podľa certifikačných noriem ISO sa zabezpečuje overovaním plnenia akreditačných požiadaviek na certifikačné orgány, ktoré vydávajú certifikáty ISO[3]

Odbornosť audítora

Keďže požiadavky prichádzajú z rôznych zdrojov, audítori potrebujú byť vyberaní z odborníkov na tieto požiadavky. Zároveň musí audítor v organizácii porozumieť súvislostiam. Nestačí len rozumieť činnostiam, na ktoré sa audítor pozerá, musí rozumieť následkom a pochopiť príčiny, vedieť vyhodnotiť dôkazy, ktoré sú pre auditovanú oblasť relevantné. Na to potrebuje mať praktické skúsenosti v odbore, kde vykonáva audit, a zároveň prax a zručnosti pri vyhodnocovaní zozbieraných informácií.

Preto požiadavky na odbornosť audítora stanovujú rôzne systémy certifikácie alebo overenia spôsobilosti. Jedným z najrozšírenejších certifikátov audítorov informačných systémov je medzinárodný certifikát CISA (Certified Information System Auditor) od spoločnosti ISACA[4]
.

Získanie certifikátu CISA predpokladá doloženie vzdelania, požadovanej dĺžky praxe a zloženie certifikačnej skúšky. Certifikačná skúška preveruje vedomosti z 5 oblastí:

Proces auditu informačných systémov

- Štandardy a procedúry auditu IT, profesionálny etický kódex
- Podnikateľské procesy
- Typy opatrení
- Plánovanie auditu na báze rizika
- Typy auditov a posúdení
- Projektové riadenie auditu
- Metodológia vzorkovania
- Techniky zberu auditných dôkazov
- Analýza dát
- Podávanie správ a komunikačné techniky

Governance a riadenie IT

- IT Governance a stratégia IT
- Frameworky súvisiace s IT
- Štandardy, politiky a procedúry IT

[3] pozri podkapitolu Ako funguje certifikácia ISO.
[4] Viac informácií http://www.isaca.sk/certification/certifikacia-cisa/

- Organizačné štruktúry
- Podniková architektúra
- Riadenie rizík v organizácii
- Modely zrelosti
- Zákony, regulácie a odvetvové štandardy ovplyvňujúce organizácie
- Riadenie IT zdrojov
- Akvizícia a riadenie poskytovateľov IT služieb
- Monitorovanie a podávanie správ o výkone IT
- Riadenie kvality IT a poskytovanie uistenia o kvalite IT

Akvizícia, vývoj a implementácia informačných systémov

- Projektové riadenie pri akvizícii a vývoji informačných systémov
- Analýza uskutočniteľnosti a obchodné prípady pri akvizícii a vývoji informačných systémov
- Metodológie vývoja systémov
- Návrh a identifikácia opatrení
- Testovacie metódy pri implementácii informačných systémov
- Riadenie konfigurácií a vydaní
- Migrácie systémov, implementácia infraštruktúry a konverzie dát
- Preskúmanie po implementácii informačných systémov

Prevádzka informačných systémov a odolnosť

- Prevádzka informačných systémov - najbežnejšie komponenty technológie
- Riadenie informačných aktív
- Plánovanie úloh a automatizácia výrobných procesov
- Rozhrania systémov
- Výpočtová technika koncových používateľov
- Dátová Governance
- Riadenie výkonnosti systémov
- Riadenie problémov a incidentov

- Riadenie zmien, konfigurácií, vydaní a bezpečnostných záplat
- Riadenie úrovne IT služieb
- Riadenie databáz
- Odolnosť - analýza dopadov na podnikanie
- Odolnosť systémov
- Zálohovanie, uchovávanie a obnova dát
- Plány kontinuity činností
- Plány obnovy po havárii

Ochrana informačných aktív

- Bezpečnosť a kontrola informačných aktív
- Rámce, štandardy a smernice pre bezpečnosť informácií
- Zásady ochrany osobných údajov
- Fyzický prístup a kontrola prostredia
- Správa identít a prístupu
- Zabezpečenie siete a koncového bodu
- Klasifikácia údajov
- Techniky šifrovania údajov
- Infraštruktúra verejného kľúča (PKI)
- Webové komunikačné techniky
- Virtualizované prostredia
- Mobilné, bezdrôtové a internetové zariadenia (IoT)
- Správa bezpečnostných udalostí
- Školenia a programy na zvýšenie povedomia o bezpečnosti
- Metódy a techniky útoku na informačný systém
- Nástroje a techniky testovania bezpečnosti
- Nástroje a techniky monitorovania bezpečnosti
- Správa reakcie na incidenty
- Zhromažďovanie dôkazov a súdne spory

Pri skúške na audítora CISA sa očakáva demonštrácia pripravenosti plniť úlohy:

- Plánovať audit tak, aby zistil, či sú informačné systémy chránené, kontrolované a či sú pre organizáciu prínosom.
- Vykonávať audit v súlade s audítorskými štandardmi IS a audítorskou stratégiou IS založenou na riziku.
- Poskytovať zainteresovaným stranám informácie o pokroku auditu, zisteniach, výsledkoch a odporúčaniach.
- Vykonať následné audity s cieľom vyhodnotiť, či sa riziká dostatočne riešili.
- Vyhodnotiť stratégiu IT z hľadiska súladu so stratégiami a cieľmi organizácie.
- Zhodnotiť efektívnosť štruktúry riadenia IT a organizačnej štruktúry IT.
- Zhodnotiť riadenie organizácie v oblasti IT politík a postupov.
- Vyhodnotiť politiky a postupy IT v oblasti dodržiavania regulačných a právnych požiadaviek.
- Vyhodnotiť správu IT zdrojov a portfólia z hľadiska súladu so stratégiami a cieľmi organizácie.
- Zhodnotiť zásady a postupy riadenia rizík organizácie.
- Zhodnotiť správu IT a monitorovanie opatrení.
- Vyhodnotiť monitorovanie a podávanie správ o kľúčových ukazovateľoch výkonnosti v oblasti IT.
- Zhodnotiť schopnosť kontinuity činnosti organizácie.
- Posúdiť, či obchodný prípad navrhovaných zmien v informačných systémoch spĺňa obchodné ciele.
- Zhodnotiť, či sú procesy výberu dodávateľov IT a procesy riadenia zmlúv v súlade s obchodnými požiadavkami.
- Zhodnotiť zásady a postupy riadenia projektov v organizácii.
- Vyhodnotiť kontroly vo všetkých fázach životného cyklu vývoja informačných systémov.
- Posúdiť pripravenosť informačných systémov na implementáciu a migráciu do výroby.
- Vykonať kontrolu systémov po implementácii a zistite, či sú splnené výstupy projektu, opatrenia a požiadavky.
- Zhodnotiť, či sa postupy riadenia IT služieb zhodujú s obchodnými požiadavkami.
- Vykonávať pravidelné kontroly informačných systémov a podnikovej architektúry.

- Vyhodnotiť operácie IT, aby ste zistili, či sú efektívne kontrolované, a pokračujte v podpore cieľov organizácie.
- Vyhodnotiť postupy údržby IT, aby ste zistili, či sú efektívne kontrolované, a naďalej podporujú ciele organizácie.
- Zhodnotiť postupy správy databázy.
- Zhodnotiť politiky a postupy správy údajov.
- Vyhodnotiť politiky a postupy riadenia problémov a incidentov.
- Vyhodnotiť politiky a postupy správy zmien, konfigurácií, vydávaní a bezpečnostných záplat.
- Vyhodnotiť bezpečnosť koncových používateľov a určiť, či sú procesy efektívne kontrolované.
- Vyhodnotiť politiky a postupy týkajúce sa informačnej bezpečnosti a ochrany osobných údajov.
- Vyhodnotiť fyzické a environmentálne kontroly a určiť, či sú informačné aktíva primerane chránené.
- Vyhodnotiť logické bezpečnostné opatrenia na overenie dôvernosti, integrity a dostupnosti informácií.
- Vyhodnotiť postupy klasifikácie údajov z hľadiska súladu s politikou organizácie a príslušnými vonkajšími požiadavkami.
- Zhodnotiť politiky a postupy súvisiace so správou životného cyklu aktív.
- Vyhodnotiť program informačnej bezpečnosti, a jeho účinnosť a súlad so stratégiami a cieľmi organizácie.
- Vykonať technické testovanie bezpečnosti na identifikáciu potenciálnych hrozieb a slabých miest.
- Využiť nástroje na analýzu údajov na zefektívnenie procesov auditu.
- Poskytovať konzultačné služby a poradenstvo pre organizáciu s cieľom zlepšiť kvalitu a kontrolu informačných systémov.
- Identifikovať príležitosti na zlepšenie procesov v IT politikách a postupoch organizácie.
- Zhodnotiť potenciálne príležitosti a hrozby spojené s novými technológiami, predpismi a priemyselnými postupmi.

Pri audite podľa požiadaviek ISO noriem sú stanovené požiadavky na kvalifikáciu, zručnosť, prax a odbornosť audítora v normách, ktoré musia dodržiavať akreditované certifikačné orgány ak chcú vydávať certifikáty podľa noriem ISO[5].

[5] pozri podkapitolu Ako funguje ISO certifikácia

Pre auditovanie systémov riadenia informačnej bezpečnosti podľa ISO 27001 sú to požiadavky na certifikačný orgán a správanie jeho audítorov uvedené v norme ISO 27006[6] a ISO 17021-1[7], podľa ktorých musí certifikačný orgán zabezpečiť minimálne, že personál, zúčastňujúci sa na audite, na kontrole auditných správ a rozhodovaní o udelení certifikátu podľa ISO 27001 má vedomosti v oblastiach:

- riadenia a prevádzky
- princípov, postupov a metód auditovania
- znalosti certifikačnej normy
- procesov certifikačného orgánu
- odvetvia klienta auditu
- produktov, procesov a organizácie klienta
- jazykových znalostí potrebných pri audite u klienta
- písania správ a záznamov z auditu
- prezentačných zručností
- vedenia rozhovorov
- riadenia auditu

Nezávislosť audítora

Aby audit mohol objektívne hodnotiť skutočnosti v organizácii, musí byť audítor nepredpojatý. Pretože je veľmi ťažké byť objektívny pri hodnotení vlastných výsledkov a svojej vlastnej práce, väčšina uznávaných postupov auditovania priamo zakazuje audítovať vlastnú prácu audítora. To isté platí pre jeho vlastných nadriadených a podriadených pracovníkov.

13.1.2 Druhy auditu z pohľadu strán auditu

Z pohľadu strán auditu, čo znamená, kto je objednávateľom auditu a pre koho sú určené výsledky, rozlišujeme tri možné situácie:

Audit prvou stranou - Interný audit

Pri internom audite je objednávateľom auditu samotná auditovaná organizácia, spravidla jej vedúci pracovníci. Audit je vykonávaný interne (sami sebou, sami pre seba - prvou stranou). Možno si poviete, že taký audit jednoznačne porušuje zásadu objektívnosti a odbornosti, ktorú sme si pred chvíľou stanovili. Nie je to tak. Interní audítori sú vyberaní tak, aby neauditovali svoju vlastnú prácu a zároveň rozumeli auditovanej oblasti.

[6] ISO 27006 Požiadavky na certifikačné orgány pre audit systémov riadenia informačnej bezpečnosti

[7] ISO/IEC 17021-1:2015 Požiadavky na orgány vykonávajúce audit a certifikáciu systémov manažérstva. Časť 1: Požiadavky

To, že je audit interný, tiež nevyhnutne neznamená, že nemôže byť použitý aj externý odborník. Rozlíšenie, že sa jedná o audit prvou stranou znamená, že aj objednávateľ aj adresát výsledkov auditu je samotná organizácia. Cieľom auditu je spravidla predovšetkým získať pravdivý obraz o plnení požiadaviek v organizácii voči dohodnutému rozsahu. Dohodnutým rozsahom môžu byť požiadavky medzinárodnej normy alebo zákona či interných predpisov.

Audit druhou stranou - Externý audit

Audity druhou stranou znamenajú, že adresátom správy je niektorá zo zainteresovaných strán. Obvykle to býva zákazník alebo investor, ktorý si objedná audit nezávislým audítorom.

Audit treťou stranou - nezávislý externý audit

Audit treťou stranou znamená, že sa jedná o úplne nezávislú audítorskú organizáciu, spravidla certifikačnú autoritu. Od externého auditu druhou stranou sa odlišuje tým, že výsledky nie sú určené pre konkrétneho objednávateľa, ale pre ľubovoľnú zainteresovanú stranu ako sú potenciálni zákazníci, investori, ale aj verejnosť.

Špecifickým, veľmi častým príkladom auditov treťou stranou sú certifikačné alebo štatutárne audity[8]. Certifikačné audity (najčastejšie z oblasti certifikačných ISO noriem) poskytujú uistenie, že organizácia spĺňa ucelený set požiadaviek certifikačných noriem a na znak súladu je vydaný certifikát. Schému vzťahov v rámci certifikačných autorít viď v prílohe Ako funguje certifikácia ISO.

13.1.3 Postup auditu z rôznych pohľadov

Z pohľadu audítora, resp. vedúceho audítora, ide o ďalšiu v rade zákaziek, ktorú je potrebné zahájiť, odriadiť a ukončiť. Prakticky to vyzerá tak, že si audítor najskôr odsúhlasí ciele, náplň a rozsah auditu s vedením spoločnosti.

Ohraničenie rozsahu je pre každý audit kľúčové. Rozsah (angl. scope) auditu dáva audítorovi mandát a zároveň hranice odkiaľ - pokiaľ audituje z pohľadu organizačných jednotiek resp. auditovaných, predmetu auditu, požiadaviek auditu. Rozsah je obvykle dokumentovaný spolu s výsledkami auditu aby čitateľovi výsledkov poskytol pravdivú informáciu, čo bolo skúmané a čo nie.

Po stanovení rozsahu si audítor s vedením preverovanej divízie dohodne termín auditu a čas jeho trvania a prístup na pracoviská a odborné sprevádzanie. Členom audítorskej skupiny určí úlohy a pridelí otázky pre preverovanú oblasť.

Z pohľadu manažmentu je audit ideálna príležitosť, ako ukázať nastavenie a fungovanie organizácie. Realisticky ide o ďalšiu, neštandardnú koordinačnú úlohu nad rámec bežných povinností. Či sa nám to páči alebo nie, audit je významný zásah do každodenného chodu organizácie.

Manažéri musia informovať podriadených zamestnancov o cieľoch, náplni a rozsahu auditu, zabezpečiť zodpovedných pracovníkov na sprevádzanie členov skupiny interných audítorov, poskytnúť skupine interných audítorov všetky potrebné prostriedky, aby bol zaistený efektívny

[8] Štatutárne audity, hlavne finančný audit vychádzajú z požiadaviek zákonov, pre potreby tejto kapitoly sa s nimi už nebudeme zaoberať

a účinný proces auditu, umožniť prístup do pracovných priestorov a k dôkazovým materiálom podľa požiadavky audítorov, spolupracovať s audítormi a umožniť dosiahnuť cieľ auditu, určiť a zahájiť realizáciu opatrení k náprave na základe protokolu o audite a komunikovať s vedúcim skupiny audítorov o akýchkoľvek námietkach, otázkach a problémoch týkajúcich sa auditu.

Príklad smernice interného auditu ISO 27001

Zavedenie plánovaného systému interných auditov má za úlohu permanentne preverovať, či činnosti organizácie stále spĺňajú požiadavky. Na základe zistenej nezhody interným auditom sú prijímané nápravné činnosti.

Audity sú vykonávané podľa plánu interných auditov alebo neplánované. Plánovanie interných auditov zabezpečuje, že minimálne raz za 12 mesiacov sú auditované všetky požiadavky normy ISO 27001.

Neplánované audity môžu byť nariadené z dôvodu vzniku podstatných zmien v organizácii, zmenami v procese, zmenami produktov, služieb alebo potrebou preveriť plnenie nápravných resp. preventívnych činností k náprave.

Neplánovaný audit je možné tiež nariadiť:

- na základe sťažností zákazníka,
- v prípade vzniku pochybnosti, že prvok systému manažérstva informačnej bezpečnosti nemá požadovanú účinnosť,
- ak sa pri meraní a monitorovaní vyskytli výsledky, ktoré svojimi hodnotami nezodpovedajú požadovaným parametrom,
- na potvrdenie, že nápravné činnosti a ostatné prijaté zmeny v systéme manažérstva informačnej bezpečnosti boli vykonané a sú účinné.

Právomoc nariadiť neplánovaný audit má riaditeľ spoločnosti na podnet predstaviteľa manažmentu.

Audity sú plánované na obdobie jedného roka. Plán programu interných auditov schvaľuje predstaviteľ manažmentu spoločnosti. Plánovanie interných auditov pozostáva z určenia auditovaného procesu, pracovníkov preverovaných v rámci procesu, termínu auditu, stanovenia audítorskej skupiny a vedúceho audítora.

Za organizačnú stránku výkonu interných auditov, zostavenie programu auditov, prípravu a výber interných audítorov zodpovedá predstaviteľ manažmentu. Pri zostavovaní skupiny interných audítorov prihliada na požiadavku kvalifikácie interných audítorov - absolvované školenie k výkonu interných auditov – a nezávislosť členov audítorskej skupiny na auditovanom procese.

Audítori resp. audítorský team môže byť menovaný aj z radov externých pracovníkov na základe zmluvy.

Je asi jasné, že z pohľadu preverovaného ide o náročnú úlohu, pri ktorej v organizácii rastie miera stresu – a to aj keď je všetko v najlepšom poriadku. V takých chvíľach je dobré si

pripomenúť základný zmysel auditu z pohľadu organizácie – zistiť a pomenovať reálny stav, nie nachytať niekoho a znevažovať ho.

V priebehu auditu audítor používa rôzne metódy na získanie informácií, ktoré vyhodnocuje pri porovnávaní s požiadavkami.

13.1.4 Možné metódy auditu

Pozorovanie

Pri audite audítor zbiera informácie formou pozorovania prebiehajúcich procesov a vyhodnocovaním získaných dôkazov.

Rozhovory

Pri audite audítor zbiera informácie formou rozhovorov s pracovníkmi zodpovedajúcimi otázky k priebehu procesov, znalosti auditovanej oblasti a logickej previazanosti na získané informácie z iných zdrojov ako sú dokumentácia a pozorovanie.

Analýza dokumentov

Pri analýze dokumentov audítor porovnáva rozsah, obsah, zmysluplnosť a logickú nadväznosť informácií v predložených dokumentoch s požiadavkami.

Vzorkovanie

Pri auditoch často nie je možné vyčerpávajúceho hodnotenie všetkých údajov, nie je možný rozhovor so všetkými pracovníkmi alebo preskúmanie všetkých záznamov. Preto je audítorovi umožnené v rámci metód auditu použiť takzvané vzorkovanie. Napr. výber intervalu dátumov, pre ktorý sa preskúmajú záznamy z logov alebo výber pracovísk, na ktorých prebehne pozorovanie a rozhovory.

13.1.5 Záver auditu

Na konci auditu musí audítor resp. vedúci audítor vykonať záverečné stručné zhodnotenie priebehu auditu počas tzv. záverečného stretnutia. Hlavným účelom tohto rokovania je predložiť zistenia auditu takým spôsobom, aby bolo zaistené, že preverovaný výsledkom auditu jasne rozumie.

V praxi to znamená, že vedúci audítor predloží vedeniu závery skupiny audítorov týkajúce sa efektívnosti systému, zistené silné stránky a slabé miesta v auditovanom procese a vo väzbách na súvisiace procesy.

V prípade zistenia tzv. nezhody[9] túto prerokuje s pracovníkmi zodpovednými za príslušné činnosti.

Zodpovedný pracovník podľa potreby navrhne na základe zistení z auditu okamžite, alebo do dohodnutého termínu písomný podklad pre Nápravné opatrenia, ktorý obsahuje analýzu

[9] Akejkoľvek odlišnosti od auditovaných požiadaviek

príčiny nezhody, vyžadované nápravné činnosti, zodpovedného pracovníka za vykonanie nápravných činností a termín odstránenia nezhody.

Opatrenia k náprave a ďalšie následné audity musia byť vykonané a ukončené v termíne odsúhlasenom preverovaným po konzultácií s audítormi a zaznačenom v zázname z auditu. Opatrenia majú v sebe zahrňovať aj stanovenie termínu a spôsobu verifikácie účinnosti prijatých opatrení voči pôvodnému slabému miestu systému.

Niekedy prichádza k nepochopeniu rolí jednotlivých aktérov. Za stanovenie a zahájenie realizácie nápravných činností, ktoré sú potrebné k odstráneniu nezhody alebo jej príčiny, je zodpovedný nadriadený pracovník preverovanej organizačnej jednotky. Audítor je zodpovedný iba za identifikáciu nezhody. Okrem toho môže na vyžiadanie podať preverovanému odporúčanie k zlepšeniu. Jeho odporúčania nie sú pre preverovaného záväzné.

O vykonanom audite vedúci audítor vyhotoví čistopis Protokolu z auditu a odovzdá ho určenému predstaviteľovi organizácie v termíne dohodnutom počas záverečného stretnutia.

V prípade, že ide o interný audit, kedy je cieľom zistiť stav a zabezpečiť zlepšenia, spravidla úloha audítora končí identifikáciou potrebných opatrení na zlepšenie alebo odstránenie nezhôd.

Ak sa však jedná o zákaznícky audit alebo certifikačných audit, prípadne audit vyžadovaný určitým zákonom, postupy ďalších krokov po zistení nesúladu môžu byť veľmi rôznorodé.

V prípade, že audit si vyžiadal zákazník alebo investor, je len na ich rozhodnutí, ako sa zachová v prípade, že audítor zistil rozpor s dohodnutými požiadavkami. Môže prísť k dohode, že sa nedostatky do určitého času odstránia alebo sa zákazník či investor rozhodnú nepokračovať v rokovaniach, ktoré viedli k auditu.

Pokiaľ je nezhoda s požiadavkami vyhodnotená ako výsledok certifikačného auditu, audítor je viazaný jasnými krokmi vyžadovanými akreditačnými normami, ktoré sú pre certifikačné orgány záväzné. To dáva záruky jednotného a transparentného postupu pre všetkých uchádzačov o certifikát ISO 27001. Pokiaľ je konštatovaná závažná nezhoda, proces certifikácie sa zastavuje až do doby odstránenia dohodnutej s auditovanou organizáciou. Po odstránení nezhody môže prísť k opakovanému auditu alebo sa dohodne len doloženie dôkazu o odstránení nezhody a proces certifikácie pokračuje ďalej. Menej závažné nezhody alebo odporúčania na zlepšovanie môžu byť po dohode a v súlade s internými postupmi certifikačného orgánu ponechané na kontrolu dohľadovým auditom, ktorý je v prípade normy ISO 27001 povinný po roku od certifikačného auditu. V prípade, že by sa auditovaná organizácia počas tohoto obdobia nevenovala odstráneniu nezhody, môže prísť k odňatiu certifikátu.

Na následky nezhôd zistených pri auditoch vychádzajúcich z požiadaviek určitých zákonných predpisov môže byť následkom nepriaznivých zistení napr. pokuta alebo neumožnenie výkonu činnosti, ktorú zákon podmieňuje auditom. Na jednotlivé scenáre sa pozrieme postupne v rámci príkladov takýchto auditov.

13.2 Rôzne príklady auditov bezpečnostných opatrení podľa zdrojov požiadaviek

Cieľom auditu je posúdiť zhodu s požiadavkami. Požiadavky môžu byť stanovené napr. ako rozsah bezpečnostných opatrení určených uznávanou medzinárodnou normou akou je ISO 27001.

Zdroje požiadaviek môžu byť tiež stanovené organizáciou interne napr. v predpisoch platných pre celú medzinárodnú korporáciu a audítorovou úlohou je preveriť, či sú aplikované v každej organizačnej jednotke. Čoraz častejšie sa tiež vyskytujú požiadavky na audit bezpečnostných opatrení v rôznych zákonoch.

13.2.1 Auditované požiadavky pri audite podľa ISO 27001

Pri audite podľa ISO 27001 audítor preveruje súlad vykonávaných činností voči požiadavkám uvedených v kapitolách 4 až 10 normy a povinnej prílohe A.

4. Súvislosti organizácie
   - 4.1 Pochopenie organizácie a jej súvislostí
   - 4.2 Pochopenie potrieb a očakávaní zainteresovaných strán
   - 4.3 Stanovenie rozsahu systému riadenia informačnej bezpečnosti
   - 4.4 Systému riadenia informačnej bezpečnosti

5 Vedenie
   - 5.1 Záväzok vedenia
   - 5.2 Politika
   - 5.3 Organizačné úlohy, zodpovednosti a právomoci

6 Plánovanie
   - 6.1 Opatrenia na riešenie rizík a príležitostí
   - 6.2 Ciele systému riadenia informačnej bezpečnosti a plány k ich dosiahnutiu

7 Podpora
   - 7.1 Zdroje
   - 7.2 Kompetentnosť
   - 7.3 Povedomie
   - 7.4 Komunikácia
   - 7.5 Zdokumentované informácie

8 Prevádzka
   - 8.1 Operatívne plánovanie a riadenie
   - 8.2 Analýza rizík
   - 8.3 Ošetrenie rizík

9 Hodnotenie výkonnosti
   - 9.1 Monitorovanie, meranie, analýzy a hodnotenia
   - 9.2 Interný audit

9.3 Preskúmanie vedením

10 Zlepšovanie

10.1 Nezhody a opatrenia na nápravu

10.2 Neustále zlepšovanie

Okruhy opatrení v povinnej prílohe A normy ISO 27001

A.5 Politiky informačnej bezpečnosti

A.6 Organizácia informačnej bezpečnosti

A.7 Personálna bezpečnosť

A.8 Riadenie aktív

A.9 Riadenie prístupov

A.10 Šifrovanie, kryptografia

A.11 Fyzická bezpečnosť a bezpečnosť prostredia

A.12 Bezpečnosť prevádzky

A.13 Komunikačná bezpečnosť

A.14 Akvizícia, vývoj a údržba informačných systémov

A.15 Riadenie vzťahov s dodávateľmi

A.16 Riadenie incidentov informačnej bezpečnosti

A.17 Aspekty informačnej bezpečnosti na riadenie kontinuity

A.18 Súlad

V rámci uvedených kapitol normy ISO 27001 sú uvádzané minimálne požiadavky na výkon činností v organizácii, ktorá pristupuje k riadeniu informačnej bezpečnosti systémovo. Vo viacerých prípadoch táto certifikačná norma vyžaduje, aby organizácia spracovala tzv. zdokumentované informácie. Audítor počas takého auditu overuje úplnosť požadovanej dokumentácie, čo v prípade ISO 27001 znamená minimálne dokumenty:

- Predmet systému riadenia informačnej bezpečnosti
- Bezpečnostná politika systému riadenia informačnej bezpečnosti
- Postup hodnotenia rizík informačnej bezpečnosti
- Postup ošetrenia rizík informačnej bezpečnosti
- Prehlásenie aplikovateľnosti

- Ciele informačnej bezpečnosti
- Výsledky hodnotenia rizík informačnej bezpečnosti
- Výsledky ošetrenia rizík informačnej bezpečnosti
- Dôkazy výsledkov monitorovania a merania
- Dokumentované informácie určené organizáciou na zaistenie efektívnosti systému
- Dôkazy výsledkov auditov a plánovania auditov
- Dôkazy výsledkov Preskúmania vedením
- Dôkazy v súvislosti s nezhodami a následných činností
- Dôkazy prijatých opatrení na nápravu

Z uvedených dokumentov je pre audit zásadným dokumentom Prehlásenie aplikovateľnosti, nakoľko stanovuje, ktoré oblasti prílohy A organizácia neaplikuje. Kvôli transparentnosti voči zainteresovaným stranám, ktoré sa spoliehajú na certifikáciu systému, sa uvádza verzia a dátum prehlásenia aplikovateľnosti aj na certifikátoch ISO 27001. Pritom je ale pri audite prísne hodnotené, prečo organizácia nejakú časť normy pri svojom systéme neaplikuje. Toto rozhodnutie nemôže byť svojvoľné, nakoľko by tým certifikácia stratila svoj zmysel. Organizácia smie vylúčiť nejakú časť normy len v tom prípade, ak v rámci povahy svojich aktivít taká požiadavka nemá v praxi vôbec žiadne uplatnenie. Zároveň musí toto vylúčenie v dokumente prehlásenie aplikovateľnosti dôkladne zdôvodniť.

Pri auditovaní podľa požiadaviek ISO 27001 sa - hlavne v prípade certifikačných auditov - audítor riadi tiež pokynmi svojho certifikačného orgánu akreditovaného na výkon certifikačných auditov, ktorý je povinný vypracovať certifikačnú schému a metodiky auditovania. Certifikačný orgán má tiež za povinnosť zabezpečiť vhodnosť audítorov zaistením audítora s praxou v oblasti odvetvia auditovaného, čo je predmetom kontroly pri akreditačných auditoch. Prínosným návodom na auditovanie normy ISO 27001 sú aj normy ISO 27007 a ISO 27008. Norma ISO 27007[10] poskytuje návod na auditovanie požiadaviek v kapitolách 4 až 10 normy ISO 27001. Norma ISO 27008[11] poskytuje návod na auditovanie požiadaviek v prílohe A, čiže poskytuje návod na hodnotenie bezpečnostných opatrení.

Auditované požiadavky pri audite podľa ISO 22301

4 Súvislosti organizácie

- 4.1 Pochopenie organizácie a jej kontext
- 4.2 Pochopenie potrieb a očakávaní zainteresovaných strán
- 4.3 Stanovenie rozsahu systému riadenia
- 4.4 Kontinuita systému riadenia

[10] IS0/IEC 27007:2020 Návod na auditovanie systémov riadenia informačnej bezpečnosti
[11] ISO/IEC TS 27008:2019 Návod na hodnotenie opatrení informačnej bezpečnosti

5 Vedenie

- 5.1 Všeobecná časť
- 5.2 Záväzok riadenia
- 5.3 Politika
- 5.4 Organizačné úlohy, zodpovednosti a rávomoci

6 Plánovanie

- 6.1 Opatrenia na riešenie rizika a príležitosti
- 6.2 Ciele a plány kontinuity prevádzky k ich dosiahnutiu

7 Podpora

- 7.1 Zdroje
- 7.2 Kompetencie
- 7.3 Povedomie
- 7.4 Komunikácia
- 7.5 Zdokumentované informácie

8 Prevádzka

- 8.1 Operatívne plánovanie a riadenie
- 8.2 Analýza a hodnotenie rizík
- 8.3 Kontinuita stratégie
- 8.4 Identifikácia a implementácia postupov kontinuity
- 8.5 Cvičenie a testovanie

9 Hodnotenie výkonnosti

- 9.1 Sledovanie, meranie, analýzy a hodnotenia
- 9.2 Interný audit
- 9.3 Preskúmanie vedením

10 Zlepšovanie

- 10.1 Nezhoda, opatrenia na nápravu
- 10.2 Neustále zlepšovanie

Ak sa vám zdá, že sú názvy požiadaviek pre ISO 27001 a ISO 22301 rovnaké, máte pravdu. Jedná sa o tzv. harmonizovaný prístup pri certifikačných normách systémov riadenia, kedy sa pri vydávaní noriem týkajúcich sa systémov riadenia dohodla jednotná štruktúra a jednotná terminológia všeobecných požiadaviek spoločných v rámci rôznych oblastí systémov riadenia. Takže napr. požiadavka na zapojenie vrcholového vedenia je vždy v kapitole 5 alebo ciele v kapitole 6. Tým je uľahčený tzv. integrovaný systém riadenia, ktorý umožňuje jednu spoločnú dokumentáciu, totožné procesy, ale aj skrátenie auditov pri aplikovaní viacerých certifikačných

noriem z rôznych oblastí ako sú napr. systém riadenia kvality podľa ISO 9001, systém environmentálneho riadenia ISO 14001, systém riadenia IT služieb podľa ISO 20000-1 alebo systém riadenia kontinuity podľa ISO 22301.

Pri audite systému riadenia kontinuity podľa ISO 22301 je rozsah minimálnej požadovanej dokumentácie:

- Zoznam zákonných, regulačných a iných požiadaviek
- Predmet systému riadenia kontinuity a zdôvodnenie vylúčení
- Politika systému kontinuity
- Ciele kontinuity
- Dôkazy o kompetentnosti personálu
- Plány a procedúry riadenia kontinuity
- Zdokumentovaná komunikácia so zainteresovanými stranami
- Záznamy o incidentoch, prijatých opatreniach a rozhodnutiach
- Dôkazy výsledkov monitorovania a merania
- Dôkazy výsledkov auditov a plánovania auditov
- Dôkazy výsledkov Preskúmania vedením
- Dôkazy v súvislosti s nezhodami a následných činností
- Dôkazy prijatých opatrení na nápravu

Audítor, ktorý chce audítovať riadenie kontinuity podľa ISO 22301, musí spĺňať okrem všeobecných požiadaviek akreditačnej normy ISO/IEC 17021-1[12], spomínaných pri ISO 27001 ešte aj akreditačnú normu ISO/IEC 17021-6, ktorá uvádza naviac vyžadované znalosti v oblastiach:

- Terminológie riadenia kontinuity
- Kontextu organizácie
- Aplikovateľných zákonov a regulácií
- Previazanosti medzi riadiacimi procesmi kontinuity
- Analýzy dopadov a hodnotenia rizík
- Stratégií riadenia kontinuity
- Riadenia incidentov

[12]ISO/IEC 17021-1:2015 Požiadavky na orgány vykonávajúce audit a certifikáciu systémov manažérstva. Časť 1: Požiadavky

- Plánov kontinuity
- Testovania kontinuity
- Vyhodnocovania výkonnosti systému riadenia kontinuity

13.2.2 Penetračné testovanie ako špecifický druh auditu

Nárastom používania cloudových a webových aplikácií narástli aj dopady pri zneužití zraniteľností takýchto aplikácií. Dopady hackerských útokov alebo únikov dát v dôsledku nedostatočne implementovaných bezpečnostných opatrení môžu byť pre organizácie likvidačné. Jedným z auditov, ktoré pomôžu predchádzať týmto následkom sú aj penetračné testy.

Penetračné testovanie je laicky povedané pokus o hackerský útok penetračným testerom, ktorý bol poverený organizáciou s cieľom overiť odolnosť webovej alebo cloudovej služby. V prípade, že by bol pokus vykonaný bez poverenia organizácie, môže byť vyhodnotený ako o zlomyseľné konanie, ktoré môže byť trestne stíhané.

Metodiku testovania môže penetračný tester pri pokuse o prienik zvoliť akúkoľvek, avšak jedna z najrozšírenejších je testovacia príručka vytvorená organizáciou OWASP na testovanie pri vývoji bezpečných webových aplikácií[13]. OWASP (Open Web Application Security Project) je nezisková organizácia založená v roku 2001 špičkovými odborníkmi na online bezpečnosť. Vznikla s cieľom zvýšiť úroveň zabezpečenia webov a aplikácií[14]. Okrem vytvárania nástrojov, prepájania odbornej komunity a vzdelávacích aktivít, vydáva tiež rebríček najčastejších zraniteľností tzv. OWASP TOP 10, ktoré sa najčastejšie vyskytujú a zároveň sú preto aj najzmysluplnejším zadaním na rozsah testovania pri penetračných testoch.

V roku 2020 boli uvedené ako najčastejšie sa vyskytujúce zraniteľnosti[15] :

- Injection – vkladanie kódu
- Poškodená autentizácia
- Odhalenie citlivých údajov
- Externé entity XML (XXE)
- Poškodené overenie prístupu
- Chybná bezpečnostná konfigurácia
- Cross Site Scripting (XSS)
- Nezabezpečená deserializácia
- Používanie komponentov so známymi zraniteľnosťami
- Nedostatočné logovanie a monitorovanie

[13] https://owasp.org/www-pdf-archive/OWASP_Testing_Guide_-_OWASP_Summit_2011.pdf
[14] https://owasp.org
[15] https://sucuri.net/guides/owasp-top-10-security-vulnerabilities-2020/

CVSS Score	Number Of Vulnerabilities	Percentage
0-1	703	0.60
1-2	914	0.70
2-3	4880	4.00
3-4	4556	3.70
4-5	27455	22.20
5-6	23785	19.30
6-7	17054	13.80
7-8	27369	22.20
8-9	553	0.40
9-10	16185	13.10
Total	123454	100.00
Weighted Average CVSS Score: 6.6		

Tabuľka 13.1: Distribution of all vulnerabilities by CVSS Scores

Možných zraniteľností, ktoré sa pri webových službách môžu vyskytovať, je však oveľa viac. Národná databáza zraniteľností je databáza vlády Spojených štátov amerických obsahujúca dáta pre manažment zraniteľností vydávaná NIST[16] . Protokol SCAP (Security Content Automation Protocol) umožňuje automatizáciu riadenia zraniteľností. Na stránke CVE (Common Vulerabilities and exposures)[17] zverejňujú organizácie z celého sveta[18] zraniteľnosti produktov v dohodnutej forme popisu a ohodnotenia skóre.

V čase písania tohoto textu bolo identifikovaných vyše 123 tisíc zraniteľností a toto číslo sa stále zvyšuje[19], pozri tabuľku 13.1[20]

13.2.3 Audit Cloudových technológií

Cloud Computing sa stáva čoraz rozšírenejšou formou prevádzky IT technológií. Štatistiky nárastu využívania najväčších poskytovateľov služieb Cloud Computingu poukazujú na prevažujúce nesporné výhody nad rizikami, ktoré nepochybne pre organizácie Cloud Computing prináša. Dnes sa za najvýznamnejších svetových poskytovateľov Cloud Computingu považujú spoločnosti Amazon, Google a Microsoft. Pritom história začiatku týchto služieb je vcelku nedávna[21]:

Amazon založil pobočku Amazon Web Services (známa pod skratkou AWS) v auguste 2006. Google spustil do prevádzky beta verziu Google App Engine v apríli 2008. V októbri 2008 Microsoft oznámil službu Microsoft Azure a do prevádzky ju spustil vo februári 2010.

Trhové podiely globálnych hráčov vo februári 2020 podľa spoločnosti Canalys> AWS 32.4%, Azure 17.6%, Google Cloud 6%, Alibaba Cloud 5.4% a ostatné cloudy 38.5%. Pozri 13.2

[16] https://nvd.nist.gov
[17] https://cve.mitre.org/cve/cna.html
[18] označované ako autority CVE – v angličtine CVE Numbering Authorities (CNAs)
[19] https://www.cvedetails.com
[20] Zdroj https://www.cvedetails.com
[21] Správa spoločnosti Canalys uvádza 37% nárast celkových výdajov na Cloud computing v poslednom štvrťroku 2019 na celkový objem 107 miliárd USD za rok 2019. https://www.canalys.com/static/press_release/2020/Canalys---Cloud-market-share-Q4-2019-and-full-year-2019.pdf

Cloud service provider	Q4 2019 (USD billion)	Q4 2019 market share	Q4 2018 (USD billion)	Q4 2018 market share	Annual growth
AWS	9.8	32.4%	7.3	33.4%	33.2%
Microsoft Azure	5.3	17.6%	3.3	14.9%	62.3%
Google Cloud	1.8	6.0%	1.1%	4.9%	67.6%
Alibaba Cloud	1.6	5.4%	1.0	4.4%	71.1%
Others	11.6	38.5%	9.3	42.4%	24.4%
Total	30.2	100.0%	22.0	100.0%	37.2%

Poznámka: Hodnoty boli zaokrúhľované, a preto súčty nemusia dávať presne 100%

Tabuľka 13.2: Worldwide cloud infrastructure spending and anual growth Canalys estimates, Q4 2019

Zdroj: https://medium.com/@jaychapel/aws-vs-azure-vs-google-cloud-market-share-2020-wh

Na Slovensku tento trend potvrdzuje aj vybudovanie tzv. vládneho cloudu predovšetkým pre štátne organizácie[22].

Za nárastom využívania cloudových technológií sú predovšetkým ekonomické výhody, ktoré sa ale môžu prejavovať aj v oblasti zvýšenej bezpečnosti. Ekonomické výhody vychádzajú z úspory z rozsahu, kedy sú vysoké investície do hardvéru, softvéru, personálu, priestorov a vybavenia globálnych dátových centier rozdelené medzi obrovské množstvo zákazníkov. Obchodný model poskytovaných služieb na požiadanie v rozsahu, aký každý zákazník momentálne potrebuje, a platenie len tej časti služieb, ktoré momentálne využíva, formou mesačného alebo ročného predplatného, umožňujú zákazníkom získať prakticky neobmedzenú výpočtovú silu a programové vybavenie za ekonomicky prijateľných podmienok.

Alternatívou sú významné investície do HW a SW, potreba interných pracovníkov, ktorí sa vedia o toto vybavenie postarať, a zabezpečenie dostatočných bezpečnostných opatrení pre tieto interne prevádzkované technológie. Neustály nárast využívania IT v každej oblasti ľudského života i života organizácií naznačuje, že investície do HW a SW, ktoré musia organizácie vynakladať, nebudú klesať.

Zároveň prieskumy ISACA[23] naznačujú problémy organizácií zabezpečiť dostatok kvalifikovaného personálu v oblasti implementácie bezpečnostných opatrení.

Používanie cloudových technológií stavia organizácie do situácie, kedy strácajú kontrolu nad časťou svojich aktív, výmenou za škálovateľnosť, ekonomické úspory ale v niektorých prípadoch aj lepšiu bezpečnosť[24] .

Model zdieľanej zodpovednosti za bezpečnosť a prevádzku jednotlivých častí prevádzkova-

[22] Viac informácií napr. http://www.informatizacia.sk/infrastruktura-ako-sluzba/22844s

[23] Link na prieskum ISACA https://www.isaca.org/go/state-of-cybersecurity-2020

[24] Máloktorá bežná menšia firma môže investovať do bezpečnosti viac než globálni hráči ako Amazon, Google alebo Microsoft

ných technológií ilustruje ENISA vo svojej správe o Cloud Computingu:

IaaS, PaaS a SaaS su najčastejšie modely poskytovania cloudových služieb a označujú rozsah služieb, ktoré si v cloude zákazník kupuje. Zdieľaná zodpovednosť znamená, že ako bezpečne si služby ďalej konfiguruje už je jeho vlastná zodpovednosť. Väčšina poskytovateľov cloudových služieb (anglicky označovaných ako Provider) poskytujú návody na správne a bezpečné používanie služieb, avšak ich aplikácia je vecou pracovníkov zákazníka (anglicky označovaného ako tenant).

IaaS (Infrastructure as a Service)

- čiže v preklade **infraštruktúra ako služba** - cloudovú službu predstavuje poskytovanie virtualizovanej infraštruktúry serverov, úložísk dát a sieťových služieb. Hlavnou výhodou tohto prístupu je, že o celý HW sa stará poskytovateľ. Poskytovateľ sa stará spravidla aj o firmvér a jeho bezpečnostné záplaty, bezpečnosť sieťovej prevádzky a správu

PaaS (Platforma as a Service)

- čiže v preklade **platforma ako služba** -cloudovú službu predstavuje poskytovanie HW a SW platformy, potrebnej na vytvorenie a správu aplikácií. Zákazník môže využívať rôzne časti platformy napr. databázové služby, sieťové služby, služby monitoringu, na správu a vývoj svojich vlastných aplikácií.

SaaS (Software as a Service)

- čiže v preklade **softvér ako služba** - cloudovú službu predstavuje poskytovanie softvéru, vrátane aplikácií, t.j. používatelia využívajú aplikačnú funkcionalitu. Na zákazníkovi zostávajú napr. zodpovednosti za správu používateľov ako aj správu dát, ktoré do aplikácie ukladá.

Samotné nakupovanie týchto vrstiev aplikačnej architektúry od poskytovateľov cloudových služieb nezbavuje zákazníkov - organizácie prevádzkujúce v cloude svoje systémy - zodpovednosti za bezpečnosť svojich dát. Zneužiteľnosť osobných údajov, ale aj konkurenčný boj robia z dát v informačných systémoch zdieľaných v cloude vďačný cieľ kybernetických útokov.

Organizácie, ktoré chcú využiť výhody cloudových technológií, musia zodpovedne pristupovať k rizikám, ktoré to prináša.

Jednou z možností ako preveriť stav bezpečnostných opatrení je aj audit bezpečnostných opatrení pri využívaní služieb cloud computingu.

Auditované požiadavky pri audite cloudových technológií podľa ISO 27017 a CSA

Auditované požiadavky pri audite cloudových technológií podľa ISO 27017

Norma ISO 27017[25] nie je síce zaradená ako oficiálna certifikačná norma, avšak auditovanie voči jej požiadavkám sa stalo významným nástrojom uistenia pre používateľov cloudových služieb. Všetci globálni hráči prezentujú súlad s touto normou overený treťou stranou[26] .

[25] ISO/IEC 27017:2015 Kódex postupov pre riadenie informačnej bezpečnosti založený na ISO / IEC 27002 pre cloudové služby

[26] https://en.wikipedia.org/wiki/ISO/IEC_27017

ISO 27017 poskytuje návody na opatrenia informačnej bezpečnosti uplatniteľné na poskytovanie a využívanie cloudových služieb v nadväznosti na opatrenia uvedené v ISO/IEC 27002 s doplnením dodatočných opatrení k implementácii, ktoré sa konkrétne týkajú cloudových služieb.

Norma poskytuje prehľad očakávaných opatrení a požiadavky na implementáciu pre poskytovateľov cloudových služieb ako aj pre zákazníkov cloudových služieb v súlade s uvedeným modelom zdieľanej zodpovednosti vysvetľovaným v predchádzajúcom texte.

Nad rámec štruktúry opatrení zodpovedajúcich obsahu 37 oblastí opatrení adresovaných v norme ISO 27002[27] sa v rozsiahlom annexe zaoberá ISO 27017 špecifickými 7 usmerneniami pre riadenie bezpečnosti v cloude v oblastiach:

- Rozdelenie zodpovedností medzi poskytovateľom cloudových služieb a cloudovým zákazníkom.
- Odstránenie alebo vrátenie aktív na konci zmluvy.
- Ochrana a oddelenie virtuálneho prostredia zákazníka.
- Konfigurácia virtuálnych počítačov.
- Administratívne postupy spojené s cloudovým prostredím.
- Monitorovanie aktivít zákazníkom cloudu.
- Nastavenie virtuálneho a cloudového sieťového prostredia

Auditované požiadavky pri audite cloudových technológií podľa CSA

Významným nástrojom uistenia pre používateľov cloudových služieb sa stali aj audity podľa požiadaviek CSA (Cloud Security Alliance). CSA je popredná svetová organizácia, ktorá sa venuje definovaniu a zvyšovaniu povedomia o najlepších postupoch, aby pomohla zaistiť bezpečné prostredie cloud computingu. CSA využíva odborné znalosti odborníkov z oblasti priemyslu, asociácií, vlád a ich podnikových a individuálnych členov s cieľom ponúkať výskum, vzdelávanie, certifikáciu, udalosti a produkty špecifické pre oblasť cloudovej bezpečnosti. Aktivity, vedomosti a rozsiahla sieť CSA prospievajú celej komunite ovplyvnenej cloudom – od poskytovateľov a zákazníkov, po vlády, podnikateľov – a poskytujú fórum, prostredníctvom ktorého môžu rôzne strany spolupracovať pri vytváraní a udržiavaní dôveryhodného cloudového ekosystému.

CSA prevádzkuje certifikačný program poskytovateľa zabezpečenia cloudu, CSA Security, Trust & Assurance Register (STAR), trojstupňový program zabezpečovania sebahodnotenia poskytovateľov, audit tretích strán a nepretržité monitorovanie. Program je postavený na princípoch transparentnosti, dôsledného auditu a harmonizácie noriem. Spoločnosti, ktoré používajú STAR, demonštrujú osvedčené postupy a overujú bezpečnostné opatrenia svojich cloudových služieb.

Tri stupne programu zahŕňajú:

[27] ISO 27002 poskytuje návod na ISO 27001 a jej štruktúra zodpovedá nadpisom oblastí opatrení v Annexe A

Na 1. úrovni môžu organizácie deklarovať jedno alebo obe sebahodnotenia bezpečnosti aj súkromia. Na hodnotenie bezpečnosti organizácie používajú maticu na vyhodnotenie a zdokumentovanie svojich bezpečnostných opatrení. Príspevky na posúdenie súkromia sú založené na Kódexe správania GDPR[28].

Na 2. úrovni absolvujú organizácie nezávislý audit treťou stranou pozostávajúci z požiadaviek jednej alebo oboch oblastí – bezpečnosti a súkromia.

Na 3. úrovni je organizácia automatizuje a zverejní svoje bezpečnostné opatrenia a podlieha tak nepretržitému monitoringu.

Register STAR dokumentuje bezpečnostné opatrania a opatrenia ochrany osobných údajov poskytované populárnymi službami cloud computingu. Tento verejne prístupný register umožňuje zákazníkom cloudu hodnotiť svojich poskytovateľov zabezpečenia s cieľom zohľadniť bezpečnosť pri obstarávaní cloudových služieb.

Auditované požiadavky na ochranu súkromia pri audite podľa ISO 27018 a GDPR

Auditované požiadavky podľa ISO 27018

Norma ISO 27018[29] nie je – rovnako ako ISO 27017 – zaradená ako oficiálna certifikačná norma, avšak auditovanie voči jej požiadavkám sa rozširuje spolu so zvyšujúcimi sa nárokmi na ochranu osobných údajov pri využívaní cloudových služieb.[30]

Norma stanovuje všeobecne uznávané ciele, opatrenia a návody na implementáciu opatrení na ochranu informácií umožňujúcich identifikáciu osôb v súlade so zásadami ochrany súkromia uvedenými v norme ISO/IEC 29100 pre verejné cloudové služby.[31]

Tento dokument konkrétne špecifikuje usmernenia založené na ISO/IEC 27002, berúc do úvahy regulačné požiadavky na ochranu osobných údajov, ktoré môžu byť uplatniteľné v kontexte rizík poskytovateľa verejných cloudových služieb.

Norma ISO 27018 je použiteľná pre všetky typy a veľkosti organizácií, vrátane verejných a súkromných spoločností, vládnych subjektov a neziskových organizácií, ktoré poskytujú služby spracovania informácií ako sprostredkovatelia spracúvajúci osobné údaje prostredníctvom cloud computingu na základe zmluvy s prevádzkovateľmi.

Auditované požiadavky podľa GDPR

Nariadenie GDPR v svojom texte predpokladá vznik akreditačných a certifikačným rámcov pre posúdenie súladu pri dodržiavaní požiadaviek na spracovanie osobných údajov v súlade s nariadením.

V praxi sa prípravy na certifikáciu rozbiehajú veľmi pomaly a ani viac než dva roky po vstúpení nariadenia do platnosti nie sú jasné konkrétne postupy pre spoločnosti, ktoré by chceli certifikačným auditom prezentovať zabezpečenie osobných údajov.

[28] https://cloudsecurityalliance.org/star/levels/

[29] ISO/IEC 27018:2015 Kódex postupov pre ochranu osobných údajov vo verejných cloudoch pre spracovateľov osobných údajov

[30] https://en.wikipedia.org/wiki/ISO/IEC_27017

[31] https://www.iso.org/standard/76559.html

Nariadenie od začiatku dáva členským štátom možnosti určiť vlastný rámec pre národné certifikácie alebo odkazuje na zavedený mechanizmus auditu produktov, procesov a služieb podľa nariadenie EU (EC) 765/2008[32], ktorý predstavuje možnosť vykonania certifikačných auditov akreditovanými certifikačnými orgánmi podľa ISO 17065[33]. Mechanizmus akreditácie a certifikácie podľa tohoto európskeho nariadenia popisujeme v nasledujúcej časti.

13.3 Ako funguje certifikácia ISO

Vplyvom veľkého rozvoja používania informačných technológií si dnes spoločnosti ani jednotlivci asi nevedia predstaviť život bez IT služieb. Závislosť firemných procesov ako aj života jednotlivcov na IT technológiách so sebou prináša potrebu zabezpečenia kvalitného a bezpečného poskytovania IT služieb. Kritériami pre definovanie miery kvality alebo bezpečnosti sa stali medzinárodné dokumenty ISO, ktoré v podobe ISO noriem, technických správ, technických špecifikácií alebo verejne dostupných technických špecifikácií poskytujú návody pre poskytovateľov IT služieb alebo základ pre nezávislú certifikáciu. Ako v prípade ostatných typov auditu aj tu platí, že hlavným prínosom akejkoľvek certifikácie podľa certifikačnej normy ISO je poskytnutie nezávislého uistenia cez prísne regulované certifikačné orgány o skutočnostiach dokladajúcich plnenie požiadaviek certifikačnej normy.

13.3.1 Aktéri certifikácie

V rámci nezávislého uisťovania zohrávajú dôležitú úlohu dva aktéri.

Certifikačný orgán:

nezávislá komerčná spoločnosť, ktorej podnikanie je prísne regulované podľa akreditačných pravidiel na základe medzinárodných štandardov platných pre akreditáciu. Napr. v súlade s podmienkami na udržanie si akreditácie musia certifikačné orgány zachovať nezávislosť od certifikovaných subjektov, nesmú im poskytovať poradenstvo a iné. Bez platnej akreditácie nemôže certifikačný orgán vykonávať vydávanie certifikátov. V prípade pozastavenia alebo odobratia akreditácie certifikačnému orgánu sú diskreditované aj certifikáty ním vydané, čo vytvára tlak na certifikačné orgány, aby sa do tejto situácie nedostali. Certifikačné orgány sú v zmysle svojej akreditácie povinné prešetriť sťažnosť na subjekty, ktorým vydali certifikáty, tým je zase vytváraný tlak na možné odobratie certifikátu v prípade porušenia plnenia požiadaviek certifikačných noriem certifikovaným poskytovateľom služieb. Pravidlá pre certifikačné orgány určujú rôzne akreditačné normy. Akreditačné normy sa môžu zaoberať napr. certifikáciou systémov riadenia, certifikáciou produktov, procesov a služieb, prípadne certifikáciou osôb.

Akreditačný orgán:

národný, spravidla štátom riadený orgán zabezpečujúci výkon dohľadu nad dodržiavaním akreditačných pravidiel pre certifikačné orgány. V prípade porušenia požiadaviek výkonu akreditovaných certifikačných spoločností má právo pozastaviť alebo odobrať akreditáciu certifikačnému orgánu jeho akreditáciu a tým právo vykonávať certifikácie. Pre slovenské prostredie je akreditačným orgánom SNAS (Slovenská národná akreditačná služba, viď www.snas.sk) avšak

[32] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32008R0765
[33] ISO/IEC 17065:2012 Požiadavky na orgány vykonávajúce certifikáciu výrobkov, procesov a služieb

Akreditačná norma	Certifikačné normy
ISO/IEC 17021 napr. v prípade certifikácie systémov riadenia	• ISO/IEC 9001 - Systém riadenia kvality • ISO/IEC 27001 - Systém riadenia informačnej bezpečnosti • ISO/IEC 20000-1 Systém riadenia IT služieb • ISO/IEC 22301 Systém riadenia kontinuity
ISO/IEC 17065	EIDAS & ETSI, jedna z uvažovaných možností pri GDPR
ISO/IEC 17024	Certifikácia audítorov kybernetickej bezpečnosti

Tabuľka 13.3: Príklady akreditačných noriem a oblastí certifikácie podľa ISO noriem

pri dodržaní medzinárodných pravidiel pre certifikáciu ako aj lokálnych právnych predpisov je možné, aby

certifikácie slovenských spoločností vykonávali aj zahraničné certifikačné orgány v zmysle svojej akreditácie iným ako slovenským akreditačným orgánom. Býva napr. obvyklé pri medzinárodných organizáciách, že ich slovenská zložka je certifikovaná medzinárodnou certifikačnou organizáciou vybranou na medzinárodnej úrovni.

Požiadavky na certifikáciu určuje tzv. vlastník schémy. Vlastníkom schémy môže byť priamo certifikačný orgán, ktorý určuje podmienky pre certifikovaných alebo je určený napr. zákonom (napr. Zákon č. 272/2016 Z.z. o dôveryhodných službách alebo zákon č. 69/2018 Z.z.o kybernetickej bezpečnosti je to tzv. Orgán dohľadu, ktorým v SR NBÚ). Tieto dve schémy auditovania uvedieme v nasledujúcej časti.

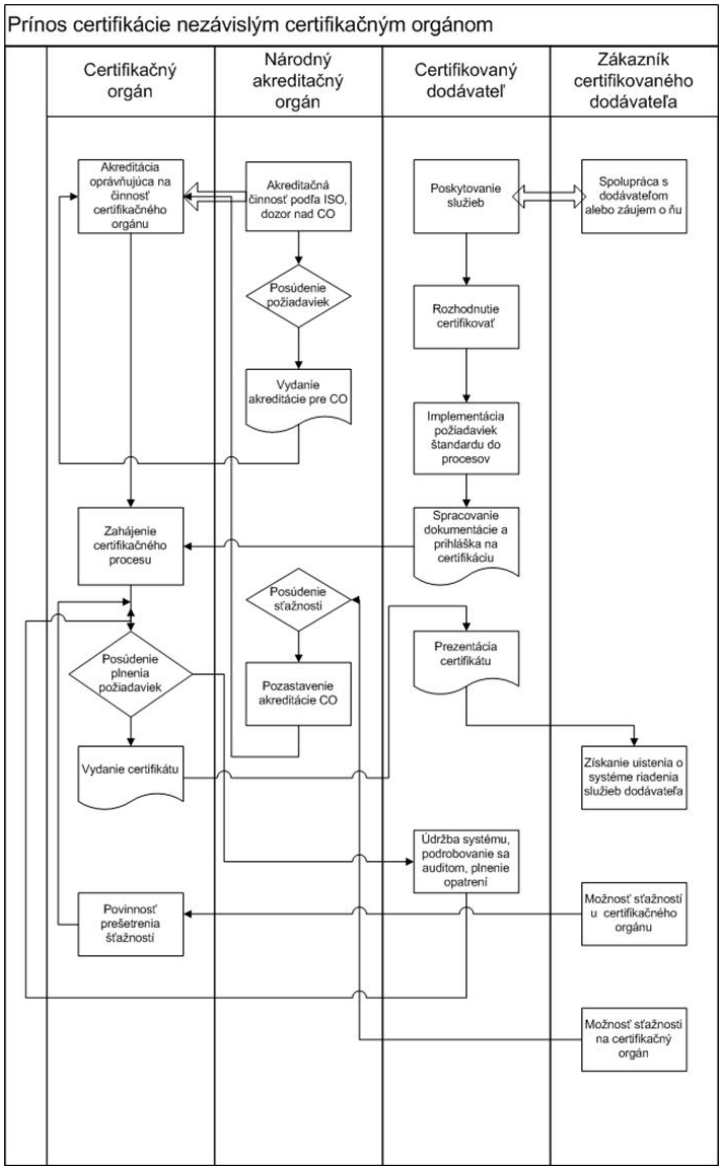
13.4 Audit podľa zákona o kybernetickej bezpečnosti

Prevádzkovatelia základných služieb sú podľa zákona o kybernetickej bezpečnosti č. 69/2018 Z.z. povinní podrobiť sa auditu kybernetickej bezpečnosti a predložiť záverečnú správu o výsledkoch auditu Národnému bezpečnostnému úradu. Audit vykonáva certifikovaný audítor kybernetickej bezpečnosti, ktorému vydal certifikát akreditovaný certifikačný orgán podľa ISO 17024[34]. Požiadavky na prax, vzdelanie, odbornosť určuje vyhláška č. 436/2019 Z.z.. Predpokladom získania certifikátu audítora je splnenie kvalifikačných predpokladov a úspešné vykonanie certifikačnej skúšky.

Prevádzkovateľ základnej služby je povinný preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek vykonaním auditu kybernetickej bezpečnosti do 2 rokov odo dňa zaradenia do registra[35] prevádzkovateľov základných služieb.

[34] ISO/IEC 17024: 2012 Všeobecné požiadavky na orgány vykonávajúce certifikáciu osôb

[35] https://www.nbu.gov.sk/wp-content/uploads/kyberneticka-bezpecnost/prevadzkovatelia-ZS-druhy-bod.htm



Obr. 13.1: Prínos certifikácie

Cieľom auditov kybernetickej bezpečnosti je overiť plnenie bezpečnostných opatrení daných zákonom o kybernetickej bezpečnosti a jeho vyhláškami.

Vyhláška č. 436/2019 Z.z. určuje aj spôsob výpočtu časového rozsahu trvania auditu kybernetickej bezpečnosti. Dĺžka trvania auditu závisí od počtu pracovníkov, ktorí sa zúčastňujú na prevádzkovaní informačných systémov a systémov bezpečnostných opatrení, ktoré podporujú činnosť základnej prevádzkovanej služby. Počet pracovníkov, ktorí musia byť pri audite súčinní, je zásadným faktorom určenia dĺžky auditu avšak audítor má k dispozícii aj možné metódy zníženia alebo zvýšenia počtu dní trvania auditu, aby mal dostatočný časový priestor na zistenie súladu alebo nesúladu opatrení.

Postup certifikácie je uvedený v certifikačnej schéme[36], ktorú vydáva Úrad ako orgán dohliadajúci na kybernetickú bezpečnosť zo zákona.

Auditom sa identifikujú nedostatky pri zabezpečovaní kybernetickej bezpečnosti prevádzkovateľom základnej služby s cieľom prijať opatrenia na ich odstránenie a nápravu a na predchádzanie kybernetickým bezpečnostným incidentom.

Výsledkom auditu je záverečná správa. Prevádzkovateľ základnej služby je povinný ju predložiť úradu spolu s opatreniami na nápravu a s lehotami na ich odstránenie do 30 dní od ukončenia auditu. Súčasťou záverečnej správy je aj kontrolný záznam, ktorý obsahuje súbor požiadaviek podľa zákona a jeho vykonávacích predpisov. V kontrolnom zázname audítor uvádza najmä súlad alebo nesúlad s požiadavkami na implementované bezpečnostné opatrenia, zistenia auditu pre jednotlivé požiadavky, získané dôkazy podporujúce uvedené zistenia a referenciu na použitú metódu overenia. Úrad na základe správ môže udeľovať pokuty za porušenia zákonných požiadaviek alebo nariadiť vykonanie vlastného auditu Úradom.

13.5 Auditované požiadavky pri audite prevádzkovateľov dôveryhodných služieb

V kontexte nariadenia eIDAS[37] sa ako dôveryhodné označujú elektronické služby[38] :

- vyhotovovania, overovania a validácie elektronických podpisov, elektronických pečatí alebo elektronických časových pečiatok, elektronických doručovacích služieb pre registrované zásielky a certifikátov, ktoré s týmito službami súvisia
- vyhotovovania, overovania a validácie certifikátov pre autentifikáciu webových sídiel
- uchovávania elektronických podpisov, pečatí alebo certifikátov, ktoré s týmito službami súvisia.

Zákon č. 272/2016 Z. z. o dôveryhodných službách[39] pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách) určuje povinnosti pre kvalifikovaných poskytovateľov dôveryhodných služieb.

Kvalifikovaná dôveryhodná služba je dôveryhodná služba, ktorá spĺňa uplatniteľné požiadavky[40] stanovené v nariadení eIDAS. Ak sa poskytovateľ dôveryhodných služieb uchádza o kvalifikovaný štatút, jednou z podmienok je vykonanie bezpečnostného auditu raz za 24 mesiacov akreditovaným certifikačným orgánom podľa požiadaviek ISO 17065 v súlade s certifikačnou schémou vydanou Úradom[41]. Výslednú správu z bezpečnostného auditu odovzdáva kandidát na kvalifikovaného poskytovateľa dôveryhodných služieb na NBÚ do 30 dní od vykonania auditu. NBÚ ako orgán dohľadu v súlade so schémou dohľadu[42] rozhodne o tom, či

[36] https://www.nbu.gov.sk/wp-content/uploads/kyberneticka-bezpecnost/NBU-Certifikacna_schema_20200319_v3.4.pdf

[37] Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES

[38] https://www.nbu.gov.sk/doveryhodne-sluzby/index.html

[39] https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2016/272

[40] http://ep.nbu.gov.sk/kca/tsl/PoziadavkyPrevadzkyTSP.pdf

[41] http://ep.nbu.gov.sk/kca/tsl/CertifikacnaSchemaNBU.pdf

[42] https://www.nbu.gov.sk/doveryhodne-sluzby/dohlad/index.html

kandidát spĺňa požiadavky na zapísanie medzi kvalifikovaných[43] poskytovateľov dôveryhodných služieb.

13.6 Audit podľa audítorských štandardov ISACA

ISACA vyžaduje od audítorov dodržiavanie audítorských štandardov IS na zabezpečenie úplnosti a spoľahlivosti výsledkov auditu. Tieto definujú povinné požiadavky na audit informačných systémov a podávanie. Asociácia pre audit informačných systémov (ISACA) poskytuje audítorskej komunite usmernenie vo forme návodov, štandardov a politík špecifických pre audit informačných systémov[44].

Existuje:

- 8 všeobecných štandardov,
- 7 výkonnostných štandardov a
- 2 štandardy na podávanie správ
- 8 všeobecných návodov
- 8 výkonnostných návodov a
- 2 návody na podávanie správ

Súčasťou štandardov a návodov sú aj auditné nástroje a techniky.

Dodržiavanie audítorských štandardov sú pri audite informačných systémov pre držiteľov certifikátov CISA povinné a akékoľvek odchýlky sa musia dokumentovať.

Všeobecné štandardy:

- 1001 Mandát auditu
- 1002 Organizačná nezávislosť
- 1003 Profesijná nezávislosť
- 1004 Primerané očakávania
- 1005 Odborná starostlivosť
- 1006 Zručnosť
- 1007 Tvrdenia
- 1008 Kritériá

Výkonnostné štandardy:

[43] https://www.nbu.gov.sk/doveryhodne-sluzby/doveryhodne-zoznamy/index.html
[44] https://www.isaca.org/bookstore/audit-control-and-security-essentials/witaf

- 1201 Plánovanie zákaziek
- 1202 Posúdenie rizika pri plánovaní
- 1203 Výkon a dohľad
- 1204 Významnosť
- 1205 Dôkazy
- 1206 Používanie práce iných expertov
- 1207 Nezrovnalosti a nezákonné činy

Štandardy na podávanie správ

- 1401 Reporting
- 1402 Následné činnosti

Všeobecné návody

- 2001 Mandát auditu
- 2002 Organizačná nezávislosť
- 2003 Profesionálna nezávislosť
- 2004 Primerané očakávania
- 2005 Odborná starostlivosť
- 2006 Zručnosť
- 2007 Tvrdenia
- 2008 Kritériá

Výkonnostné návody

- 2201 Plánovanie zákaziek
- 2202 Posúdenie rizika v plánovaní auditu
- 2203 Výkon a dohľad
- 2204 Významnosť
- 2205 Dôkaz
- 2206 Používanie práce iných expertov

- 2207 Nezrovnalosti a nezákonné akty
- 2208 Vzorkovanie

Návody pre podávanie správ

- 2401 Podávanie správ
- 2402 Následné činnosti

Text štandardov a návodov na auditovanie je organizovaný tak, aby bolo zrejmé, ktorá časť textu je záväzná a ktorá poskytuje návod. Záväzná časť textu platí pre štandardy, čo sú spravidla krátke stručné tvrdenia určujúce povinnosti pri výkone auditu. Následne sú pri každom z týchto štandardov uvedené kľúčové aspekty a ďalšie pojmy umožňujúce pochopenie požiadavky. Tiež je uvedená referencia na návod, ktorý pomáha premietnuť požiadavku do praxe. Štandardy a návody sa neustále vyvíjajú spolu s tým, ako sa vyvíja auditovaná oblasť - informačné systémy. Preto je pri každom štandarde a návode uvedený dátum platnosti. Štandardy a návody sú k dispozícii bezplatne na stiahnutie na webovom sídle ISACA[45] .

13.7 Prílohy

13.7.1 Pojmy

audit

[46] Nezávislé formálne preskúmanie reálneho stavu systému (organizácie) oproti želanému stavu, definovanému napr. zákonom, štandardom, bezpečnostnou politikou alebo nejakým interným dokumentom organizácie. Bezpečnostný audit je zameraný na posúdenie adekvátnosti bezpečnostných opatrení, na zistenie súladu s ustanovenými politikami a prevádzkovými postupmi a overenie skutočného stavu systému oproti želanému stavu. Výsledkom bezpečnostného auditu je vyjadrenie miery zhody so želaným stavom a odporúčania nevyhnutných zmien opatrení, politík a procedúr s cieľom vyhodnotiť a zlepšiť účinnosť a efektívnosť riadenia rizík a riadiacich a kontrolných procesov. Audit ako: Vytváranie záznamov o bezpečnostne relevantných činnostiach v systéme

13.7.2 Opatrenia a ciele opatrení podľa prílohy A ISO 27001:2013

Tabuľka 13.4: Referenčný zoznam opatrení a cieľov opatrení

číslo	**Názov podľa prílohy A ISO 27001:2013**
A.5	Politiky informačnej bezpečnosti
A.5.1	Usmernenie pre informačnú bezpečnosť
A.5.1.1	Politiky informačnej bezpečnosti

[45] https://www.isaca.org/bookstore/audit-control-and-security-essentials/witaf

[46] Slovník Olejár a kol. 2015 definuje dva významy pojmu audit: 1. Nezávislé formálne preskúmanie reálneho stavu systeému (organizácie) oproti želanému stavu, definovanému napr. zákonom, štandardom, bezpečnostnou politikou alebo nejakým interným dokumentom organizácie. 2. Vytváranie záznamov o bezpečnostne relevantných činnostiach v systéme

A.5.1.2	Preskúmanie politiky informačnej bezpečnosti
A.6	Organizácia informačnej bezpečnosti
A.6.1	Vnútorná organizácia
A.6.1.1	Roly a zodpovednosť v informačnej bezpečnosti
A.6.1.2	Oddelenie právomocí
A.6.1.3	Kontakty s orgánmi moci
A.6.1.4	Kontakt so špeciálnymi záujmovými skupinami
A.6.1.5	Informačná bezpečnosť v projektovom riadení
A.6.2	Mobilné zariadenia a práca na diaľku
A.6.2.1	Politika pre mobilné zariadenia
A.6.2.2	Práca na diaľku
A.7	Personálna bezpečnosť
A.7.1	Pred nástupom do zamestnania
A.7.1.1	Preverovanie
A.7.1.2	Pracovná náplň a podmienky zamestnania
A.7.2	Počas zamestnania
A.7.2.1	Manažérska zodpovednosť
A.7.2.2	Povedomie o informačnej bezpečnosti, vzdelávanie a školiaca činnosť
A.7.2.3	Disciplinárny proces
A.7.3	Ukončenie a zmena zamestnania
A.7.3.1	Zodpovednosti pri ukončení alebo zmene zamestnania
A.8	Riadenie aktív
A.8.1.1	Inventárny zoznam aktív
A.8.1.2	Vlastníctvo aktív
A.8.1.3	Prijateľné používanie aktív
A.8.1.4	Vrátenie aktív
A.8.2	Klasifikácia informácií
A.8.2.1	Klasifikácia informácií
A.8.2.2	Označovanie informácií
A.8.2.3	Zaobchádzanie s aktívami
A.8.3	Zaobchádzanie s médiam
A.8.3.1	Riadenie prepisovateľných médií
A.8.3.2	Likvidácia médií
A.8.3.3	Fyzický prenos médií
A.9	Riadenie prístupov
A.9.1	Požiadavky na riadenie prístupov
A.9.1.1	Politika riadenia prístupov
A.9.1.2	Prístup do sietí a sieťových služieb
A.9.2	Riadenie používateľských prístupov
A.9.2.1	Registrácia a deregistrácia používateľov
A.9.2.2	Poskytovanie používateľských prístupov
A.9.2.3	Riadenie privilegovaných prístupov
A.9.2.4	Riadenie utajených autentizačných údajov
A.9.2.5	Preskúmanie prístupových práv

A.9.2.6	Odstránenie alebo prispôsobenie prístupových práv
A.9.3	Zodpovednosť používateľov
A.9.3.1	Používanie utajených autentizačných údajov
A.9.4	Riadenie systémových a aplikačných prístupov
A.9.4.1	Obmedzenie prístupu k informáciám
A.9.4.2	Bezpečné postupy prihlasovania
A.9.4.3	Systém riadenia hesiel
A.9.4.4	Používanie privilegovaných programov
A.9.4.5	Riadenie prístupu k zdrojovým kódom programu
A.10	Šifrovanie, kryptografia
A.10.1	Riadenie šifrovania
A.10.1.1	Politika pri používaní opatrení na šifrovanie
A.10.1.2	Riadenie šifrovacích kľúčov
A.11	Fyzická bezpečnosť a bezpečnosť prostredia
A.11.1	Zabezpečené oblasti
A.11.1.1	Perimeter fyzickej bezpečnosti
A.11.1.2	Riadenie fyzických prístupov
A.11.1.3	Zabezpečenie kancelárií, miestností a prostriedkov
A.11.1.4	Ochrana pred externými hrozbami a hrozbami prostredia
A.11.1.5	Práca v zabezpečených priestoroch
A.11.1.6	Priestory pre nakladanie a vykladanie
A.11.2	Bezpečnosť zariadení
A.11.2.1	Umiestnenie zariadení a ich ochrana
A.11.2.2	Podporné služby
A.11.2.3	Bezpečnosť kabeláže
A.11.2.4	Údržba zariadení
A.11.2.5	Odstránenie aktív
A.11.2.6	Bezpečnosť zariadení mimo organizácie
A.11.2.7	Bezpečné vyradenie alebo opätovné používanie zariadení
A.11.2.8	Neobsluhované zariadenia
A.11.2.9	Politika čistého stola a prázdnej obrazovky
A.12	Bezpečnosť prevádzky
A.12.1	Prevádzkové postupy a zodpovednosť
A.12.1.1	Dokumentované prevádzkové postupy
A.12.1.2	Riadenie zmien
A.12.1.3	Riadenie kapacít
A.12.1.4	Oddelenie vývoja, testovania a prevádzkového prostredia
A.12.2	Ochrana pred škodlivým kódom
A.12.2.1	Opatrenia proti škodlivému kódu
A.12.3	Zálohovanie
A.12.3.1	Zálohovanie informácií
A.12.4	Zaznamenávanie dát a monitorovanie
A.12.4.1	Zaznamenávanie udalostí
A.12.4.2	Ochrana záznamov informácií

A.12.4.3	Záznamy činnosti správcov a operátorov
A.12.4.4	Synchronizácia času
A.12.5	Riadenie operačného softvéru
A.12.5.1	Inštalácia softvéru na operačné systémy
A.12.6	Riadenie technickej zraniteľnosti
A.12.6.1	Riadenie technickej zraniteľnosti
A.12.6.2	Obmedzenia pri inštalácii softvéru
A.12.7	Audit informačných systémov
A.12.7.1	Opatrenia auditu informačných systémov
A.13	Komunikačná bezpečnosť
A.13.1	Riadenie bezpečnosti v sieťach
A.13.1.1	Sieťové opatrenia
A.13.1.2	Bezpečnosť sieťových služieb
A.13.1.3	Oddeľovanie sietí
A.13.2	Prenos informácií
A.13.2.1	Politiky a postupy pri prenose informácií
A.13.2.2	Dohody o výmene informácií
A.13.2.3	Výmena elektronických správ
A.13.2.4	Zmluvy o dôvernosti alebo utajení
A.14	Akvizícia, vývoj a údržba informačných systémov
A.14.1	Bezpečnostné požiadavky na informačné systémy
A.14.1.1	Analýza a špecifikácia bezpečnostných požiadaviek
A.14.1.2	Zabezpečenie aplikačných služieb vo verejných sieťach
A.14.1.3	Ochrana pri transakciách aplikačných služieb
A.14.2	Bezpečnosť pri vývoji a pri podporných procesoch
A.14.2.1	Politika bezpečného vývoja
A.14.2.2	Postupy riadenia systémových zmien
A.14.2.3	Technické preskúmanie aplikácií po zmene operačného systému
A.14.2.4	Obmedzenia zmien v softvérových balíkoch
A.14.2.5	Princípy bezpečného vývoja systému
A.14.2.6	Prostredie na bezpečný vývoj
A.14.2.7	Vývoj externými zdrojmi
A.14.2.8	Bezpečné testovanie systémov
A.14.2.9	Akceptačné testy systémov
A.14.3	Testovacie údaje
A.14.3.1	Ochrana testovacích údajov
A.15	Riadenie vzťahov s dodávateľmi
A.15.1	Informačná bezpečnosť vo vzťahoch s dodávateľmi
A.15.1.1	Politika informačnej bezpečnosti na vzťahy s dodávateľmi
A.15.1.2	Určenie bezpečnosti v zmluvách s dodávateľmi
A.15.1.3	Dodávateľské reťazce informačných a komunikačných technológií
A.15.2	Riadenie dodávateľských služieb
A.15.2.1	Monitorovanie a preskúmanie dodávateľských služieb
A.15.2.2	Riadenie zmien v službách dodávateľa

A.16	Riadenie incidentov informačnej bezpečnosti
A.16.1	Riadenie incidentov informačnej bezpečnosti a zlepšovania
A.16.1.1	Zodpovednosť a postupy
A.16.1.2	Informovanie o udalostiach informačnej bezpečnosti
A.16.1.3	Informovanie o slabinách informačnej bezpečnosti
A.16.1.4	Posúdenie udalostí informačnej bezpečnosti a rozhodnutia o nich
A.16.1.5	Odpoveď na incidenty informačnej bezpečnosti
A.16.1.6	Poučenie z incidentov informačnej bezpečnosti
A.16.1.7	Zber dôkazov
A.17	Aspekty informačnej bezpečnosti na riadenie kontinuity
A.17.1	Kontinuita informačnej bezpečnosti
A.17.1.1	Plánovanie kontinuity informačnej bezpečnosti
A.17.1.2	Implementovanie kontinuity informačnej bezpečnosti
A.17.1.3	Overenie, preskúmanie a vyhodnotenie kontinuity informačnej bezpečnosti
A.17.2	Redundancia
A.17.2.1	Dostupnosť zariadení na spracúvanie informácií
A.18	Súlad
A.18.1	Súlad s právnymi a zmluvnými požiadavkami
A.18.1.1	Identifikácia platnej legislatívy a zmluvných požiadaviek
A.18.1.2	Práva duševného vlastníctva
A.18.1.3	Ochrana záznamov
A.18.1.4	Súkromie a ochrana osobných údajov
A.18.1.5	Nariadenie o šifrovacích opatreniach
A.18.2	Preskúmanie informačnej bezpečnosti
A.18.2.1	Nezávislé preskúmanie informačnej bezpečnosti
A.18.2.2	Súlad s bezpečnostnými politikami a normami
A.18.2.3	Preskúmanie technického súladu

Kapitola 14

Forenzná analýza počítačových systémov

Peter Pištek

14.1 Úvod

Forenzná analýza nie je novou vedeckou disciplínou a prvé známky jej použitia boli už v starovekej Čine pred niekoľkými tisíckami rokov [28]. Už vtedy sa používali odtlačky prstov na validovanie dokumentov. Postupne sa táto disciplína vyvíjala v čase, kde významne prispel Edmond Lockard, ktorý presadzoval používanie vedeckých metód pri kriminálnom vyšetrovaní. Známym sa stal aj so svojím princípom výmeny [1]:

> Kedykoľvek dva objekty prídu navzájom do kontaktu, tak nastane medzi nimi výmena materiálu alebo informácie.
>
> Edmond Lockard

Forenzná analýza počítačových systémov (ako podmnožina forenznej analýzy) je výrazne mladšia. Jej vznik sa datuje približne 35 rokov dozadu, kedy v USA začali zodpovedné zložky pozorovať rastúcu tendenciu v počte kriminálnych činov súvisiacich s počítačmi (tzv. „e-zločiny“). V roku 1984 zriadila FBI pod vedením Michaela Andersona Magnetic Media Program [1], v dnešnej dobe známejší ako CART (Computer Analysis and Response Team). Neskôr v roku 1997 krajiny G8 založili svoju podskupinu orientovanú na high-tech kriminalitu [28]. V rámci tejto skupiny, experti prvýkrát prediskutovali Princípy počítačovej forenznej analýzy.

Spolu s nárastom využívania výpočtových prostriedkov, ktoré sú zároveň čoraz viac prepojené prostredníctvom počítačových sietí, nastáva výrazný rozvoj forenznej analýzy počítačových systémov. Vznikajú nové smernice, laboratória, či takzvané CERT/CSIRT tímy na národných úrovniach. So narastajúcim uvedomením si hodnoty duševného vlastníctva, ale aj z dôvodu ochrany osobných údajov sa stávajú tieto tímy v dnešnej dobe nevyhnutnou súčasťou už aj firemného prostredia (napríklad pri dokazovaní porušenia podmienok kontraktu alebo firemnej politiky). Dopyt po expertoch v doméne forenznej analýzy počítačových systémov však

dnes výrazne prekračuje možnosti trhu práce, ako aj možnosti vzdelávacieho systému. Viaceré univerzity vo svete posilňujú predmety s týmto zameraním, prípadne rozbiehajú celé študijné programy so zameraním na počítačovú bezpečnosť.

Ako sme už naznačili, s forenznou analýzou počítačových systémov sa môžeme stretnúť pri kriminálnych vyšetrovaniach (štát), pri porušeniach firemných pravidiel a politík (korporácie) alebo pri súkromnom hľadaní odpovedí (fyzické osoby).

14.1.1 Druhy forenznej analýzy počítačových systémov

Poznáme viacero kategorizácií druhov digitálnej forenznej analýzy. Z hľadiska stavu vyšetrovaného systému môžeme použiť rozdelenie:

Post mortem – predmetom vyšetrovania sú systémy, ktoré boli nájdené vypnuté, alebo po zhodnotení možností a vykonaní niektorých krokov boli vypnuté.

Živá – forenzná analýza je aplikovaná na bežiace systémy. Ich vypnutím by sa mohli stratiť niektoré dôležité dôkazy (napríklad v operačnej pamäti).

Z hľadiska konkrétneho zamerania na jednotlivé časti digitálnych zariadení vieme rozlišovať forenznú analýzu:

- Počítačov / systémov.
- Počítačových sietí (aj v prostredí cloudu).
- Mobilných zariadení (Android, IOS a i.).
- Digitálnych obrázkov, audio a videozáznamov.
- Pamäte (stále a nestále pamäte).

Podľa častí, na ktoré sa zameriavame sa môžeme presúvať medzi rôznymi vrstvami abstrakcie (od konkrétnej časti v počítači až po úroveň aplikácií), napríklad:

1. Forenzná analýza počítačov.
2. Forenzná analýza pevných pamätí.
3. Forenzná analýza súborových systémov.
4. Forenzná analýza operačných systémov.
5. Forenzná analýza webových prehliadačov.

Vyšetrovanie v rámci forenznej analýzy môže, ale nemusí začínať prvým bodom. Každý bod má svoje špecifiká z hľadiska získavania a zabezpečenia dôkazov ako aj samotného vyšetrovania.

14.2 Forenzná analýza

Vo všeobecnosti možno forenznú analýzu chápať ako aplikovanie vedeckých metód na získanie faktických odpovedí na právne problémy. Snahou forenzného analytika je pokúsiť sa o rekonštrukciu zločinu alebo incidentu, prostredníctvom určenia akcií a udalostí, ktoré súvisia so spáchaným zločinom.

Počas vyšetrovania sa snaží systematicky identifikovať a odhaľovať overiteľné fakty. Vychádzajúc z práce [41] štandardne používame tzv. „5WH prístup“ (z angličtiny: “who” – kto, “where” – kde, “when” – kedy, “what” – čo, “why” – prečo a “how” – ako), ktorá definuje tieto ciele vyšetrovania:

Kto (Who) – osoby zahrnuté vo vyšetrovaní (vrátane svedkov, podozrivých, či obetí).

Kde (Where) – miesto, ktoré sa spája so zločinom alebo iné relevantné miesta.

Kedy (When) – čas, ktorý sa spája so zločinom a ostatnými udalosťami, ktoré predchádzali alebo nasledovali po zločine.

Čo (What) – opis faktov viažucich sa k zločinu.

Prečo (Why) – zdôvodnenie motivácie k zločinu a prečo sa stal v danom čase.

Ako (How) – ako bol zločin spáchaný.

V prípade forenznej analýzy počítačových systémov hovoríme o digitálnom vyšetrovaní, ktoré používa vedecky odvodené a overené metódy zamerané na zachovanie, zaistenie, validáciu, identifikáciu, analýzu, interpretáciu, dokumentáciu a prezentáciu digitálnych dôkazov. Tieto dôkazy sú odvodené z digitálnych zdrojov za účelom uľahčenia a ďalšej rekonštrukcie zločinu alebo bezpečnostného incidentu a udalostí, ktoré s nimi súvisia. Použitie dôkazov môže byť aj za účelom predvídania neautorizovaných aktivít, ktoré môžu narúšať priebeh štandardných, plánovaných operácií [36].

14.2.1 Digitálna stopa a digitálny dôkaz

Základným rozdielom medzi digitálnou stopou a digitálnym dôkazom je, že [40]:

Digitálne stopy sú všetky dáta, ktoré sú spracovávané, uchovávané alebo prenášané prostredníctvom digitálnych zariadení a môžu súvisieť s prešetrovaným prípadom.

Digitálne dôkazy [5] sú ľubovoľné digitálne stopy, ktoré obsahujú relevantné a spoľahlivé informácie, ktoré môžu podporovať alebo vyvracať hypotézu viažucu sa k bezpečnostnému incidentu alebo zločinu. Digitálny dôkaz je možné predložiť súdu.

Blízky pojem k digitálnemu dôkazu je elektronický dôkaz, ktorý môže byť definovaný ako: elektronicky uložená informácia, ktorá je uznaná ako dôkaz počas súdu alebo vypočúvania [20]. Digitálne stopy, či dôkazy poskytujú digitálne zariadenia, najčastejšie počítače, komponenty informačných systémov, nosiče údajov, digitálne prenosy údajov, digitálne záznamy (fotografie,

videa) a iné. Vôbec nemusí záležať na tom, či sa jedná o niekoľko gigabajtové dokumenty alebo len o jeden konkrétny bit.

Digitálne dôkazy treba vnímať v kontexte viacerých úrovní abstrakcie. Základnú – binárnu úroveň majú spoločnú všetky. Ako príklad si môžeme predstaviť obnovu zmazaného disku na binárnej úrovni tak, aby sme v obnovenom súborovom systéme dokázali zo súboru, ktorý sa viaže k e-mailovému klientovi, obnoviť mail, ktorý obsahuje konkrétnu prílohu medzi konkrétnymi dvoma používateľmi. Podobný príklad si môžeme predstaviť aj v rámci dobre známeho RM-OSI modelu[1].

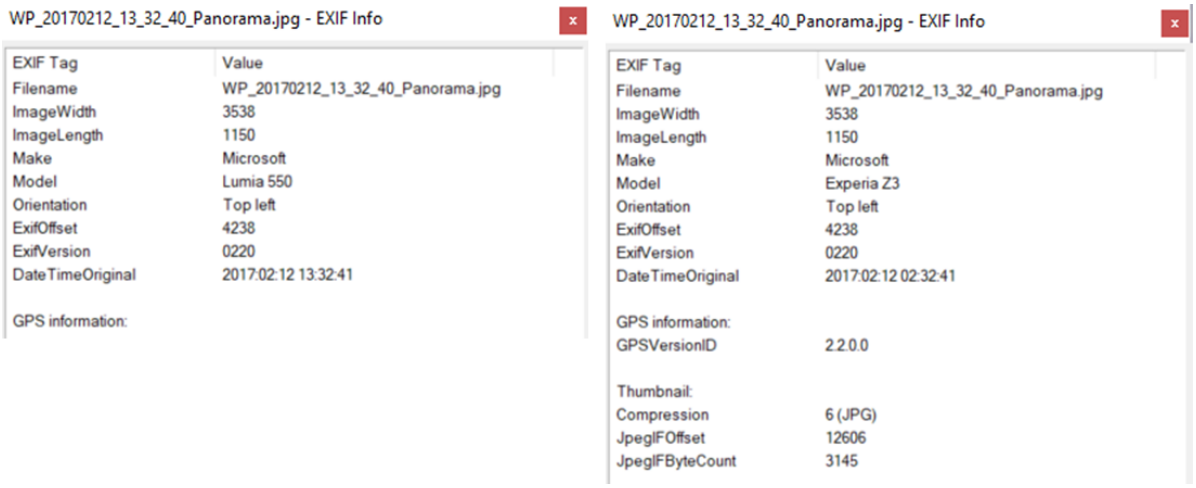
Významným zdrojom digitálnych dôkazov môžu byť metadáta (tzv. „údaje o údajoch“), ktoré obsahujú informácie o údajoch. Napríklad metadáta viažuce sa k digitálnej fotografii môžu obsahovať čas zhotovenia fotografie, GPS súradnice, informácie o fotoaparáte. Ak máme k dispozícii fotografiu Ríma na obrázku 14.1, vieme si k nej pozrieť jej metadáta, z ktorých sa môžeme snažiť získať ďalšie informácie.

Obr. 14.1: Ukážka digitálnej fotografie.

Majme dva rôzne príklady metadát (obrázok 14.2). Naľavo korektné metadáta a napravo podozrivé. Kým z metadát uvedených v ľavej časti vieme vyčítať prídavné informácie o fotografii, ktoré nie sú ničím podozrivé (a len nám dopĺňajú informáciu o dôkaze), tak pravá strana budí podozrenie. V prvom rade spoločnosť Microsoft síce vyrábala mobilné telefóny, ale žiadny z modelových radov nemal označenie Experia Z3. V druhom rade čas zhotovenia fotografie je o 2:32 ráno 12. februára 2017. Ak vieme, že mobilný telefón má nastavené stredoeurópske časové pásmo, tak v túto dobu určite nemohlo svietiť slnko s takou intenzitou. Je veľmi pravdepodobné, že sa bude jednať o podvrh, prípadne daná fotografia môže obsahovať skryté údaje (napríklad steganografického charakteru [22]). Vidíme ako nám metadáta môžu vnuknúť rôzne pohľady na získaný elektronický dôkaz, čím môžu pomôcť potvrdiť alebo vyvrátiť niektorú z hypotéz danú vyšetrovaním.

Pre korektnú manipuláciu s dôkazmi je potrebné dodržiavať princípy integrity dôkazov a reťazca zodpovednosti sledovania dôkazových materiálov (z angličtiny: “Chain of custody”), ktoré sú definované v neskorších kapitolách.

[1] https://sk.wikipedia.org/wiki/Model_OSI



Obr. 14.2: Metadáta digitálnej fotografie.

14.2.2 Digitálny dôkaz a dôkaz

Keďže sa zaoberáme hľadaním stôp (a dôkazov) v digitálnom prostredí, tak to má svoje špecifiká oproti hľadaniu stôp v reálnom svete. Základné rozdiely oproti stopám z reálneho sveta sú [40]:

Nehmotnosť – nezaberajú žiadny objem v priestore, ale je potrebné hmotné prostredie na ich uloženie (rôzne druhy úložných médií).

Latentnosť – pre ľudské zmysly sú nezaznamenateľné. Je potrebné použiť špeciálne prostriedky na ich „zviditeľnenie“ (napríklad prehliadač fotografií, monitor, a iné).

Časová trasovateľnosť – digitálne stopy bývajú obvykle spojené s veľmi presným časovým údajom (aj s presnosťou na nanosekundy). Vďaka čomu je možné ich chronologicky zoraďovať. Je nutné poznať systémový čas (a jeho odchýlku oproti reálnemu času), prípadne mať zosynchronizované (napríklad pomocou NTP protokolu[2]) viaceré zariadenia.

Vysoká obsažnosť (a veľký dátový objem) – hrozí presýtenie údajmi, najmä v dnešnej dobe veľkokapacitných diskov, či úložísk v prostredí cloudu.

Reštaurovateľnosť – aj zničené (rozumej zmazané) údaje je možné niekedy obnoviť, aj do pôvodnej formy.

Originálnosť – vhodným spôsobom zhotovený duplikát je považovaný za zhodný s originálom.

Priestor – digitálne stopy môžu pochádzať z veľkého počtu diametrálne odlišných geografických miest (napríklad útoky typu DDoS).

Šifrovanie – napriek priamemu prístupu k dôkazom nevieme o nich získať žiadne ďalšie informácie, ani zaručene potvrdiť, či sa na danom médiu nachádzajú.

[2] https://tools.ietf.org/html/rfc958

Predovšetkým posledné dva body môžu spôsobiť nepoužiteľnosť digitálnej stopy v ďalšom vyšetrovaní.

14.2.3 Dôkazná dynamika

Dôkazná dynamika je definovaná ako ľubovoľný vplyv, ktorý [18]:

- pridá,
- zmení,
- premiestni,
- zakrýva,
- kontaminuje,
- alebo potiera dôkazy, bez ohľadu na zámer.

Táto dynamika hrá významnú úlohu pri rekonštrukcii zločinov a bezpečnostných incidentov. Pri nedodržaní správnych postupov môže spôsobiť nepoužiteľnosť dôkazu v súdnom pojednávaní.

14.2.4 Základné princípy

Počas forenzného vyšetrovania počítačových systémov je potrebné dodržiavať základné princípy, metódy pre vyšetrovanie, ako aj prácu s dôkazmi.

Forenzná dôkladnosť

Vyšetrovanie je dôkladné z hľadiska forenznej analýzy, ak dodržiava stanovené princípy, štandardy a procesy digitálnej forenznej analýzy. Použité vedecké prístupy (metódy, procedúry,...) musia byť plne zopakovateľné treťou stranou s dosiahnutím rovnakého výsledku. Toto musí platiť aj pre prípady, kedy je získanie digitálneho dôkazu komplikované (napríklad, získanie obrazu operačnej pamäte) [1].

Integrita dôkazov

Pre zachovanie integrity dôkazov je potrebné zabezpečiť dôkaz v jeho originálnej forme. Na prvý pohľad sa to môže javiť jednoduché. Získaný pevný disk uchovávame bezpečne v trezore. Ak však chceme z neho získať údaje, pri nesprávnej manipulácii spôsobíme zápis na tento disk (najčastejšie prepísaním metadát). Napríklad, vo forme aktualizovanie času prístupu k súboru, čím môžeme spôsobiť nežiadúcu zmenu a spochybnenie celého dôkazu. Pri práci s operačnou pamäťou, resp. so „živými“ systémami vo všeobecnosti, sú tieto úkony ešte komplikovanejšie, niekedy až nedosiahnuteľné v klasickom ponímaní.

Medzi niektoré štandardné metódy pre zabezpečenie integrity dôkazov patria:

- Spôsob uloženia fyzických dôkazov s dôrazom na ochranu pred falšovaním.
- Hašovacie funkcie (z angličtiny: "hash"), ktoré vytvoria jedinečný odtlačok digitálneho dôkazu.

- Duplikovanie – vytvorenie forenzného obrazu získaného dôkazu.

Reťazec zodpovednosti sledovania dôkazov

Reťazec zodpovednosti sledovania dôkazov (z angličtiny: "Chain of Custody") obsahuje informácie o:

- získaní,
- kontrole,
- analýze,
- a dispozícii

s fyzickým alebo elektronickým dôkazom od momentu jeho získania až po moment jeho prezentovania pred súdom. Pri práci s týmto typom dokumentu potrebujeme dbať na jeho udržiavanie pre zachovanie integrity dôkazu počas všetkých fáz vyšetrovania dôkazov a odpovedá na 3W typy otázok (z angličtiny "who" – kto, "what" – čo, "when" – kedy) [24]:

- Ako bol dôkaz získaný (označenie, odpojený od PC, atď.)?
- Kedy bol získaný?
- Ako bol presunutý (napríklad zapečatené vrecia, obaly alebo bezpečnostnom boxe)?
- Ako bol sledovaný (napríklad pomocou sekvenčného čísla)?
- Ako bol uložený (napríklad v trezore forenzného laboratória)?
- Kto mal k nemu prístup (proces odovzdania a prevzatia)?

14.3 Proces forenznej analýzy počítačových systémov

Definovať takýto proces potrebujeme, kvôli vytvoreniu štruktúry vyšetrovania zločinu alebo bezpečnostného incidentu. Tradičná forenzná analýza sa zaoberá tým ako získať aký typ dôkazu, ktorý môže podporiť alebo vyvrátiť stanovenú forenznú hypotézu. Proces musí byť dostatočne univerzálny, aby bol použiteľný na ľubovoľné vyšetrovanie vo všetkých jeho fázach. Typicky začína na základe pozorovania, upozornenia, notifikácie, udalosti alebo incidentu, ktoré sa viažu k incidentu.

Existuje viacero modelov opisujúcich takýto typ procesu, najčastejšie sa líšia v počte jednotlivých fáz, ktoré môžu byť v niektorých modeloch zlúčené do jednej. My si vyberieme model [1], ktorý má dostatočne oddelené fázy pre jednoduchšie pochopenie:

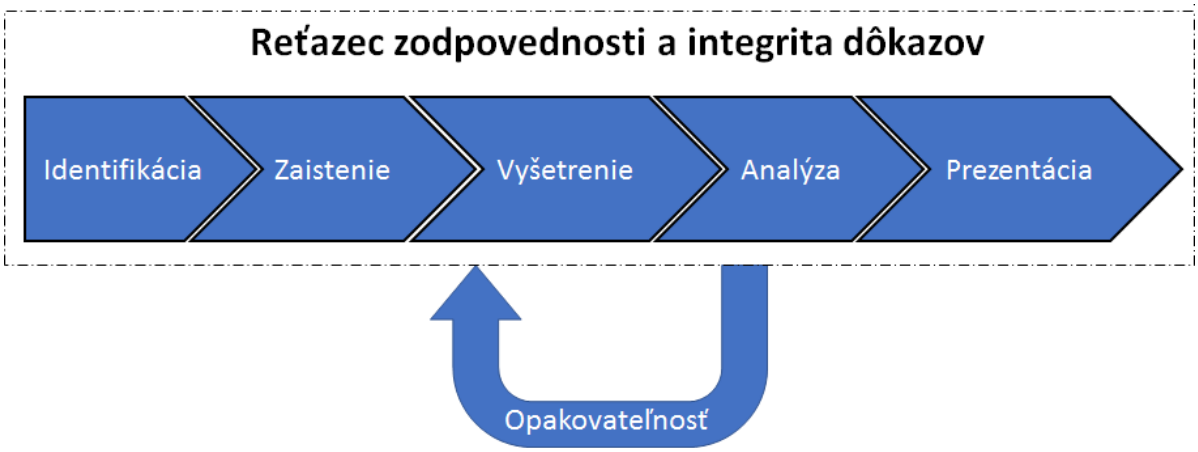
1. Identifikácia – Cieľom je identifikovať digitálne zariadenia ako potencionálne zdroje digitálnych dôkazov.
2. Zaistenie – Ukladanie, kopírovanie a klonovanie „surových" – nespracovaných údajov spôsobom, ktorý možno označiť ako forenzne dôkladný.

3. Vyšetrenie – Surovým údajom sa priradia štruktúry tak, aby sa dali ľahko pochopiť a analyzovať.

4. Analýza – Snažíme sa údaje čo najlepšie pochopiť a identifikovať digitálne objekty, ktoré môžu byť v ideálnom prípade použité pri súdnom procese ako digitálne dôkazy.

5. Prezentácia – Prezentovanie zistených výsledkov pre súdom alebo iným oprávneným subjektom.

Ako vidíme na obrázku 14.3, tak jednotlivé fázy na seba logicky nadväzujú. Počas každej fázy je nutné udržiavať reťazec zodpovednosti sledovania dôkazov, dbať na dodržiavanie integrity dôkazov. Zároveň, každá z fáz je opakovateľná a vieme sa z nej vrátiť do ľubovoľnej predchádzajúcej fázy. Ako príklad si môžeme zobrať vyšetrovanie notebooku. Pri vyšetrovaní zistíme, že bol k notebooku pripojený USB kľúč, ku ktorému sa nám v operačnom systéme viaže odkaz na dôležitý súbor, ktorý nie je v danom notebooku. Na základe tohto zistenia vieme rozšíriť (po schválení príslušnými autoritami) naše vyšetrovanie aj o daný USB kľúč a snažiť sa dopátrať k chýbajúcemu dokumentu.



Obr. 14.3: Proces forenznej analýzy počítačových systémov [1].

Vo väčšine iných modelov [23], [30] zostáva zachovaná vyššie uvedená podstata. Obvykle sú niektoré fázy zlúčené do jednej, ale to platí potom aj o vykonaných činnostiach v rámci takejto fázy. Napríklad postačujú aj 4 fázy, pričom časti venované vyšetrovaniu a analýze môžu byť zlúčené do jednej časti.

Bez ohľadu na zvolený konkrétny model procesu, vieme ich jednotlivé časti rozdeliť do troch fáz:

Prípravná fáza – V niektorých prípadoch môže predchádzať samotnému procesu. Je dôležité uskutočniť všetky potrebné kroky tak, aby forenzní experti mohli kedykoľvek začať svoju činnosť. Napríklad: príprava čistých médií, definované procedúry vyšetrovania, ale aj získanie právne záväzného povolenia pre vstup na miesto činu, spolu s oprávneniami a cieľmi potrebnými pre vyšetrovateľov.

Na mieste činu – Primárne zamerané na získanie možných digitálnych dôkazov, ich uloženie a garantované zachovanie v pôvodnom stave.

Práca viazaná na forenzné laboratórium – Samotné vyšetrovanie a analýza možných digitálnych dôkazov za účelom rekonštrukcie zločinu alebo bezpečnostného incidentu za účelom prezentovania týchto výsledkov oprávneným subjektom.

14.3.1 Identifikácia

Spúšťa sa na základe incidentu, ktorý je definovaný sťažnosťou, upozornením, notifikáciou. Neustále musíme mať v tejto fáze na pamäti 5WH otázky. Úlohou tejto fázy je zistenie a rozpoznanie incidentu alebo zločinu, ktoré majú byť vyšetrované [39]. Definujeme alebo začíname s prvotnými hypotézami o tom, čo sa mohlo stať a kde je pravdepodobné, že nájdeme digitálne dôkazy. V tomto okamihu začína pre viacero dôkazov ich sledovanie v dokumente reťazca zodpovednosti za dôkazy. Pri každý dôkaz by sme mali pri jeho zaistení uviesť minimálne tieto údaje [24]:

- Osoba zaisťujúca dôkaz.
- Proces a procedúry, ktoré boli pri tomto vykonané (napr. pri zaistení).
- Čas a dátum získania dôkazu.
- Pôvodná poloha a pozícia dôkazu.
- Dôvod, prečo bol daný dôkaz zaistený.

Spolu s týmito údajmi je možné použiť rôzne ďalšie podporné materiály ako sú fotografie, snímky obrazovky, videá, správy, kontrolné zoznamy, tzv. „log súbory“.

Príprava

Pre začatím samotného vyšetrovania je potrebné byť pripraveným na jeho začatie a priebeh. Zlá príprava môže spôsobiť neskoré alebo nesprávne reakcie, či chybnú manipuláciu s dôkazmi, ktoré môžu viezť až k neželane zlým výsledkom (napríklad: oslobodenie/nevypátranie zodpovednej osoby za incident).

Vždy je potrebné mať oficiálne potvrdenie pre začatie vyšetrovania od príslušnej autority (policajní vyšetrovatelia, zodpovedná osoba vo firme). V firmách to platí najmä ak sa jedná o vyšetrovanie na kritickej infraštruktúre. Je potrebné mať pripravené forenzné laboratórium, ktoré musí mať správnu výbavu a príslušné certifikácie.

Osoba prvého kontaktu

Osoba prvého kontaktu je primárne zodpovedná za zachovanie miesta činu v nekompromitovanom stave z hľadiska nasledujúceho vyšetrovacieho procesu. Je potrebné zdokumentovať všetko na mieste činu, ako sú zariadenia zapojené, ktoré porty majú obsadené, ktoré zo zariadení sú zapnuté, akú aktivitu vykonávajú skontrolovať čas na zariadenia (kvôli neskoršej synchronizácii).

Je potrebné mať zadefinované štandardné operačné procedúry, ktoré sú štruktúrované, identifikujú jednotlivé aktivity, pre ktoré sú určené, napr. pre nájdený, zapnutý mobilný telefón na mieste činu, určujú spôsob dokumentovania a ako zabezpečiť integritu dôkazu. V závislosti od konkrétnej procedúry by mohlo byť najvhodnejšie vložiť tento telefón do Faradayovej klietky, aby sa zamedzil vzdialený prístup k zariadeniu, ale aby zostalo zapnuté.

Takouto osobou môže, ale nemusí byť člen tímu digitálneho forenzného laboratória. Najmä v prípade kriminálnych zločinov sa môže najčastejšie jednať o policajných vyšetrovateľov, pre ktorých však stále platia vyššie uvedené pravidlá. Ak by napríklad vyšetrovateľ našiel na mieste vyšetrovania zablokovaný mobilný telefón, ktorý by sa snažil viackrát odomknúť zlým PIN alebo PUK kódom, mohlo by to viezť k zmazaniu usvedčujúcich dôkazov. Naopak, obhajoba by mohla tvrdiť, že boli zmazané kľúčové dôkazy dosvedčujúce nevinu podozrivého.

14.3.2 Zaistenie

Fáza zaistenia dát je zodpovedná za zber údajov z digitálnych zariadení prostredníctvom vytvorenia digitálnej kópie s dôrazom na forenzné postupy a metódy. Pre digitálne dôkazy by mali byť vytvorené metadáta, ktoré obsahujú dôležité údaje, napríklad identifikačné (názov a číslo prípadu, vyšetrovateľ), časové pečiatky.

Pri vytvorení digitálnej kópie údajov sa môžeme stretnúť s viacerými identickými pojmami: duplikát, klon, obraz bitového toku, bitová kópia, kópia surových údajov. Všetky majú z hľadiska digitálnej forenznej analýzy rovnaký význam.

Cieľom je vytvoriť si minimálne dve kópie. Zdroj digitálneho dôkazu treba potom uložiť na bezpečné miesto, napríklad do trezoru. Potom s jednou kópiou pracujeme pri ďalšom vyšetrovaní a druhá, ku ktorej je obmedzený prístup nám môže slúžiť ako záloha pre obnovenie, keby došlo k nekorektnému zásahu do údajov.

Pri zaisťovaní údajov musíme dbať na dva základné body:

Garantovať žiadne alebo len minimálne zmeny v zdrojových údajoch. Minimálne zmeny sú za určitých okolností povolené pri získavaní údajov zo živých systémov. Pre získanie obrazu pevného disku by sme naopak mali garantovať zachovanie presného stavu údajov, najčastejšie pomocou blokovania zápisu (softvérovou alebo hardvérovou realizáciou).

Garantovať autenticitu získaných údajov. Najčastejšie sa používa vytvorenie hašu (z angličtiny: “hash”) originálnych údajov a vytvoreného duplikátu, ktoré musia byť totožné. Toto platí najmä pre zariadenia s pamäťou nezávislou na napájaní.

Z právneho hľadiska je takto získaný duplikát považovaný za totožný s originálom a je použiteľný počas vyšetrovania.

Zabezpečenie integrity

Patrí medzi základné činnosti digitálnej forenznej analýzy. Dôkaz musí zostať nezmenený, resp. zmenený v dobre zdokumentovanej miere. Z tohto dôvodu sa pri získavaní klonu údajov vytvárajú haše aj originálu aj kópie. Odtlačok originálu sa nesmie v čase meniť a oba odtlačky

sú získané pomocou štandardných jednosmerným matematických algoritmov. Tieto nám garantujú výstup fixnej dĺžky bez ohľadu na veľkosť vstupu a majú zabezpečiť matematicky nedosiahnuteľnú možnosť pre zaistenie toho, aby mali dva rôzne súbory rovnaký odtlačok.

Najčastejšie sa používajú MD5, SHA1 a SHA256. Aj keď MD5 a SHA1 patria medzi zastaralé a v bežnom použití by sa už nemali používať [25]. Pre účely digitálnej forenznej analýzy sú stále postačujúce, avšak odporúčajú sa v takomto prípade robiť odtlačky pomocou oboch algoritmov zároveň.

JumpKit

Špeciálny kufrík alebo set zariadení a pomôcok potrebných pre použitie na mieste činu, ktorý by mal obsahovať:

- Notebook s nainštalovaným softvérom, napríklad: pre odpočúvanie sieťovej komunikácie, prehliadače pre internet, registre, zobrazenie súboru v hexadecimálnom tvare.
- Prázdne média pre ukladanie.
- Základné aktívne sieťové prvky a príslušná kabeláž.
- Médium operačným systémom bez nutnosti inštalácie.
- Poznámkový blok, perá a zvýrazňovače.
- Fotoaparát.

Zdroje digitálnych dôkazov

Medzi zdroje digitálnych dôkazov patria počítače, vnorené systémy, mobilné telefóny, ale aj počítačové a mobilné siete.

Systémy fyzicky viazané na lokalitu sú také, ktoré nie je možné presúvať, odoberať alebo sa nachádzajú na inej fyzickej lokalite bez prístupu, napríklad centrálne firemné servery nadnárodných korporácií. V takýchto prípadoch máme dve možnosti:

- Vytvoriť kópiu údajov na mieste.
- Vytvoriť kópiu údajov prostredníctvom počítačovej siete.

Pri zbere digitálnych dôkazov treba počítať s tým, že možný dôkaz sa nemusí nachádzať na jednom médiu. Napríklad z údajov na mailovom serveri zistíme, že bola prijatá podozrivá príloha. Na počítači konkrétneho používateľa zistíme, že s ňou bolo pracované, ale nachádza sa na USB kľúči. Pre vytvorenie korektného záveru v tomto prípade potrebujeme získať údaje zo všetkých troch zdrojov.

Vzdialená akvizícia prostredníctvom počítačovej siete

V tomto prípade treba počítať s tým, že údaje budeme posielať po nedôveryhodnom kanáli. Je nutné posielať údaje šifrovaným spôsobom, aby sme predišli ich modifikácií, napríklad útokom človeka uprostred (z angličtiny: "man-in-the-middle" útok). Medzi ďalšie riziká patrí aj riziko nutnosti inštalovania softvéru na cieľové zariadenie, čo môže narušiť originálnosť a integritu údajov. Rovnako sme v tomto prípade závislý na hardvérových obmedzenia zariadenia.

V niektorých prípadoch zariadenie môže patriť tretej strane (napr. Google, Amazon a iné). V tomto prípade môže celá snaha o získanie dôkazov zlyhať, najmä ak je potrebné, aby prevádzkovateľ zariadenia dostal príkaz od súdu v mieste sídla svojej centrály alebo dátovom centre.

Nestálosť údajov

Ako sme naznačili v predchádzajúcich častiach, nie všetky údaje sú na nosičoch s porovnateľnými parametrami. Dôležitými rozdielmi sú (ne)závislosť digitálnych nosičoch na napájaní a rýchlosti prepisovania údajov. Tieto informácie nám môžu pomôcť určiť si priority získavania údajov na mieste činu. Chybným krokom býva vypnutie zariadenia (napr. počítača) a získanie obrazu jeho údajov z pevného disku. Týmto krokom by sme prišli o všetky údaje uložené v operačnej pamäti, ukončili by sme všetky sieťové spojenia, a teda by sme stratili veľké množstvo potenciálnych dôkazov.

Príklady poradia nestálosti údajov (od tých najviac nestálych):

- Systémové registre, vyrovnávacie pamäť.
- Operačná pamäť.
- Sieťová premávka.
- Bežiace systémové procesy.
- Údaje v tzv. „cloude“.
- Údaje na disku.
- Média založené na princípe magnetizmu (diskety, magnetické pásky).
- CD, DVD, SSD, flash pamäte.

Čo zbierať

Ak vieme, že niektoré údaje sú v čase nestále, môžu sa meniť, že nám nemusia stačiť údaje len z jedného zdroja (napr. pevný disk), tak to môže zavážiť pri voľbe údajov, ktoré chceme získať. Existuje viacero faktorov, ktoré treba brať do úvahy pri zaisťovaní možných digitálnych dôkazov [1]:

Nestálosť údajov – čím sú údaje menej stále a potrebujeme ich, tým majú vyššiu prioritu.

Prístup k obmedzeniam a šifrovaniu – údaje s obmedzeným prístupom alebo šifrované údaje, ku ktorým je momentálne prístup v ich priamej forme je potrebné získať, kým je tento prístup k dispozícii (napríklad šifrované partície na disku).

Napájanie – zariadenia, ktoré sú v daný moment zapnuté, majú prioritu pred vypnutými zariadeniami.

Vypnutie – korektný spôsob vypnutia môže spôsobiť stratu dôležitých údajov (napríklad pomocou skriptov, ktoré sa vykonávajú pri vypínaní). Vybratie baterky alebo odpojenie zdroja energie môže tomu zabrániť, ale spôsobí stratu nestálych údajov.

Fyzické rozhrania – na rôznych rozhraniach môžeme nájsť rôzne typy údajov (USB, wifi, ...). Podobne to platí aj o komunikačných protokolov v počítačových sieťach.

Zdroje digitálneho forenzného laboratória – prostriedky, ktoré máme k dispozícii nás môžu limitovať.

Interpretácia – ak nevieme dáta správne interpretovať, tak môžu byť pre nás nepoužiteľné.

14.3.3 Vyšetrovanie

Samotná fáza vyšetrovania súvisí s prípravou a extrakciou potenciálnych dôkazov zo získaných zdrojov údajov. Tak, ako v predchádzajúcich krokoch, je dôležité udržiavať aktuálne dokumenty, viažuce sa k manipulácii s dôkazmi. Okrem manipulácie je potrebné zaznamenávať aj všetky činnosti vykonané nad údajmi, aby mohli byť bez problémov rekonštruovateľné prípadnou treťou stranou.

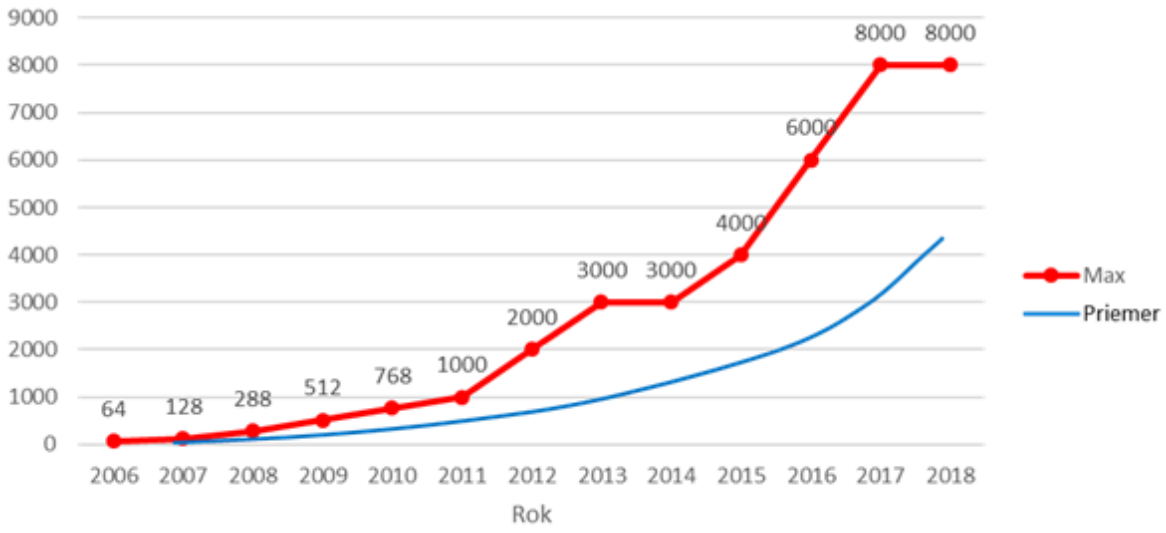
V tejto fáze začíname pôvodné bloky bitov upravovať, rekonštruovať, či predspracovať tak, aby boli zrozumiteľné pre forenzných vyšetrovateľov. Cieľom je získať potenciálny dôkaz, ktorý môže pochádzať aj z viacerých zdrojov údajov.

Vyšetrovanie a predspracovanie

Údaje, ktoré sme získali vo fáze zaistenia môžeme považovať za typ tzv. „čiernej skrinky“. V princípe sa jedná o binárne a neštruktúrované údaje. Bez použitia ďalších metód nemusíme vedieť rozpoznať, či sa pozeráme na partíciu disku alebo na obraz operačnej pamäte.

V dnešnej dobe sa štandardne používajú nástroje pre digitálnu forenznú analýzu, ktoré pomáhajú získaným údajom dávať štruktúru. Napríklad: v získanom obraze pevného disku sa budeme vedieť pohybovať po štruktúre jeho priečinkov, súborov.

Na digitálnu forenznú analýzu má nepriamy dôsledok Mooreov zákon, ktorého dôsledkom je exponenciálny nárast množstva údajov. Len bežná veľkosť operačnej pamäte vzrástla od roku 2006 do rok 2018 z niekoľko megabajtov na jednotky gigabajtov (Obrázok 14.4). NASA [48] pracovala v programe Apollo s počítačmi a pamäťou 2048 slov (4096 B). Je nepredstaviteľné v dnešnej dobe, kedy mobilné zariadenia môžu mať viac ako 12 GB RAM, čo je viac ako 3 000 000-krát väčšia pamäť.



Obr. 14.4: Kapacita operačnej pamäte v čase v MB [12].

Obnova dát

Výhodou práce s digitálnymi materiálmi je možnosť obnovy zmazaných údajov. Keďže elektronické zariadenia majú ako primárny cieľ poskytovať čo najlepší používateľský zážitok, tak mnohé iné prvky idú do úzadia. Medzi prvé takéto prvky patrí aj bezpečné mazanie alebo zničenie údajov. Môžeme si predstaviť mazanie 10 GB súboru (napríklad filmu vo FULL HD rozlíčení), pri dnešných rýchlostiach zápisu by bezpečné zmazanie takéhoto súboru z pevného disku trvalo približne 20 sekúnd. Ak tieto údaje len zneplatníme, tak zmazanie bude trvať zlomok takéhoto času. Voľná kapacita disku sa zväčší, používateľ takmer nič nepostrehol. Reálne údaje na disku zostali, i keď sú označené ako voľné miesto. Z tohto vyplýva, že údaje zmiznú až vtedy, keď sú prepísané novými údajmi.

Pod obnovou údajov môžeme z hľadiska forenzného vyšetrovania rozumieť aj ďalšie úkony:

- Detekcia nesprávnych koncoviek súborov vzhľadom k ich obsahu a ich opravenie.
- Komprimované súbory by mali byť dekomprimované.
- Šifrované súbory by mali byť identifikované a mali by sme sa pokúsiť prelomiť ich heslá.
- Identifikovať použité prvky zahmlievania, najmä použitie steganografie alebo anti-forenzných techník.

Redukcia dát a filtrovanie

Bez ohľadu na Mooreov zákon, spomenutý v predchádzajúcich podkapitolách, platí, že vyšetrovatelia nemajú k dispozícii nekonečné zdroje, ako sú čas, vybavenie, či financie. Pri ich dispozícii nie je problém analyzovať všetky dôkazy do hĺbky. Vybavenie a financie sú obmedzenia, ktoré upravujú ponuku služieb konkrétneho forenzného laboratória. Pre efektívnu prácu

s časom je vhodné vykonať vhodné zúženia nad získanými údajmi. Analogicky sa dá na túto situáciu pozerať ako na prístup k pacientom na pohotovosti alebo vojnovej zóne. Prednosť majú najviac ohrození pacienti a postupne sa prechádza k tým menej závažným zraneniam bez ohľadu na príchod pacienta. Tento istý prístup vieme aplikovať aj v tejto doméne. Potrebujeme vychádzať z informácií, ktoré už sú známe o prípade. Môžu nám pomôcť pri stanovovaní priorít a určiť začiatok nášho vyšetrovania údajov. Začneme identifikovať údaje, o ktorých vieme, že sa tam (napr. na disku) musia nachádzať, ako napríklad: obrázky, malware, TCP komunikácia na porte 80 a iné.

Iným prístupom k redukcii množstva údajov je filtrácia na základe známych súborov. Ak vezmeme do úvahy, že vyšetrujeme počítač, ktorý mal nainštalovaný OS Windows 10, tak len samotný priečinok Windows, môže obsahovať desaťtisíce súborov a priečinkov. Ak vieme, že sa tam môže nachádzať infikovaný súbor, tak je to hľadanie „ihly v kope sena“. Pri použití filtrácie na základe známych súborov viem zvoliť dva prístupy:

1. Známe dobré súbory – máme k dispozícii databázu[3] systémových súborov a ich hašov (z angličtiny: “hash”), ktoré ak nie sú zmenené, nemajú pridanú hodnotu pre vyšetrovanie.

2. Známe zlé súbory – podobný princíp ako v predchádzajúcom prípade, avšak nájdenie zhody znamená, že sme našli niečo zaujímavé pre vyšetrovanie.

Podobný princíp môžeme uplatniť aj na iné typy údajov, ako sú napríklad IP adresy, ktoré majú tiež svoje databázy. Ak vytvoríme surovým údajom správne štruktúry, tak môžeme filtrovať podľa typov údajov, napríklad obrázky na disku, spustené procesy v operačnej pamäti. Ak zanedbáme pôvod a typ údajov, ďalší spôsob redukovania objemu údajov môžeme realizovať na základe zúženia časového rámca, v rámci ktorého budeme hľadať digitálne dôkazy alebo koreláciu medzi nimi. V tomto prípade je potrebné vedieť ako bude zobrazovať použitý nástroj čas analyzovaných údajov, napríklad: zohľadní pôvodnú časovú zónu?

Dolovanie dát a súborov

Ak údaje majú svoju štruktúru a vykonali sme potrebné zúženie (resp. chceme vykonať zúženie na základe typu súboru), tak sa snažíme nájsť všetky relevantné súbory, či sa jedná o známe typy súborov alebo iné špeciálne typy. Medzi špeciálne typy určite patria poškodené alebo zmazané súbory, ktoré môžu stále poskytnúť podstatné informácie. Veľmi dôležitým prvkom pri dolovaní súborov a údajov je ich extrakcia (po ich nájdení) tak, aby sme s nimi vedeli ďalej pracovať.

Často používanou metódou je hľadanie hlavičiek a pätičiek požadovaných typov súborov [21], kedy hľadáme konkrétne série bitov, na základe ktorých vieme identifikovať, že sa jedná napríklad o súbor typu PDF. Aplikovaním tohto prístupu vieme na inej úrovni abstrakcie analyzovať maily (v rámci súboru s mailami), či bežiace procesy (v operačnej pamäti).

Keďže táto fáza je veľmi náročná na zdroje, je snahou ju čo najviac automatizovať a používať známe nástroje, či skripty (aj vlastnej tvorby). Tieto nástroje vieme používať aj na hľadanie konkrétnych reťazcov, používať regulárnych výrazov.

[3]Napríklad: National Software Reference Library – www.nsrl.nist.gov

14.3.4 Analýza

Predposledná fáza vyšetrovania je zameraná na spracovanie informácií, ktoré súvisia s cieľom vyšetrovania, so zameraním na pomenovanie faktov o udalosti, významnosti dôkazu a zodpovednej osoby. Môže tu prísť k preformulovaniu pôvodných hypotéz alebo definovaniu nových, čo môže viesť k novým zberom údajov a opakovaniu predchádzajúcich fáz vyšetrovania. Z tejto fázy sa vraciame do predchádzajúcich, kým nie sme spokojný so zisteniami a ak nám to okolností dovoľujú.

V závislosti od typu prípadu nám môžu postačovať rôzne typy dôkazov v rôznom rozsahu. Napríklad poslaný mail môže dokazovať, že sa ľudia poznali, čas prístupu k súboru znalosť informácie v ňom a iné. Regulárne výrazy a hľadanie kľúčových slov (maily, IP adresy, webové stránky, telefónne čísla a iné) tvoria významnú časť práce.

Udalosti zoraďujeme na základe času ich výskytu na časovú os. Pracujeme s MAC časmi[4] (z angličtiny: "modification" – modifikácia obsahu, "access" – prístup, "change" – zmena metadát). Rôzne operačné a súborové systémy nám môžu poskytnúť aj ďalšie časy, ako sú vznik súboru alebo čas jeho zmazania. Tu je potrebné poznať špecifiká systému, s ktorým pracujeme, aby nedošlo k nesprávnej interpretácii. Ďalej môžeme pripravovať výpisy z tzv. „log súborov", či robiť linkovú analýzu, ktorá zobrazuje vzťahy medzi jednotlivými objektmi. Často sa používa pri sociálnych sieťach, mailoch, či prehliadaní webu.

14.3.5 Prezentácia

Prezentácia je tá časť vyšetrovania, v ktorej vyšetrovateľ predstavuje zistené výsledky z fázy analýzy vo forme záverečnej správy pre všetky dotknuté strany. Zdokumentované sú objektívne nálezy na postačujúcej miere istoty a končí sa evidovanie v dokumentoch reťazca zodpovednosti pre jednotlivé dôkazy.

Záverečná správa

Finálna správa obsahuje všetky relevantné informácie spolu s ich kontextom a pozadím:

- Čo bolo urobené?
- Kto realizoval vyšetrovanie?
- Čo bolo vyšetrované?

Medzi typické informácie, ktoré záverečná správa obsahuje patria [1]:

- Role a úlohy.
- Manažérske zhrnutie (z angličtiny: "executive summary").
- Forenzné zaistenie a analýza, ktoré reflektujú integritu dôkazu a dokumentáciu reťazec zodpovednosti manipulácie s dôkazmi.
- Vizualizácie a diagramy.

[4] https://en.wikipedia.org/wiki/MAC_times

- Obrázky a snímky obrazovky.
- Informácie, ktoré sú overiteľné opakovateľnosťou.
- Použité nástroje.
- Zistenia.

14.4 Forenzná pripravenosť

Forenzná analýza počítačových systémov potrebovala definovat pre svoj rozvoj viaceré nové časti v rámci vtedajších právnych systémov. Významne v tomto pomohol konvent venujúci sa počítačovej kriminalite (ďalej len „Konvent“), ktorý sa konal v Budapešti [6]. Konvent nastolil viaceré právne rámce, ktoré boli prevzaté do národných právnych systémov. Nastolil dohodu medzi štátmi, ktoré sa zaviazali ošetrením (kriminalizáciou) konkrétnych aktivít počítačovej kriminality vo svojich právnych úpravách.

Vyšetrovanie počítačovej kriminality je obvykle závislé na odhalení (kybernetického) bezpečnostného incidentu. To sa môže stať pomocou automatizovaných nástrojov alebo nahlásením od zodpovednej osoby. Náš zákon [34] definuje bezpečnostný incident takto:

- „kybernetickým bezpečnostným incidentom akákoľvek udalosť, ktorá má z dôvodu narušenia bezpečnosti siete a informačného systému, alebo porušenia bezpečnostnej politiky alebo záväznej metodiky negatívny vplyv na kybernetickú bezpečnosť alebo ktorej následkom je:
  1. strata dôvernosti údajov, zničenie údajov alebo narušenie integrity systému,
  2. obmedzenie alebo odmietnutie dostupnosti základnej služby alebo digitálnej služby,
  3. vysoká pravdepodobnosť kompromitácie činností základnej služby alebo digitálnej služby alebo
  4. ohrozenie bezpečnosti informácií,“.

S počítačovou kriminalitou súvisí podmienka dokázania porušenia príslušných právnych úprav [1]:

1. Čin musí byť rozpoznaný v právnom systéme, do ktorého jurisdikcie spadá. Legislatíva musí definovať podmienky, ktoré musí čin naplniť, aby spadal do oblastí trestnoprávnych ustanovení. Musia nastať objektívne podmienky trestnoprávnej aktivity. Toto je spojené s otázkami: „Kedy?“ „Kde?“ a „Ako?“ modelu 5WH.
2. Osoba musí konať s úmyslom (t.j. musí vedieť, čo robí). Zámer musí zahŕňať fakty zločinu a pokrýva všetky objektívne podmienky. Je silno previazaný s otázkou „Prečo?“ z 5WH modelu.
3. Osoba musí byť trestnoprávne zodpovedná. To znamená, že musí spĺňať vekovú podmienku určenú zákonom a musí byť aj mentálne schopná. V tomto bode hovoríme primárne o otázke „Kto?“ z modelu 5WH.

4. Nesmeli nastať okolnosti, ktoré by mohli spôsobiť označenie za zločin aktivitu, ktorá je právne v poriadku. Napríklad núdzové alebo naliehavé okolnosti. Zameriavame sa na otázky „Kedy?“, „Kde?“, „Ako?“ a „Prečo?“ z 5WH modelu.

Kybernetické zločiny najčastejšie súvisia s manipuláciou s údajmi na počítačových systémoch, ku ktorým bol neoprávnený prístup alebo boli odpočúvané. Je viacero význačných pojmov, ktoré Konvent definuje (alebo ukladá povinnosť definovať v národnej legislatíve) [6]:

Počítačový systém – jedno alebo viacero prepojených alebo navzájom súvisiacich zariadení, kde jedno alebo viacero z týchto zariadení, na základe programu automaticky spracovávajú údaje.

Počítačové údaje – ľubovoľná reprezentácia faktov, informácií, konceptov vo forme spracovateľnej počítačovým systémom, vrátane možnosti vykonania zvolenej funkcie počítačovým systémom.

Neoprávnený prístup – prístup k počítačovému systému alebo jeho časti bez oprávnení.

Neoprávnené odpočúvanie – zrealizované technickými prostriedkami na neverejne prenášané údaje z/vo vnútri počítačového systému, vrátane elektromagnetického žiarenia z počítačového systému, ktorý nesie takéto údaje.

Modifikácia údajov – poškodenie, zmazanie, zhoršenie, zmena alebo znemožnenie prístupu k údajom bez oprávnení.

Modifikácia/ovplyvnenie systému – vážna prekážka vo fungovaní počítačového systému zadávaním, prenášaním, poškodzovaním, vymazaním, zhoršovaním, pozmeňovaním alebo potláčaním počítačových údajov.

Počítačová kriminalita môže mať rôzne podoby, ale v princípe sa jedná o protiprávne konanie človeka alebo skupiny ľudí, pri ktorom sú cieľom alebo prostriedkom informačné systémy alebo ich komponenty so zameraním [40]:

Na hmotný majetok informačných systémov – krádež alebo poškodzovanie počítačov alebo ich príslušenstva, vrátane nosičov informácií.

Nehmotný majetok informačných systémov – proti programovému vybaveniu, databázam a informáciám (ich odcudzovanie, modifikácia, nelegálne používanie, mazanie a iné).

Využitie počítačovej techniky ako prostriedkov na páchanie trestnej činnosti – napríklad: krádež identity, hospodárska kriminalita, detská pornografia, podnecovanie alebo schvaľovanie trestných činov.

Špecifikom počítačovej kriminality je ich veľmi častá cezhraničná pôsobnosť. Nie je vôbec nezvyčajným javom, že útočník z jednej krajiny útočí prostredníctvom zariadení z viacerých rôznych krajín na cieľ, ktorý sa nachádza v inej krajine. Rovnako, vzhľadom na rozšírené používanie služieb (napríklad mail, sociálne siete a iné), je častý prípad, že údaje, ktoré sú v oblasti záujmu vyšetrovania, sa nachádzajú v inej krajine ako prebieha samotné vyšetrovanie. Vďaka Konventu sa podarilo zadefinovať cezhraničný prístup k uloženým počítačovým údajom, ktoré sú verejne dostupné (článok 32a Konventu) [6]:

- Strana (napr. krajina, vyšetrovací orgán) môže bez nutnosti autorizácie od inej strany pristupovať k verejne dostupným uloženým počítačovým údajom bez ohľadu na to, kde sa údaje nachádzajú geograficky.

Aj keď je táto definícia pomerne vágna, pretože jasne nedefinuje, čo všetko sú „verejne dostupné údaje“ a čo už nie, a ktoré údaje možno považovať za „uložené“, vie pomôcť pri vyšetrovaní. Je potrebné brať do úvahy okolností konkrétneho prípadu s ohľadom na zámer vyšetrovania. Pod špeciálnym dohľadom je právo na súkromie každého človeka. Dôležité je, že článok 32b Konventu rieši prístup k cezhraničným údajom aj inou formou: legálnym a dobrovoľným súhlasom osoby, ktorá má autoritu (z hľadiska zákona) zverejniť tieto údaje vyšetrujúcej strane.

Dostávame sa k pojmu digitálna forenzná pripravenosť, ktorá je definovaná ako [1]:

- schopnosť vykonať digitálne vyšetrovanie s minimálnymi nákladmi, ale s maximalizáciou užitočnosti dôkazov.

Vyšetrovanie vo firme vs. Kriminálne vyšetrovanie

Firmy našli využitie pre forenznú analýzu počítačových systémov aj v rámci svojich štandardných procesov. Najčastejšie sa môže využívať pri vyšetrovaní príčin bezpečnostných incidentov, hľadanie odchýlok od požadovaného správania, či ako podpora pre disciplinárne potrestanie.

Firemné vyšetrovanie môže prebiehať nezávisle na kriminálnom vyšetrovaní ako súčasť definovaných vnútropodnikových procedúr. Musia platiť rovnaké prístupy, aby získané dôkazy mohli byť použité pri kriminálnom vyšetrovaní. Ak nastane situácia, kedy bežný bezpečnostný incident prerastie do trestného činu, v takom prípade je nutné kontaktovať príslušné autority, aby prevzali vyšetrovanie. Ako príklad si môžeme predstaviť detegované nedovolené použitie torrent klienta[5] a pri ďalšom vyšetrovaní sa nájde na dotknutej počítačovej stanici detská pornografia.

Na rozdiel od kriminálneho vyšetrovanie sa pri firemnom vyšetrovaní kladie dôraz na zabezpečenie plynulosti chodu firmy bez ohrozenia kľúčových operácií. Z tohto nám vyplýva drobná úprava pojmu digitálna forenzná pripravenosť pre firemné prostredie (tzv. „firemná digitálna pripravenosť“):

- schopnosť firmy vykonať digitálne vyšetrovanie s minimálnymi nákladmi, minimálnym narušením firemných operácií, ale s maximalizáciou užitočnosti dôkazov.

Aj pri kriminálnom aj firemnom vyšetrovaní sa opierame o pojem „užitočnosť dôkazu“. Bola navrhnutá [11] definícia všeobecného digitálneho dôkazu, ktorá je daná:

- Váhou dôkazu počas súdneho procesu.
- Relevantnosťou a dostatočnosťou pre:
  - zistenie hlavnej príčiny,

[5] https://sk.wikipedia.org/wiki/BitTorrent

– spojenie útočníka s incidentom.

Najmä pri firemnom vyšetrovaní, kde sa uplatňuje zvýšený dôraz na minimalizáciu škôd na chod podnikania, platí, že môže byť ohrozená aj existencia samotných dôkazov, ktoré je pomerne zložité zaistiť, ale veľmi jednoduché zničiť. Ak máme vo firme počítač, ktorý sa správa „zvláštne“, tak s veľkou pravdepodobnosťou sa postupuje scenárom:

1. Reštartnutie počítača.
2. Ak problémy pretrvávajú, vykonať kontrolu diagnostickým softvérom (napríklad antivírus).

Ak by sme vykonali vyššie uvedené kroky, tak je takmer isté, že prišlo k zničeniu niektorých dôkazov. Je dôležité, aby mali firmy rozumne vybalancovanú koordináciu medzi tímami zodpovednými za reakciu na incidenty a tímami zodpovednými za vyšetrovanie. V princípe majú oba tieto tímy protichodné záujmy. Kým jeden potrebuje čo najrýchlejšie odstrániť problém a obnoviť štandardnú funkčnosť, tak druhému môže za určitých okolnosti vyhovovať aj dlhšie pozorovanie predmetu vyšetrovania (napríklad: prebiehajúci sieťový útok). Vhodným kompromisom môže byť, v niektorých prípadoch, vytvorenie obrazu z postihnutého počítača, jeho obnovenie do funkčného stavu, ďalšie vyšetrovanie realizované na vytvorenom obraze (disku, operačnej pamäte, ...).

14.4.1 Rámce, štandardy a metodológie

Neexistuje jediný spôsob ako zabezpečiť forenznú pripravenosť. Viacero štandardizačných entít a organizácií navrhlo rôzne rámce a metodológie, pričom táto oblasť sa neustále vyvíja, aj vzhľadom na dynamickosť celého odvetvia informatiky.

Štandardy:

ISO/IEC 27037 – definuje digitálny dôkaz a definuje tri základné princípy riadenia orientované na relevantnosť, spoľahlivosť a dostatočnosť. Poskytuje všeobecné podmienky manipulovania s dôkazmi, aby boli použiteľné v právnom procese, od identifikácie, cez zaistenie, zber až po ich bezpečné uchovanie.

ISO/IEC 17025 – štandard zameraný na požiadavky, ktoré sú kladené na forenzné laboratória. Zahŕňajú rovnako technické aj manažérske požiadavky (ako napríklad zabezpečenie kvality, požiadavky kladené na metodológiu).

NIST SP 800-86 – organizácia NIST vo všeobecnosti patrí k významným tvorcom štandardov v tejto oblasti. Definuje základné návody pre získavanie dôkazov zo súborov, operačných systémov, sietí, aplikácií, či iných zdrojov.

Na štandardy nadväzujú smernice. V našom európskom priestore má významné postavenie ENFSI (European Network of Forensics Science Institutes) pravidelne publikuje návody zamerané na najlepšie skúseností z jednotlivých oblastí.

Firemná pripravenosť pre digitálnu forenznú analýzu musí byť schopná jednoduchého premostenia na súdne vyšetrovanie. Zároveň, keďže firmy majú plne k dispozícii svoju infraštruktúru, vedia sa pripraviť tak, aby prípadné vyšetrovanie prebiehalo čo najlepšie (a najrýchlejšie). Najčastejšie sa to realizuje formou zbierania údajov už dopredu. V takýchto prípadoch môžeme naraziť na legislatívne obmedzenia, pretože nie všetky údaje je možné zbierať a analyzovať bez súhlasu súdu. Najčastejšie sa môže jednať o údaje zákazníkoch a ich maily, alebo aj kompletné sieťové rámce. Pri sieťových rámcoch sa zvyknú zbierať a analyzovať len hlavičky konkrétnych protokolov.

Platí, že firemné politiky, procesy a procedúry musia pamätať rovnako na zotavenie sa z bezpečnostného incidentu ako aj na digitálnu forenznú analýzu. Najmä, z dôvodu, že tieto dva druhy aktivít môžu často stáť na opačných koncoch a činnosti jedného typu môžu spôsobiť nezvratné, katastrofálne zmeny pre činnosti druhého typu aktivít.

14.4.2 Ľudia

Ľudia sú významným aspektom pri forenznej analýze počítačových systémov. Pre správny a bezproblémový priebeh vyšetrovania je potrebné mať zostavený tím s presne definovanými rolami a zodpovednosťami. Tím musia tvoriť profesionáli s požadovanými zručnosťami, ktoré si v čase aj naďalej trénujú. Zároveň, všetci by mali prechádzať pravidelnými tréningami na zvyšovanie povedomia. Tohto tréningu by sa v prípade firmy mali zúčastňovať všetci kľúčoví pracovníci (v závislosti od kompetencií), aby vedeli ako majú reagovať v prípade bezpečnostného incidentu (čo robiť, čo určite nerobiť, komu zavolať a i.).

Úlohy a zodpovednosti

Existuje viacero možností ako usporiadať úlohy v tíme. Vychádzajúc z procesu forenznej analýzy počítačových systémov, môžeme definovať role takto [1]:

Osoba prvého kontaktu – začatie vyšetrovania, zabezpečenie miesta incidentu, prvotná identifikácia digitálnych dôkazov.

Špecialista na digitálnu forenznú analýzu – identifikácia a zaistenie dôkazov, vrátane forenznej analýzy živých systémov.

Forenzný analytik – analyzuje rôzne typy digitálnych dôkazov a podáva správu o zistených výsledkoch.

Forenzný vyšetrovateľ – zodpovedný za vyšetrovanie, koordinuje jednotlivé aktivity, interpretuje zistenia a podáva správu o výsledkoch.

Špecialista na uchovávanie údajov – zodpovedný za uchovávanie dôkazov v súlade so schválenými politikami alebo kladenými požiadavkami.

Samozrejme nie každá firma alebo forenzné laboratórium musí disponovať presne týmito pozíciami. V prípade potreby je možné zodpovednosti spájať do jednej fyzickej osoby. Naopak, niektoré môžu byť znásobené, typicky najmä forenzný analytik, ktorý sa môže špecializovať na rôzne časti, či systémy.

RACI matica

Pri zložitejšom prístupe k forenznej analýze je vhodné v každú chvíľu vedieť v akej fáze je proces vyšetrovania, kto sú zaangažované osoby na strane vyšetrovateľov a aký je tok údajov. Na toto nám slúži tzv. „RACI matica“ [1]:

Zodpovednosť za činnosť (z angličtiny: “**R**esponsibility”) – kto vykonáva aktivitu.

Zodpovednosť za dodanie (z angličtiny: “**A**ccountability”) – kto zodpovedá za úspech aktivity, spolu so schvaľovacími kompetenciami.

Konzultovanie (z angličtiny: “**C**onsulted”) – kto zodpovedá za konzultovanie, dodávanie vstupných informácií pre aktivitu.

Informovanosť (z angličtiny: “**I**nformed”) – kto má prístup k informáciám súvisiacich s aktivitou, rozhodnutiami a výstupmi.

14.4.3 Digitálne forenzné laboratórium

Pre zaistenie forenznej analýzy počítačových systémov potrebujeme mať k dispozícii viacero zariadení alebo technologických postupov, ktorým sa budeme venovať v ďalších podkapitolách. Najmä v prípade firiem nie je nutné mať u seba vybudovanú potrebnú infraštruktúru. Aktivity potrebné pre forenznú analýzu počítačových systémov si môžu zazmluvniť u dodávateľov (z angličtiny: “outsourcing”). Rovnako platí, že nie každé digitálne forenzné laboratórium musí poskytovať všetky služby, môžu byť aj užšie špecializované. Laboratória musia vykonávať tzv. objektívne testy a analýzy, čo znamená, že musia byť zopakovateľné iným nezávislým laboratórium, resp. hocikým, kto dodrží zdokumentovaný postup.

Akreditácia a certifikácia

Digitálne forenzné laboratórium vo firemnom prostredí musí plniť menej podmienok ako laboratórium, ktoré participuje na súdnych vyšetrovaniach. Na tieto laboratória sú kladené primárne národné legislatívne požiadavky, ktoré musia byť splnené. Legislatíva môže vychádzať s existujúcich štandardov alebo ukladať požiadavky na ich plnenie. Medzi najznámejšie patria ISO 17025, ISO 27001, ISO 9001 a ILAC-G19:2002. Dodržaním týchto štandardov by mali vyplynúť informácie o činnosti laboratória, práce s dôkazmi, poskytované služby, ako sa spravujú a kontrolujú záznamy viažuce sa k prípadu a bezpečnostné politiky.

Ak je laboratórium súčasťou tzv. CERT/CSIRT tímov, môže sa uchádzať o certifikát CERT, ktorý je chránenou značkou Carnegie Mellon University[6]. Dôležitou súčasťou týchto tímov je vyplnený formulár o tíme v súlade s RFC 2350, ktorý by mal obsahovať predovšetkým [2]:

- dátum poslednej aktualizácie dokumentu,
- kontaktné údaje (vrátane verejných kľúčov),
- informácie o členoch tímu (môže byť aj informácia, že to nie je verejne dostupná položka),
- misia, pôsobnosť (oblasť, kde pôsobí ako autorita),

[6] https://www.sei.cmu.edu/about/divisions/cert/index.cfm

- poskytované postupy a služby,
- spôsob nahlásenia bezpečnostného incidentu.

V rámci slovenskej legislatívy definuje pravidlá a podmienky získania akreditácie pre jednotku CSIRT zákon 69/2018 z 30. januára 2018 o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov [34], v §12, §13 a §14. Rovnako tak v iných častiach definuje pravidlá fungovania takto akreditovaného tímu.

Dôležitou zložkou je spolupráca takýchto laboratórií, za účelom vymieňania si informácií a koordinovania aktivít (napr. každé laboratórium sa zameriava na inú časť forenznej analýzy). V závislosti od zamerania digitálneho forenzného laboratória pripadá do úvahy viacero možností:

ENISA (odborné centrum pre kybernetickú bezpečnosť v Európe[7]),

ENSFI (Európska sieť forenzných inštitúcií[8]),

CERT.org (divízia Carnegie Mellon University[9]).

Nástroje a infraštruktúra

Činnosti vykonávané v laboratóriách musia byť vykonávané vhodnými forenznými nástrojmi. Vhodné forenzné nástroje chápeme v zmysle, že sú otestované a overené a ich výstupy sú správne z forenzného hľadiska a použiteľné pred súdom. Túto definíciu môžu spĺňať nie len komerčné nástroje, ale aj voľne šíriteľné nástroje, či vlastné malé programy alebo skripty.

Použité nástroje musia byť dostatočne otestované, validované (objektívne testy, že nástroj funguje korektne tak, ako sa od neho očakávalo) a verifikované (potvrdenie validácie s laboratórnymi nástrojmi, technikami alebo procedúrami) [1]. Napríklad NIST[10] vykonal sériu testov digitálnych forenzných nástrojov a publikoval svoje výsledky. Pre overenie funkčnosti nástrojov je možné tieto výsledky použiť ako referenčnú vzorku.

14.5 Disky a diskové systémy

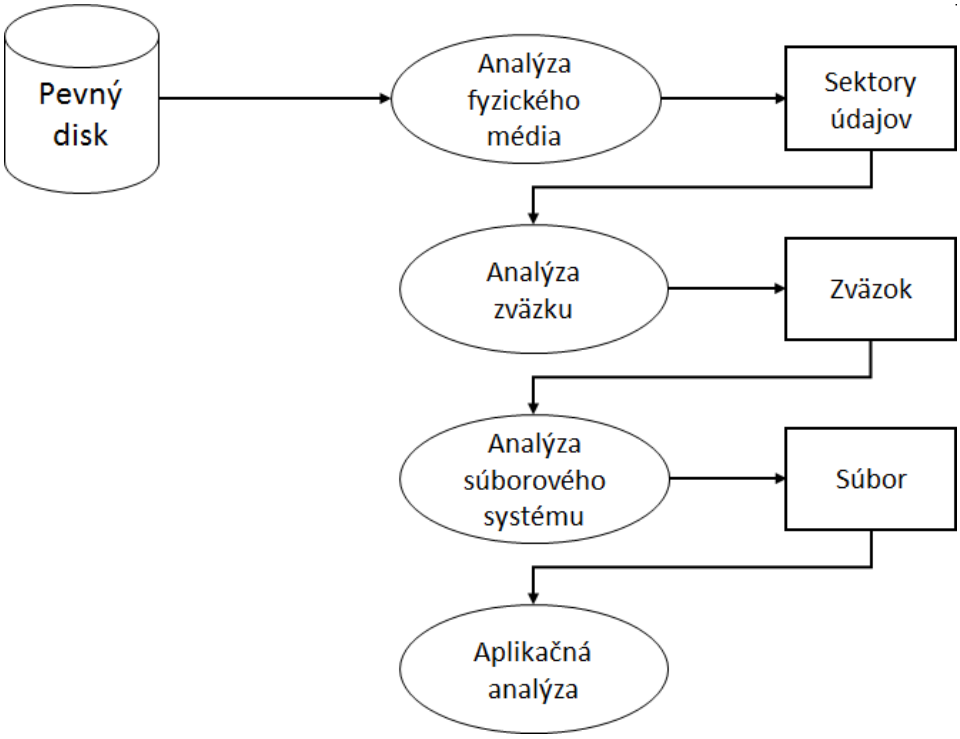
Počnúc touto kapitolou prechádzame na viac technickú časť forenznej analýzy počítačových systémov. Uvedieme si, akým spôsobom sa získavajú digitálne dôkazy z niektorých zdrojov údajov a ako k nim pristupovať.

14.5.1 Proces analýzy údajov

Pri získavaní informácií z pevných diskov musíme poznať ich fyzickú štruktúru, aby sme vedeli zvoliť najlepší prístup k obnove údajov. Postupujúc podľa obrázku 14.5, po zistení fyzickej štruktúry sa snažíme obnoviť sektory s údajmi, ktoré nám hovoria o jednotlivých partíciách a zväzkoch. Po nájdení konkrétneho zväzku sa snažíme určiť typ použitého súborového systému. Ak vieme určiť súborový systém, tak sa v ňom môžeme orientovať a prehľadávať ho. Na základe

[7] https://www.enisa.europa.eu
[8] https://enfsi.eu
[9] https://www.cert.org
[10] https://www.nist.gov

definovaných pravidiel (časový rámec, typ alebo názov súboru) sa snažíme nájsť dôležité súbory pre vyšetrovanie. Po ich nájdení realizujeme analýzu na aplikačnej úrovni (analýza adresáta mailu, zistenie použitého fotoaparátu pri konkrétnej digitálnej fotografii a iné).



Obr. 14.5: Proces analýzy údajov od fyzickej po aplikačnú úroveň [3].

14.5.2 Získanie údajov

Vychádzajúc zo základných odporúčaní, môžeme špecifikovať postup získania údajov z nosiča dát pre vyšetrovanie. Vychádzame z toho, že na počítači už boli zrealizované ostatné úkony pre zabezpečenie údajov z ostatných zdrojov a môže byť vypnutý, resp. bol vypnutý [17]:

1. Vybrať pevný disk.
2. Pripojiť ho na tzv. “write blocker”, pre blokovanie zápisu. Pri starších zariadeniach môžeme fyzicky vypnúť možnosť zápisu pomocou prepínačov (tzv. “jumper” pri pevných diskoch, SD kartu prepneme do režimu čítania a i.).
3. Pripojiť prázdne médium.
4. Pripojiť tieto zariadenie k počítaču (ak je to potrebné).
5. Vytvoriť obraz.
6. Originál je udržiavaný, chránený a dokumentovaný (reťazec zodpovednosti pre správu dôkazov).

7. Kópia (kópie) je pripravená na vyšetrovanie.

Aj pri práci s kópiou by sa mali stále používať len operácie, ktoré nespôsobujú zápis žiadnych údajov na vytvorenú kópiu.

Pripojiť prázdne médium je jednoznačný prvý krok. Ale ako garantovať, že použité médium sa dá považovať za prázdne a nemôže ovplyvniť žiadnym spôsobom vyšetrovanie? Je viacero spôsobov ako to dosiahnuť:

- Najvhodnejšie je použiť postup a softvér odporúčaný výrobcom pamäťového média[11].
- Prepísať celé médium náhodnými znakmi alebo jednotkami a na záver nulami.

Ak existuje podozrenie na použitie šifrovania disku, tak je vhodné vytvoriť kópiu pevného disku zo zapnutého zariadenia, kde máme v danom momente prístup k súborom na disku.

Digitálny obraz vs. digitálna kópia

Aj keď sme v kapitole 14.3.2 hovorili, že viacero pojmov je možné pomerne jednoducho zamieňať, tak v prípade pevných diskov môžeme rozlišovať medzi dvoma pojmami:

Digitálny obraz – jedná sa o súbor, ktorý je tvorený rovnakým bitovým poradím ako zdrojový disk.

Digitálna kópia – bitová kópia zdrojového disku na iné fyzické médium, ktoré má identickú alebo väčšiu kapacitu.

14.5.3 Vyšetrovanie

Poznáme viacero typov pamäťových médií, ako sú magnetické (pevné disky, diskety), optické (cd, dvd, blue ray) a elektronické (USB kľúče, pamäťové karty). Každé si vyžaduje špecifický prístup, napríklad pri optických médiách je najjednoduchšie zabezpečiť médium pred kontamináciou nechtiac zapísanými údajmi. Je to alebo úplne nemožné, alebo musí človek vykonať zámernú aktivitu, či musí byť obzvlášť nedbalý vo výkone svojej práce. Je to úplný opak práce s pevnými diskami, kde ich vloženie do počítača spôsobí rýchle prehľadanie operačným systémom na pozadí, čo môže vytvoriť nové údaje (minimálne zmena prístupových časov k niektorým súborom).

K týmto zariadeniam je potrebné pristupovať obvykle cez definované rozhrania, ktoré je potrebné mať k dispozícii v digitálnom forenznom laboratóriu. Poznať konkrétny typ rozhrania je dôležité, keďže rôzne generácie podporujú rôzne prístupy, ktoré môžu napomáhať k úmyselnému schovávaniu údajov.

[11] Napríklad: https://www.seagate.com/gb/en/tech-insights/how-to-ise-your-drive-master-ti/

ATA

Štandardne využívame integrované rozhranie (z angličtiny: "Integrated Drive Electronics" – IDE), pričom najpopulárnejšie je paralelné ATA / ATAPI (z angličtiny: "Advanced Technology Attachment / Packet Interface") rozhranie pre pevné disky. Spomenieme si význačné vlastnosti z hľadiska digitálnej forenznej analýzy v rámci jednotlivých generácií [3]:

ATA 1 – podpora CHS adresovania a 28-bitového LBA adresovania (vysvetlené v kapitole 14.5.5).

ATA 3 – zvýšená spoľahlivosť vďaka samostatnému testovaniu (tzv. SMART) a predstavenie používania hesiel.

ATA / ATAPI 4 – práca s 80-žilovými káblami. Uvedenie HPA (Host Protected Area).

ATA / ATAPI 6 – 48-bitové LBA adresovanie, odstránené CHS adresovanie a pridaná podpora DCO (Device Configuration Overlay).

ATA / ATAPI 7 – štandard zameraný na sériový prístup v ATA (SATA).

SATA

Zavedením SATA sa podarilo odstrániť niektoré limitácie, ktoré vznikali pri ATA, ako sú najmä veľké káble (používa len 7 kontaktov na dátovom kábli). Odpadáva nutnosť nastavovania prepínačov (z angličtiny: "jumper") do polohy "master", "slave", či "cable select", pretože každý SATA disk sa tvári ako hlavný (z angličtiny: "master") disk na vlastnom kanáli, vďaka radiču, ktorý môže byť umiestnený v počítači a tým pádom počítač nevie rozlíšiť, či komunikuje s ATA alebo SATA diskom. Posledným, ale najvýraznejším mínusom ATA rozhraní bola rýchlosť prenosu údajov (v súčasnosti pre SATA až do 6 Gbit/s [42]).

SCSI

Populárnym rozhraním pri používaní diskov v serveroch je SCSI (z angličtiny: "Small Computer Systems Interface"). Konektory SCSI môžu byť rôznych tvarov, či typov konektorov. Okrem základných typov paralelných konektorov existujú aj napríklad [52]:

- sériové (modifikácia SATA),
- optické,
- iSCSI, kde sa používa Ethernet ako prenosové médium,
- prístup cez USB zbernicu.

SCSI rozhranie nepotrebuje prítomnosť radiča a je navrhnuté ako zbernica tak, aby rôzne zariadenia mohli spolu komunikovať (nemusí sa vždy jednať o pevné disky). Z pohľadu forenznej analýzy je tiež dôležité, že disk je možné jednoducho pomocou prepínačov (z angličtiny: "jumper") prepnúť do režimu čítania, čím zabránime kontaminácii dôležitých údajov.

SSD

Aj keď je koncept SSD (z angličtiny: "Solid State Drive") známy viac ako 40 rokov, jeho výraznejšie nasadenie nastalo až v poslednej dobe. Na rozdiel od predchádzajúcich typov diskov neobsahuje žiadne pohyblivé platne, či čítaciu hlavicu. Hlavné výhody sú vyššia prenosová rýchlosť, či odolnosť voči otrasom.

Z hľadiska forenznej analýzy sa však jedná o komplikáciu pri vyšetrovaní, vďaka použitiu nových technologických prístupov. Tieto majú vplyv na vyšší výkon a životnosť SSD diskov, napríklad [13], [14], [51]:

- Pri modifikácii údajov nedochádza k ich prepísaniu v existujúcom bloku, ale údaje sa zapíšu na nové miesto. Staré miesto sa označí ako pripravené na zmazanie.
- Výrobcovia pridávajú 25 % prídavnej kapacity, ktorá sa používa z dôvodu limitovaného počtu zápisov jednotlivých buniek. Takto je možné predĺžiť životnosť zariadení. Táto zvýšená kapacita nie je nijako rozumne adresovateľná mimo SSD disku (napríklad z operačného systému) a nie je možné bezpečne zmazať uložené údaje. Pri vybratí pamäťových čipov by sme teda mohli teoreticky pristúpiť k týmto údajom. Kvôli tomu nie je možné využiť SSD disky v najmä tzv. „silových rezortoch", ale aj všade tam, kde sa prichádza do kontaktu s citlivými, či utajovanými skutočnosťami.
- Údaje na disku sa môžu javiť „rozhádzane", pretože sa využíva logické adresovanie, ktoré nemá k dispozícii celú kapacitu disku (vyššie spomenutých pridaných 25 % kapacity). V čase teda môžu údaje pôsobiť, že sú „rozhádzané" na disku.
- Na pozadí prebieha viacero procesov (niektoré sú riadené operačným systémom, napr. príkaz TRIM), ktoré postupne odstraňujú vymazané súbory. V závislosti od použitej stratégie, môže byť možné ešte niekoľko hodín po zmazaní údajov niektoré z nich obnoviť, ale nie je možné sa na to spoliehať. Keďže tieto procesy prebiehajú nezávisle, na pozadí, nepomôže ani odpojenie disku a jeho pripojenie na zariadenie s blokovaním zápisu. Pri zaistení disku a za účelom minimalizovania straty obnoviteľných zmazaných údajov je potrebné odpojiť riadiaci čip SDD disku.

Kvôli procesom na optimalizovanie a odstraňovanie údajov nastáva pri SSD diskoch problém s vyhotovením odtlačku (hash funkcia), ktorý sa môže v čase líšiť, i keď používateľ, operačný systém, či aplikácie nevykonali žiadnu zmenu.

Pri SSD diskoch poznáme viacero prípadov, kedy je práca forenzného vyšetrovateľa pomerne jednoduchá a vyššie uvedené kroky neohrozujú vyšetrovanie [13]:

- Poškodené údaje na disku zabraňujú spúšťaniu príkazu TRIM. To spôsobuje jednoduchosť práce s poškodenými súborovými systémami.
- Chybne implementované mikroprogramové vybavenie (z angličtiny: "firmware") môže spôsobiť, že sa nebudú spúšťať procesy zodpovedné za čistenie údajov.
- „Marketingové SSD disky" (lacná náhrada) reálne sa jedná o klasické tzv. „flash pamäte", ktoré nemajú inak nič spoločné s plnohodnotnými SSD diskami.

- Použitie v ultrabookoch, keďže klasický SSD disk sa nemusí vojsť do vnútra, tak sa použije PCIe rozhranie, ktoré nepodporuje príkaz TRIM (pre OS Windows).

RAID

Využívanie technológie RAID sa týka primárne serverov, ale môže sa príležitostne nájsť aj v osobných počítačoch. Pracuje na princípe spájania viacerých diskov cez špeciálny typ radiča a sledujú sa tým výkonnostné dôvody alebo spoľahlivosť a dostupnosť údajov. Jednotlivým typom [38] sa nebudeme výraznejšie venovať, len spomenieme ich základný vplyv na forenznú analýzu.

Vo všeobecnosti platí pravidlo, že by sa mali robiť zálohy celých zväzkov (napríklad pomocou živej distribúcie OS Linux na prenositeľnom médiu, viac o zväzkoch v 14.5.4). Výhodou tohto prístupu je získanie kompletnej kópie bez ohľadu na použitý typ RAID-u. Nevýhodou riešenia je, že konkrétne zapojenie do RAID-u nemusí využívať všetky sektory na každom disku. Na diskoch tak môžu zostať skryté údaje, ktoré nevieme zálohovať.

V prípade zálohovania jednotlivých diskov máme garantované získanie všetkých údajov, ktoré obsahujú. Napríklad, pri RAID 0, ktorý rozdeľuje súbor medzi viaceré pripojené disky za účelom zvýšenia výkonu, môže nastať problém. Keďže súbory sú rozdelené medzi jednotlivé disky, tak môže byť výrazný problém spojiť údaje opäť do prehľadnej formy. Naopak, pri RAID 1, ktorý duplikuje ten istý súbor na zapojené disky, toto nie je taký problém a teoreticky nám stačí získať k dispozícii jeden zo všetkých diskov, keďže každý by mal mať klon všetkých údajov.

14.5.4 Fyzická štruktúra

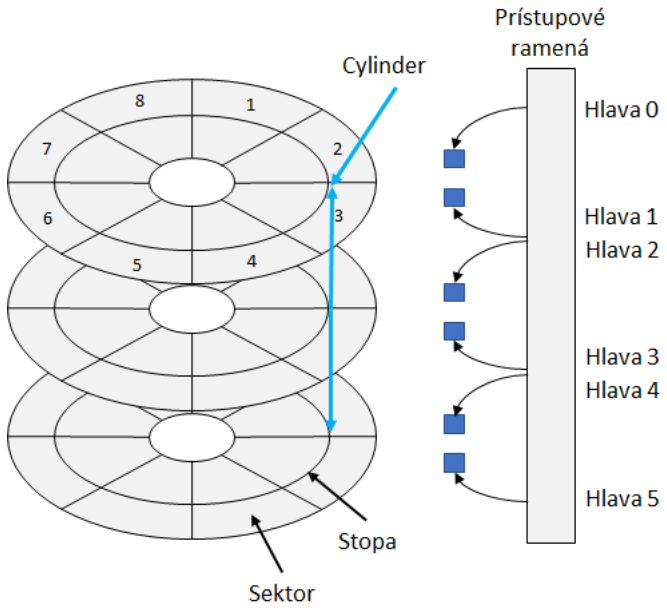
Stopa, sektor, cylinder

Pevné disky sú tvorené viacerými platňami (Obrázok 14.6), pričom každá ma z oboch strán magnetickú vrstvu. Na týchto vrstvách sa ukladajú údaje v binárnej forme. Pre čítanie aj zápis sa používajú **hlavy**, pričom každá magnetická vrstva ma svoju hlavu.

Údaje sú ukladané v sústredených kružniciach z vnútra smerom von. Každú kružnicu nazývame **stopa** (z angličtiny: “track”). Ak vezmeme všetky stopy, ktoré sú na všetkých platniach, ktorých kružnice majú rovnaký polomer, tak ich vieme označiť súhrnným pojmom **cylinder**. Počet stôp v jednom cylindri je rovný dvojnásobku počtu platní (počet povrchov jednotlivých diskov).

Stopy sú delené na menšie časti – **sektory**, pričom štandardne býva veľkosť 512 bajtov [4]. Sektor je najmenšou jednotkou pre zápis na disku. Ak teda chceme zapísať na disk napríklad súbor o veľkosti 10 bajtov, reálne sa musí prepísať 512 bajtov. Zostávajúce bajty môžu byť vyplnené napríklad nulami. Staré verzie operačných systémov (najmä DOS) zapisovali zvyšné bajty informáciami z operačnej pamäte, čo bolo bezpečnostné riziko, ale z hľadiska forenznej analýzy sa získal ďalší zaujímavý zdroj údajov.

Kým sektor je najmenšia jednotka určená pre zápis, tak viacero sektorov vytvára zhluk sektorov (tzv. „cluster“). **Cluster** je najmenšia adresovateľná jednotka na disku. Kým kedysi platila rovnosť: jeden sektor = jeden cluster, tak v dnešnej dobe môže byť na úrovni súborového systému definovaná iná veľkosť. Napríklad štandardom pre NTFS je 1 cluster = 8 sektorov (4096 bajtov).



Obr. 14.6: Fyzická štruktúra pevného disku.

Ak platí fyzické obmedzenie, že nevieme na disk zapísať menej ako veľkosť jedného sektora, tak toto obmedzenie môže platiť aj na úrovni clusteru. Záleží na konkrétnej kombinácii: operačný systém a súborový systém. Pri zápise 1 bajtu môže dochádzať k variáciám:

- od zapísania jedného bajtu, prepísanie všetkých ostatných bajtov v rámci všetkých sektorov daného clusteru (menej bežné),
- až po zapísanie jedného bajtu, prepísanie všetkých bajtov v danom sektore a ostatné sektory tvoriace konkrétny cluster zostanú nedotknuté (bežnejší prístup).

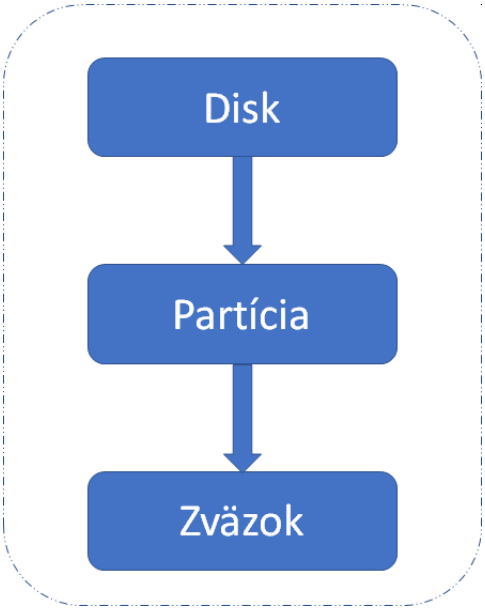
Tento nevyužitý priestor (z angličtiny: “slack space”) môže mať významný vplyv na forenznú analýzu. Na vyšetrovanom počítači sa môžu v clusteroch, ktoré ukladajú menšie súbory ako je veľkosť clustera (konkrétne s veľkosťou menšou aspoň o jeden sektor), nachádzať:

- zámerne ukryté informácie,
- neúmyselne zabudnuté dôležité informácie (podozrivý otvoril súbor, zmazal jeho obsah a uložil prázdny súbor, ktorý potom zmazal),
- ostatné informácie (obsah súborov), ktoré zostávajú vo forme zvyškov v čase pri práci s diskom.

K týmto informáciám nemáme prístup cez štandardné nástroje operačného systému (napríklad cez zobrazenie obsahu súboru), ale existujú programy, ktoré ich vedia zobraziť.

Zväzky a partície

Disky, či už jednotlivo alebo ich skupiny sa zvyknú deliť na menšie časti, ktoré sa nazývajú zväzky (z angličtiny: "volume") a partície (z angličtiny: "partition"). Často sa pracuje s modelom na obrázku 14.7, kde disk je delený na partície a tie sú delené na zväzky, pričom často sa tieto pojmy zamieňajú.



Obr. 14.7: Delenie disku na partície a zväzky.

Presnejšie vieme definovať **zväzok** ako:

- súbor adresovateľných sektorov, ktoré nemusia nasledovať fyzicky za sebou,
- operačný systém vie adresovať tieto sektory,
- existuje okrem fyzickej adresy aj logické adresovanie sektorov alebo hardvérové zariadenie (napr. radič pri RAID-e), ktoré sa stará o preklad adries.

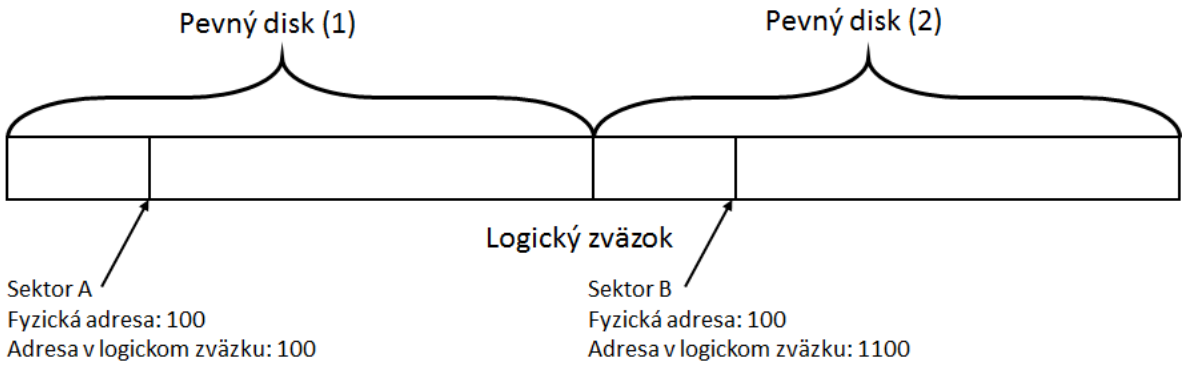
Pod pojmom **partícia** môžeme rozumieť:

- Súbor adresovateľných sektorov, ktoré nasledujú za sebou v rámci zväzku.

Z definície vyplýva, že každá partícia je zároveň aj zväzok, preto sa tieto pojmy často zamieňajú. Nie celý zväzok musí byť súčasťou partície. Čím nám vzniká nevyužitý priestor (z angličtiny: "slack space") na úrovni zväzku, kde sa môžu nachádzať skryté údaje, či už zámerne alebo ako dôsledok bežnej manipulácie so zväzkami a partíciami. Viaceré tieto definície si vieme predstaviť podľa schémy (Obrázok 14.8), kde vidíme:

- dva fyzické disky tvoria jeden logický zväzok,

- sektor A aj sektor B majú identický rozsah fyzických adries, ale ich logická adresa v rámci zväzku sa líši,
- ak by partícia bola vytvorená zo zväzku po adresu sektora B, tak časť zväzku medzi sektorom B a koncom zväzku by tvorila nevyužitú časť a potenciálny zdroj informácií.



Obr. 14.8: Logický zväzok vytvorený dvoma fyzickými diskmi [28].

Rozdeľovať disky na partície má svoje výhody:

- jednoduchá záloha a obnova systému (často sa používa oddelenie operačného systému od používateľských údajov),
- ľahké zdieľanie medzi viacerými operačnými systémami na rovnakom počítači,
- dostupnosť údajov (vďaka zmenšeniu adresovateľného priestoru sa zrýchli prístup k údajom na disku),

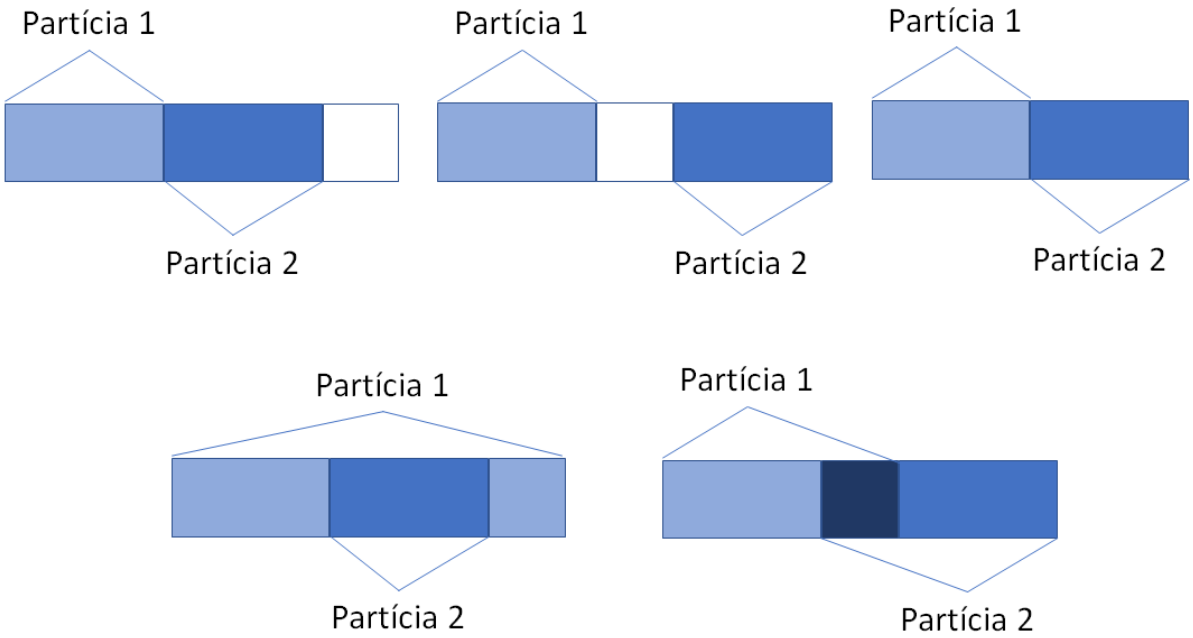
ale aj nevýhody:

- fragmentácia (čím je menší ukladací priestor, tým je väčšia pravdepodobnosť jeho zaplnenia, potom je nutné v partícií hľadať voľný priestor na celej partícii a súbory rozdeľovať do rôznych častí),
- obmedzenia (vytvorené partície obmedzujú využiteľnosť inak postačujúceho priestoru, napríklad: na dve 5 GB partície nemôžeme uložiť 10 GB databázu).

Kontrola konzistencie

Ak analyzujeme duplikát fyzického disku (diskov), na ktorom sa nachádza viacero partícií, jedným z prvých krokov je vykonanie kontroly konzistencie, či nedošlo k poškodeniu adresovania. Existuje päť základných rozdelení partícií na zväzku, s ktorými sa môžeme stretnúť (Obrázok 14.9).

Prvé tri prípady sú v poriadku a môžu bežne nastať (nevyužitie celého priestoru zväzku alebo odstránenie staršej partície na konci, či v strede, alebo využitie celej dostupnej kapacity



Obr. 14.9: Rôzne rozdelenie dvoch partícií na jednom zväzku.

zväzku). Ak narazíme na posledné dva prípady, tak sme našli chybu v konzistencii, pretože táto situácia nemôže nastať. Oba prípady majú spoločný typ chyby a tou je prekrytie priestoru dvoma partíciami. Ak by partícia 1 obsahovala operačný systém a partícia 2 používateľské údaje, tak veľmi ľahko a rýchlo by mohla nastať situácia, že:

- do spoločnej oblasti uloží operačný systém kriticky dôležité súbory pre svoj chod,
- používateľ si na svoju partíciu uloží napríklad fotky z dovolenky.

Keďže priestor na zväzku je len jeden, tak dôjde k prepísaniu kriticky dôležitých súborov a pádu operačného systému. Preto, ak narazíme na takéto prípady, je potrebné ďalej pátrať na disku a určiť (napríklad na základe začiatku súborového systému), kde partície končia a kde začínajú. Po nájdení a upravení adresovania na korektné hodnoty sa dostaneme do jedného z prvých troch prípadov rozdelenia partícií.

Kopírovanie partícií

Existuje viacero spôsobov ako vytvoriť kópiu disku, či partície. Z hľadiska programov a použitých postupov je obvykle jedno, o ktorú možnosť sa jedná. Môžeme bežné, voľne dostupné nástroje, ktoré obvykle zhotovujú verný, tzv. „surový obraz“ pamäte (kopíruje presne po jednotlivých bajtoch). Medzi najznámejšie patria:

- dd[12]

[12] https://forensicswiki.xyz/wiki/index.php?title=Dd

- dcfldd[13]

Linuxový príkaz *dd* (existuje aj jeho verzia pre Windows) vytvára obraz pomerne jednoduchým spôsobom. Avšak, ak narazí na chybu, tak má problém dokončiť vytváranie obrazu. Po vytvorení obrazu je potrebné vytvoriť samostatným príkazom odtlačok skopírovanej časti disku (z angličtiny: "hash"), aby bola garantovaná zhoda s originálom. Podporuje sériu základných prepínačov: *if*, *of*, *bs*, *skip*, *count*, *conv*. Tie definujú vstupný (*if*) a výstupný súbor (*of*), veľkosť bloku (*bs*), počet blokov, ktoré sa majú preskočiť (*skip*) alebo skopírovať (*count*) a spôsob konverzie súboru (*conv*).

Príkaz *dcfldd* funguje na veľmi podobnom princípe (jedná sa o odnož príkazu *dd*). Významným zlepšením bolo zavedenie vstavaného vytvárania odtlačkov (z angličtiny: "hash") a možnosť rozdeľovania výstupného súboru na menšie časti. To je výhodné pri zálohe veľkých partícií, a zároveň to významne zlepšuje čas potrebný pre vytvorenie odtlačkov.

Výpis 14.1: Príklad použitia dcfldd:

```
dcfldd if=/dev/zdrojovy_disk hash=md5,sha256 hashwindow=10G
    md5log=md5.txt sha256log=sha256.txt hashconv=after bs=512
    conv=noerror,sync split=10G splitformat=aa of=vystup.dd
```

Význam jednotlivých parametrov [7]:

- *if=/dev/zdrojový_disk* – vstupný súbor,
- *hash=md5,sha256* – vytvorenie odtlačku typu MD5 a SHA256,
- *hashwindow=10G* – vytvárať odtlačok každých 10 GB,
- *md5log=md5.txt* – názov výstupného súboru pre MD5 funkciu pre zhotovenie odtlačkov,
- *sha256log=sha256.txt* – názov výstupného súboru pre SHA256 funkciu pre zhotovenie odtlačkov,
- *hashconv=after* – vytváranie odtlačku po konverzii,
- *bs=512* – veľkosť bloku 512 bajtov,
- *conv=noerror,sync* – spôsob práce s výstupným súborom. Pokračuj v prípade nájdenia chyby a vyplň blok prázdnymi znakmi namiesto jeho preskočenia (užitočné pri chybných blokoch),
- *split=10G* – rozdeľovať výstupný súbor každých 10 GB,
- *splitformat=aa* – formát rozdeľovania súborov (výstup.dd.aa, výstup.dd.ab, výstup.dd.ac, ...),
- *of=vystup.dd* – názov výstupného súboru

[13] https://forensicswiki.xyz/wiki/index.php?title=Dcfldd

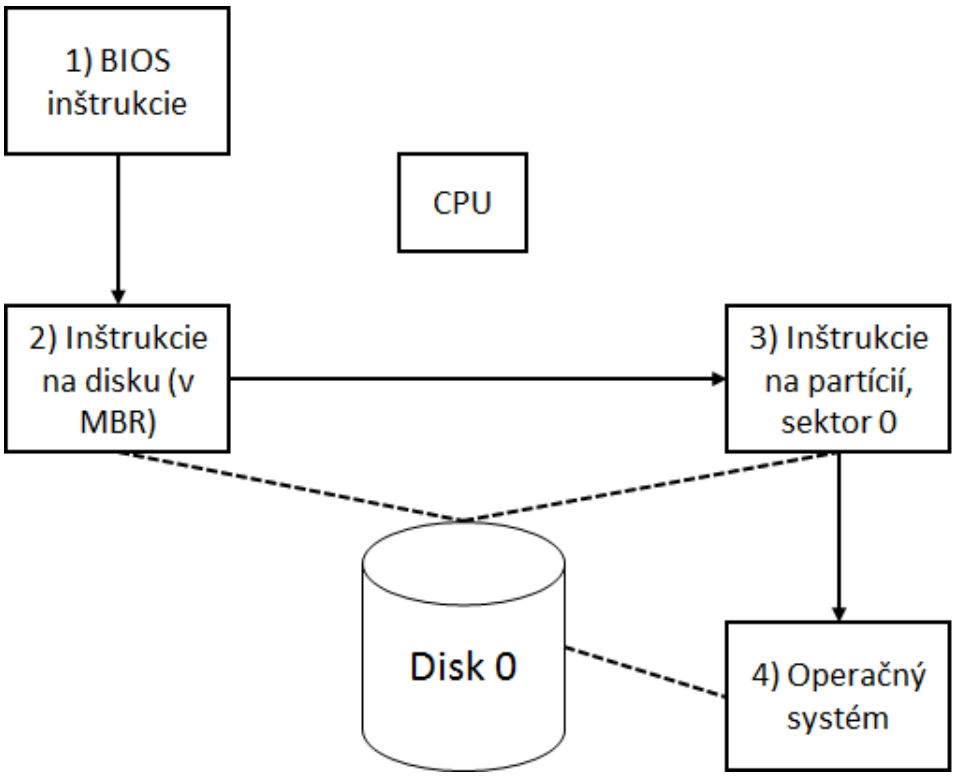
14.5.5 Logická štruktúra

Ak nadviažeme na partície, tak niekde o ich nastavení musí byť zmienka na disku. Zároveň, partície ukladajú informácie o jednotlivých súborových systémoch, ale aj súbory samotné. V ďalších podkapitolách sa pozrieme na základné pravidlá, ktoré platia na tejto úrovni abstrakcie.

Proces zavedenia systému

Pri spustení počítača procesor vie, že začína hľadať inštrukcie v špeciálnej časti pamäte bez prístupu na zápis (ROM). Obvykle sa skontrolujú jednotlivé komponenty, prípadne sa aj nastavia. Na tomto princípe funguje aj práca so systémom BIOS (alebo jeho nástupca UEFI), ktorý hľadá prítomnosť médií, s ktorými vie komunikovať (Obrázok 14.10). Po úspešnom nájdení ich začína skúmať a pozerá sa na prvý sektor na týchto médiách. Pri nájdení správneho sektoru (z angličtiny: "boot sector"), spracuje tabuľku partícií a hľadá partíciu, ktorá je určená pre zavedenie operačného systému (bootable). Po jej nájdení lokalizuje štartovacie sekvencie operačného systému a odovzdá mu riadenie.

Ak sa ľubovoľná časť z vyššie popísaného nepodarí, tak dôjde k chybe a používateľ je o nej informovaný.



Obr. 14.10: Spustenie počítača od zapnutia po zavedenie operačného systému [3].

Najrozšírenejší je tzv. „DOS (z angličtiny: "Disk Operating System") prístup" k partíciám. Využívajú sa na to dva základné spôsoby: MBR a GPT, ktoré si bližšie predstavíme.

Endianita

Pri práci s pamäťovými médiami alebo forenznými kópiami potrebujeme vedieť ako sú ukladané údaje na tej najnižšej úrovni, aby sme ich vedeli správne interpretovať. Štandardne sa pojem endianita viaže k údajom na úrovni bajtov, ale v niektorých prípadoch sa môže jednať aj o spôsob ukladania na úrovni bitov. Ak sa plánovane rozhodujeme, ktorý typ endianity máme použiť na úrovni bitov, tak je odporúčané použiť ten istý typ, ako máme na úrovni bajtov.

Existujú dva základné typy endianity:

1. Big-endian.
2. Little-endian.

Big-endian ukladá najvýznamnejší bajt na prvé miesto, ostatné bajty nasledujú postupne s klesajúcou významnosťou. Big-endian si vieme predstaviť ako klasický zápis čísel, s ktorými sa stretávame v bežnom živote. Používa sa pri prenose údajov cez internet, je optimálny na testovanie operácií so znamienkom a je jednoduchý pre kontrolu človekom.

Little-endian ukladá na prvé miesto najmenej významný bajt. Ak počítač načítava prirodzené číslo postupne po bajtoch, je tento spôsob preňho rýchlejší a vhodnejší pre bežné počítanie. Jedná sa o lepšiu formu pre zachovanie jednoduchej presnosti pri číslach, ktoré sú väčšie ako je prirodzená veľkosť v systéme (v dnešnej dobe 32 alebo 64-bitové systémy).

Ak máme číslo v šestnástkovej sústave 0x1234567890AB, tak zápisy po jednotlivých bajtoch pomocou Big-endian a Little-endian budú vyzerať takto:

- Big-endian: 12|34|56|78|90|AB
- Little-endian: AB|90|78|56|34|12

Oba prístupy majú rôznych zástancov od výrobcov procesorov až po vývoj operačných systémov. Samozrejme platí, že ak použijeme číslo v nesprávnom zápise, než v akom ho daná časť systému očakáva, tak môžeme spôsobiť nekorektné správanie tejto časti systému alebo chybné uloženie údajov. Existuje viacero jednoduchých metód[14], ako zistiť s akou endianitou pracuje konkrétny systém. Pri súborových systémoch je toto štandardne dopredu známe a definované.

Okrem týchto prístupov, existuje aj tretí typ – tzv. Middle-endian, ktorý nie je na toľko rozšírený ako predchádzajúce dva, takže sa mu bližšie nebudeme venovať.

Adresovanie

Ako sme spomínali v kapitole 14.5.4, pevné disky majú svoju fyzickú štruktúru. Z nej boli odvodené aj spôsoby adresovania a prístupu k jednotlivým sektorom na disku.

[14] https://www.geeksforgeeks.org/little-and-big-endian-mystery/

CHS (Cylinder-Head-Sector) adresovanie

Staršia metóda vychádza z fyzických komponentov, ktoré pevné disky obsahujú. Pre určenie adresy konkrétneho sektora potrebujeme vedieť, na akom cylindri sa nachádza. Potom potrebujeme určiť presnú stopu, čo zistíme pomocou čísla hlavy, ktorá s ňou pracuje. Na záver potrebujeme určiť, ktorý je to sektor v rámci nájdenej stopy. Položky majú definované tieto rozsahy v rámci ATA špecifikácie / používané v starších BIOS systémoch:

- Cylinder (C): 16/10 bitov.
- Hlava (H): 4/8 bitov.
- Sektor (S): 8/6 bitov.

S týmto spôsobom adresovania vedia pracovať aj novšie zariadenia (najčastejšie USB kľúče), aj keď je ich princíp fungovania na fyzickej úrovni úplne iný a neobsahujú napríklad magnetické platne. Jedná sa o podporu skôr na logickej úrovni, keďže podpora CHS adresovania bola odstránená v špecifikácii ATA 6 [33].

Nevýhodou tohto adresovania je, že jeho maximálna kapacita pre disky (pri správnej podpore BIOS-u) je 8,1 GB, čo je v dnešnej dobe nepostačujúce. Z tohto dôvodu sa prešlo na nový spôsob adresovania LBA.

LBA (Logical Block Addressing)

V dnešnej dobe sa LBA adresovanie stalo štandardom. Využíva sa jediné číslo, ktoré reprezentuje číslo sektora od začiatku disku (zväzku, partície, ...). Jeho výhodou je, že je úplne nezávisle na geometrii disku.

Keďže viaceré súborové systémy stále používajú CHS adresovanie, tak potrebujeme zabezpečiť konverziu medzi oboma spôsobmi adresovania.

Prvou základnou informáciou je adresa prvého sektoru:

- pri CHS: 0, 0, 1,
- pri LBA: 0.

Vidíme, že posun je v začiatočnej adrese. Všeobecný vzorec pre prevod je:

```
LBA = (((Cylinder * Pocet_hlav_na_cylinder) + Hlava) *
    Pocet_sektorov_na_stopu) + Sektor -1,
```

kde Cylinder, Hlava a Sektor reprezentujú čísla z CHS adresovania. LBA má aj iné použitie ako len na adresovanie fyzických adries na disku (tzv. „fyzická adresa“), ale používa sa aj v rámci zväzkov, či partícií (napr. logická adresa zväzku – viď. obrázok 14.8).

Príklad 1: Prevod CHS na LBA adresovanie

Máme adresu CHS (2, 3, 4). Vieme, že počet hláv na cylinder je 16 a počet sektorov na stopu je 63.

Výpis 14.2: Riešenie na základe vzorca:

```
LBA = (((2 * 16) + 3) * 63) + 4 - 1
LBA = 2208
```

Príklad 2: Prevod LBA na CHS adresovanie

Máme LBA adresu 1204. Vieme, že počet hláv na cylinder je 16 a počet sektorov na stopu je 63.

$$1204 = (((Cylinder * 16) + Hlava) * 63) + Sektor - 1$$

$$1205 = (((Cylinder * 16) + Hlava) * 63) + Sektor$$

Sektor na stope získame vydelením čísla 1205 číslom 63. Celočíselný výsledok opäť vynásobíme číslom 63. Tento výsledok odpočítame od pôvodné čísla a získame číslo sektora v rámci stopy.

$$1205 \ div \ 63 = 19$$

$$19 * 63 = 1197$$

$$1205 - 1197 = 8$$

Keď vieme číslo sektora, tak môžeme ďalej pracovať s číslom 1197 (1204 + 1 - 8 = 1197)

$$1197 = ((Cylinder * 16) + Hlava) * 63,$$

vydelíme číslom 63

$$19 = (Cylinder * 16) + Hlava,$$

pre určenie hlavy a cylindra. Vydelíme číslom 16. Celočíselný výsledok je číslo cylindra a zvyšok po delení reprezentuje hlavu, pretože musí platiť:

$$(19 - Hlava),$$

16 je prirodzené číslo

$$19 \ div \ 16 = 1$$

$$19 \ mod \ 16 = 3$$

$$LBA \ 1204 = CHS \ 1, 3, 8$$

Môžete si vyskúšať vyriešiť prevod LBA 2208 na CHS adresu a prevod CHS 1,3,8 na LBA adresu a uvidíte, že prídete k hodnotám, ktoré boli v príkladoch použité ako zadanie.

MBR

MBR (z angličtiny: "Master Boot Record") sa používa pre správu partícií od roku 1983, aj keď pre niektoré jeho nevýhody už začína byť na ústupe, najmä pri novších osobných počítačoch.

Všetky informácie o MBR sa ukladajú v nultom sektore na disku (prvých 512 bajtov na disku). Nachádzajú sa tu:

- Inštrukcie pre zavedenie systému (z angličtiny: "boot code"), ktorý obsahuje informácie o tom, ako má počítač spracovať tabuľku partícií a ako vyhľadať operačný systém. Veľkosť: 466 bajtov.
- Tabuľka partícií s definovanými primárnymi partíciami (maximálne 4 primárne partície). Veľkosť: 64 bajtov.
- Magické číslo (z angličtiny: "Magic number"): 0x55AA, ktoré sa nachádza na konci MBR sektora. Veľkosť: 2 bajty.

Každý záznam v tabuľke partícií má 16 bajtov (Tabuľka 14.1). Pod pojmom základný údaj (v tabuľke) rozumieme informáciu, bez ktorej by sme nevedeli identifikovať a pracovať s danou partíciou. Vidíme, že dôležité základné údaje tvoria výhradne adresy partície, ostatné nie sú nevyhnutné pre prácu s partíciami. Bližšie informácie o adresovaní sú uvedené v kapitole 14.5.5.

Tabuľka 14.1: Záznam v tabuľke partícií.

Rozsah v bajtoch	Popis	Základný údaj?
0-0	Identifikátor pre závadzanie	Nie
1-3	Úvodná CHS adresa	Áno
4-4	Typ partície	Nie
5-7	Posledná CHS adresa	Áno
8-11	Prvá LBA adresa	Áno
12-15	Veľkosť v sektoroch	Áno

Ak je k dispozícií typ partície, môže nám to uľahčiť identifikovanie súborového systému, ktorý sa na nej používa. Najznámejšie druhy partícií si môžete pozrieť v tabuľka 14.2. Pri tabuľke partícií treba mať na pamäti, že údaje sú ukladané pomocou Little-endian a teda bajty treba preusporiadať, aby boli ľahko čitateľné človekom.

Pre CHS adresovanie máme vyhradené v oboch prípadoch po 3 bajty (24 bitov). Ich rozdelenie medzi cylindre, hlavy a sektory je takéto:

- Hlava: <0,7>,
- Sektor: <8,13>,
- Cylinder: <14,23>.

Tabuľka 14.2: Vybrané druhy partícií [3].

Typ partície	Popis
0x00	Prázdna partícia
0x07	NTFS, HPFS, exFAT
0x0B	FAT32 s CHS adresovaním
0x0C	FAT32 s LBA adresovaním
0x0E	FAT16 s LBA adresovaním
0x0F	Rozšírená partícia s LBA adresovaním
0x82	Linux swap
0x83	Natívny súborový systém Linuxu
0xA8	Mac OSX (UFS)
0xEE	GPT protective MBR

Príklad na partície

Na obrázku 14.11 máme ukážku MBR záznam vrátane použitých partícií (štyri rôznofarebné pásy v dolnej časti obrázku).

Vieme z toho identifikovať tieto záznamy o partíciách:

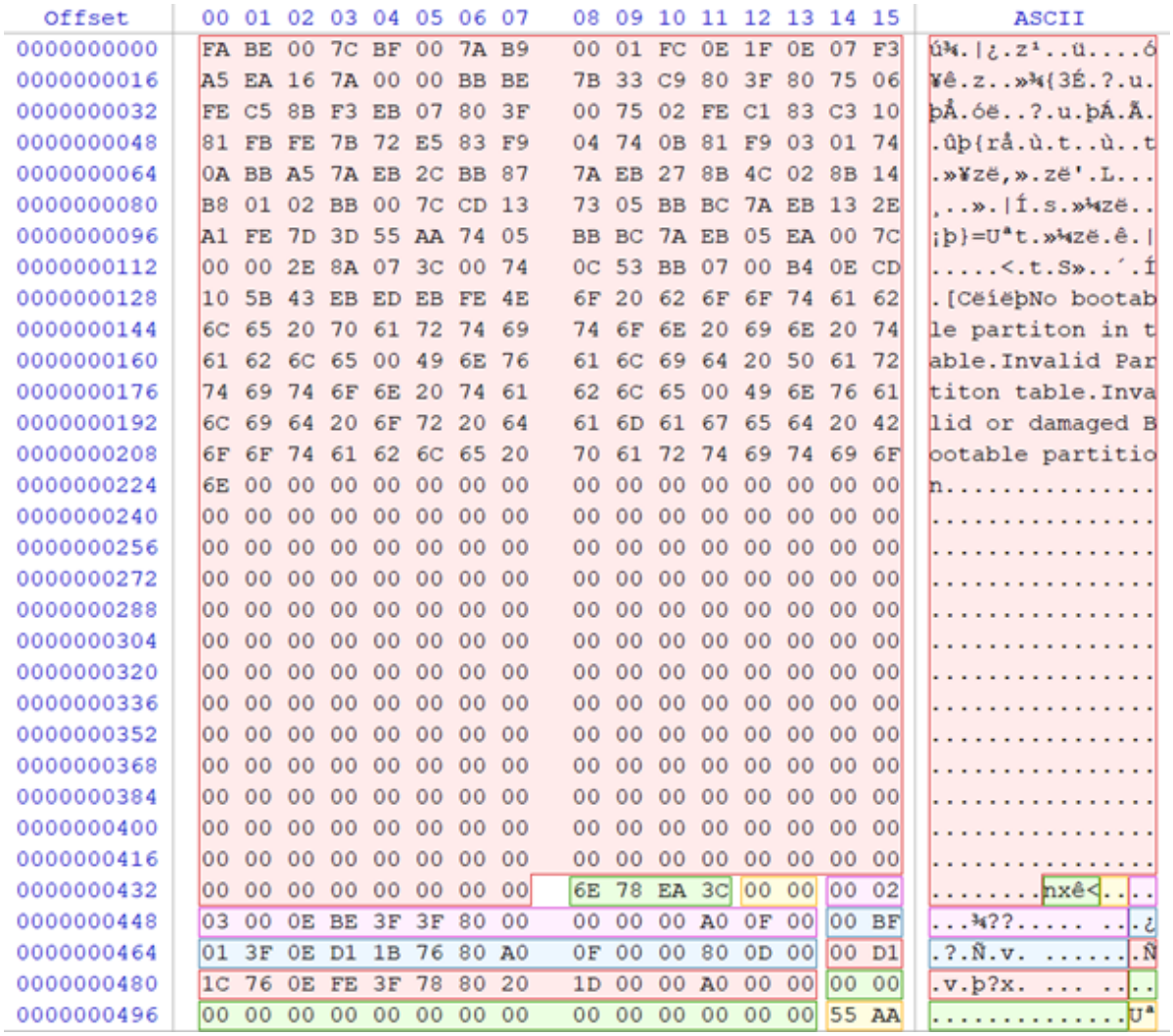
1. 00 02 03 00 0E BE 3F 3F 80 00 00 00 00 A0 0F 00
2. 00 BF 01 3F 0E D1 1B 76 80 A0 0F 00 00 80 0D 00
3. 00 D1 1C 76 0E FE 3F 78 80 20 1D 00 00 A0 00 00
4. 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Keďže táto reprezentácia je dosť neprehľadná, tak ju upravíme na základe tabuľky 14.1 do tabuľky 14.3.

Tabuľka 14.3: Príklad partícií.

Partícia č.	ID	CHS začiatok	Typ partície	CHS koniec	LBA začiatok	LBA veľkosť
1	00	02 03 00	0E	BE 3F 3F	80 00 00 00	00 A0 0F 00
2	00	BF 01 3F	0E	D1 1B 76	80 A0 0F 00	00 80 0D 00
3	00	D1 1C 76	0E	FE 3F 78	80 20 1D 00	00 A0 00 00
4	00	00 00 00	00	00 00 00	00 00 00 00	00 00 00 00

Dôležitou vecou, ktorú netreba prehliadnuť je rozdiel pri CHS a LBA. Kým pri CHS máme presnú adresu začiatku aj konca, tak pri LBA máme zadanú adresu začiatku a následnú veľkosť v sektoroch. Najjednoduchšia situácia je pri partícií 4, ktorá obsahuje samé nuly a teda nie je použitá. Analýzu ostatných si vysvetlíme. Všetky partície majú spoločné to, že neobsahujú kód pre zavedenie systému (v stĺpci ID majú všetky hodnotu 00).



Offset	00 01 02 03 04 05 06 07	08 09 10 11 12 13 14 15	ASCII
0000000000	FA BE 00 7C BF 00 7A B9	00 01 FC 0E 1F 0E 07 F3	ú¾.|¿.z¹..ü....ó
0000000016	A5 EA 16 7A 00 00 BB BE	7B 33 C9 80 3F 80 75 06	¥ê.z..»¾{3É.?.u.
0000000032	FE C5 8B F3 EB 07 80 3F	00 75 02 FE C1 83 C3 10	þÅ.óë..?.u.þÁ.Ã.
0000000048	81 FB FE 7B 72 E5 83 F9	04 74 0B 81 F9 03 01 74	.ûþ{rå.ù.t..ù..t
0000000064	0A BB A5 7A EB 2C BB 87	7A EB 27 8B 4C 02 8B 14	.»¥zë,».zë'.L...
0000000080	B8 01 02 BB 00 7C CD 13	73 05 BB BC 7A EB 13 2E	¸..».|Í.s.»¼zë..
0000000096	A1 FE 7D 3D 55 AA 74 05	BB BC 7A EB 05 EA 00 7C	¡þ}=Uªt.»¼zë.ê.|
0000000112	00 00 2E 8A 07 3C 00 74	0C 53 BB 07 00 B4 0E CD	.....<.t.S»..´.Í
0000000128	10 5B 43 EB ED EB FE 4E	6F 20 62 6F 6F 74 61 62	.[CëíëþNo bootab
0000000144	6C 65 20 70 61 72 74 69	74 6F 6E 20 69 6E 20 74	le partiton in t
0000000160	61 62 6C 65 00 49 6E 76	61 6C 69 64 20 50 61 72	able.Invalid Par
0000000176	74 69 74 6F 6E 20 74 61	62 6C 65 00 49 6E 76 61	titon table.Inva
0000000192	6C 69 64 20 6F 72 20 64	61 6D 61 67 65 64 20 42	lid or damaged B
0000000208	6F 6F 74 61 62 6C 65 20	70 61 72 74 69 74 69 6F	ootable partitio
0000000224	6E 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	n.....
0000000240	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
0000000256	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
0000000272	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
0000000288	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
0000000304	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
0000000320	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
0000000336	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
0000000352	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
0000000368	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
0000000384	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
0000000400	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
0000000416	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
0000000432	00 00 00 00 00 00 00 00	6E 78 EA 3C 00 00 00 02	........nxê<....
0000000448	03 00 0E BE 3F 3F 80 00	00 00 00 A0 0F 00 00 BF	...¾??..... ...¿
0000000464	01 3F 0E D1 1B 76 80 A0	0F 00 00 80 0D 00 00 D1	.?.Ñ.v. ....Ñ
0000000480	1C 76 0E FE 3F 78 80 20	1D 00 00 A0 00 00 00 00	.v.þ?x. ... .
0000000496	00 00 00 00 00 00 00 00	00 00 00 00 00 00 55 AA	..............Uª

Obr. 14.11: Ukážka MBR záznamu s partíciami.

Ako získať z daných záznamov konkrétne adresy? Netreba zabúdať, že LBA adresy sú uložené obvykle vo formáte Little-endian, teda je potrebné ich preusporiadať, aby sme s nimi vedeli jednoducho pracovať. Na druhú stranu CHS adresovanie tvoria tri bajty (napríklad 02 03 00 pre prvú partíciu), ale interpretovať ich treba takto:

- 1. bajt – číslo hlavy,
- 6.-7. bit z 2. bajtu a k nim pripojený 3. bajt – číslo cylindra,
- 0.-5. bit z 2. bajtu – číslo sektora.

Partícia č. 1

- CHS začiatočná adresa je 0x02 03 00 (binárne: 0000 0010 0000 0011 0000 0000)

  - Hlava: 2
  - Sektor: 3
  - Cylinder (podčiarknutá časť): 0
- CHS koncová adresa je 0xBE 3F 3F (binárne: 1011 1110 0011 1111 0011 1111)
  - Hlava: 109
  - Sektor: 63
  - Cylinder (podčiarknutá časť): 63
- LBA adresa začiatku partície je 0x00 00 00 80, teda 128. sektor v poradí.
- Veľkosť partície podľa LBA je 0x00 0F A0 00, teda 1 024 000 blokov.

Partícia č. 2

- CHS začiatočná adresa je 0xBF 01 3F (binárne: 1011 1111 0000 0001 0011 1111)
  - Hlava: 191
  - Sektor: 1
  - Cylinder (podčiarknutá časť): 63
- CHS koncová adresa je 0xD1 1B 76 (binárne: 1101 0001 0001 1011 0111 0110)
  - Hlava: 209
  - Sektor: 27
  - Cylinder (podčiarknutá časť): 118
- LBA adresa začiatku partície je 0x00 0F A0 80, teda 1 024 128. sektor v poradí.
- Veľkosť partície podľa LBA je 0x00 0D 80 00, teda 884 736 blokov.

Partícia č. 3

- CHS začiatočná adresa je 0xD1 1C 76 (binárne: 1101 0001 0001 1100 0111 0110)
  - Hlava: 209
  - Sektor: 28
  - Cylinder (podčiarknutá časť): 118
- CHS koncová adresa je 0xFE 3F 78 (binárne: 1111 1110 0011 1111 0111 1000)
  - Hlava: 254
  - Sektor: 63
  - Cylinder (podčiarknutá časť): 120
- LBA adresa začiatku partície je 0x00 1D 20 80, teda 1 908 864. sektor v poradí.

- Veľkosť partície podľa LBA je 0x00 00 A0 00, teda 40 960 blokov.

To, že sme sa nemýlili si môžeme potvrdiť analýzou prvých dvoch partícií na obrázku 14.12. Pre analýzu bol použitý program Active Disk Editor[15].

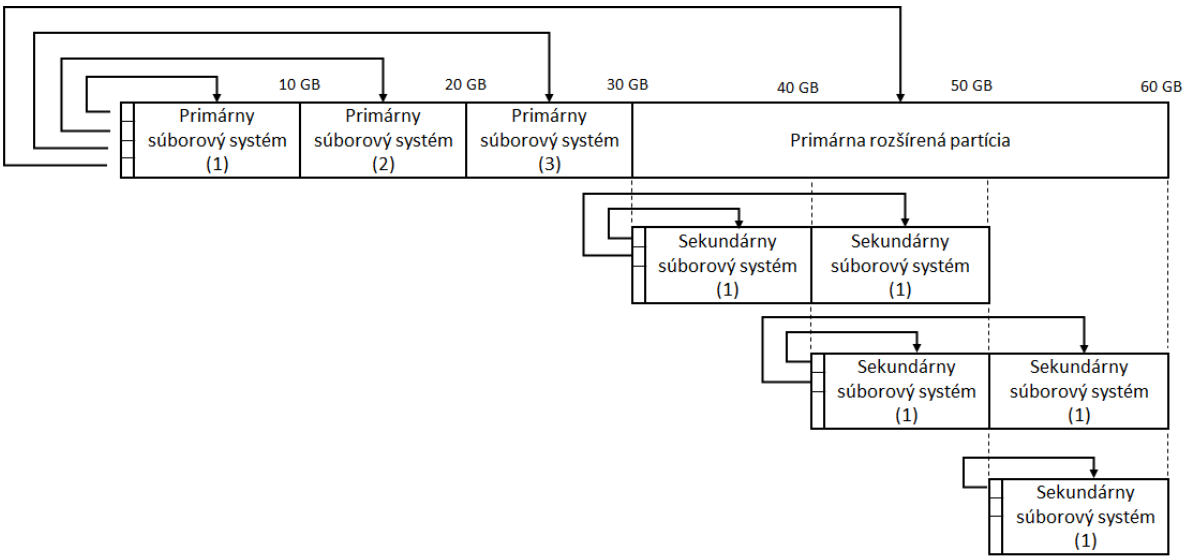
Partition 1 (FAT, 500 MB)	**446**	
Active partition flag (80 = active)	446	0x00
Start head	447	2
Start sector (bits 0-5), cylinder (bits 6-7)	448	0x03
Start cylinder (lower 8 bits)	449	0x00
File system ID	450	0x0E
End head	451	190
End sector (bits 0-5), cylinder (bits 6-7)	452	0x3F
End cylinder (lower 8 bits)	453	0x3F
First sector	454	128
Total sectors	458	1 024 000
Partition 2 (FAT, 432 MB)	**462**	
Active partition flag (80 = active)	462	0x00
Start head	463	191
Start sector (bits 0-5), cylinder (bits 6-7)	464	0x01
Start cylinder (lower 8 bits)	465	0x3F
File system ID	466	0x0E
End head	467	209
End sector (bits 0-5), cylinder (bits 6-7)	468	0x1B
End cylinder (lower 8 bits)	469	0x76
First sector	470	1 024 128
Total sectors	474	884 736
Partition 3 (FAT, 20.0 MB)	**478**	
Partition 4 (Unused)	**494**	
Signature (55 AA)	510	55 AA

Obr. 14.12: Analýza MBR záznamu so zameraním na prvé dve partície.

Rozšírené partície

MBR ponúka možnosť štyroch primárnych partícií, čo v dnešnej dobe už nemusí byť postačujúce. Z tohto dôvodu vieme pracovať aj s konceptom rozšírených partícií (v OS Windows známe aj ako logické partície – obrázok 14.13). Princípom je, že primárna logická partícia má v MBR svoju počiatočnú adresu. V prvom sektore sa nachádza informácia o tejto partícií (začiatok a dĺžka) a o adrese sekundárnej logickej partícií. Sekundárna logická partícia opäť obsahuje informácie o sebe a ďalšej partícií. Jedná sa o lineárne zreťazený zoznam, kde posledná partícia uchováva len informácie o sebe. Nevýhodou tohto prístupu je, že ak dôjde k chybe v rámci zoznamu, tak strácame prístup k všetkým rozšíreným partíciám, ktoré sa nachádzajú za touto chybou.

[15] https://www.disk-editor.org/index.html



Obr. 14.13: Použitie rozšírených partícií [3].

Koncept primárnych aj rozšírených partícií ponúka možnosti skrývania údajov. Keďže MBR nekontroluje žiadnym spôsobom konzistenciu a správnosť informácií, jednoduchou editáciou tabuľky partícií vieme skryť existenciu partície. Nájsť ju by sa nám podarilo až po kontrole adresných rozsahov jednotlivých partícií a zistení, či sa v celkovom adresnom rozsahu nenachádzajú medzery. Pri nájdení medzier by bolo potrebné prešetriť, či je niektorá z nich tvorená skrytou partíciou alebo sa tam nachádzajú iné stopy z predchádzajúceho rozdelenia zväzku.

Podobne, pri rozšírených partíciách môžeme v zreťazenom zozname vynechať informáciu o jednej z partícií tak, že informáciu o jej začiatku (v jej predchodcovi) prepíšeme informáciou o jej nasledovníkovi. Tým spôsobíme medzeru v adresnom priestore, ale nie v lineárne zreťazenom zozname, ktorý pokračuje normálne do konca. Opäť je možné tento krok odhaliť pri starostlivej kontrole adries jednotlivých rozšírených partícií.

GPT

MBR postupne stráca svoje postavenie a je v dnešnej dobe bežne nahradzovaná s GPT (z angličtiny: “GUID Partition Table”). Môže za to viacero nedostatkov, najmä:

- Limitovaný počet primárnych partícií.
- 32 bitové LBA adresovanie (maximálne 2 TB partície).

GPT prekonáva tieto obmedzenia a okrem toho zavádza základnú kontrolu konzistencie pomocou algoritmu CRC32. Používať sa začala s nástupom 64-bitových procesorov od Intelu, ktoré zároveň prestali používať BIOS a miesto neho zaviedli EFI (známe aj ako UEFI, z angličtiny: “Unified Extensibile Firmware Interface”). Práve UEFI má, okrem iného, na starosti spracovanie GPT údajov. Pri adresovaní sa používa 64 bitov, ktoré umožňujú adresovať až 16 EB. MBR postačovalo pre ukladanie informácií, vrátane tabuľky partícií jeden sektor a aj

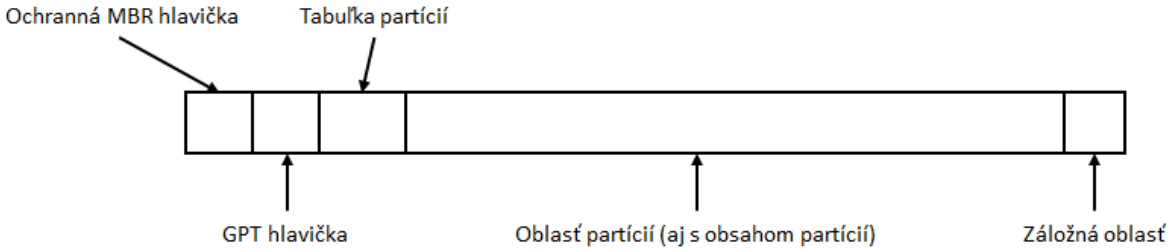
z dôvodu nedostatku miesta sa nedali niektoré obmedzenia ľahko vyriešiť. Na obrázku 14.14 vidíme základnú štruktúru GPT, ktorá reprezentuje tieto časti:

Ochranná MBR (z angličtiny: "Protective MBR", adresa LBA 0) – jedná sa o klasickú MBR štruktúru, ktorá obsahuje jedinú partíciu o veľkosti celého disku (v rámci bitových obmedzení pre adresovanie), ktorá je typu 0xEE (GPT protective MBR). Zabezpečuje spätnú kompatibilitu so staršími systémami, aby nedošlo k formátovaniu disku. UEFI reálne s touto časťou nepracuje.

GPT hlavička (adresa LBA 1) – obsahuje magické číslo ("EFI PART"), kontrolnú sumu (CRC32) hlavičky aj tabuľky partícií, adresu primárnej a záložnej GPT hlavičky veľkosť údajovej časti partícií ako aj počiatočnú adresu tabuľky partícií.

Tabuľka partícií (adresa LBA 2 – 3) – môže obsahovať záznamy až pre 128 partícií. Každý záznam má 128 bajtov. V tabuľke 14.4 sú uvedené atribúty záznamu jednej partície.

Záložná oblasť: nachádza sa za údajovou časťou partícií, ktorá obsahuje zálohu GPT hlavičky aj tabuľky partícií.



Obr. 14.14: Základná štruktúra GPT.

Pri GPT platí, že si treba dávať pozor na to, že rovnako ako pri MBR, sú údaje ukladané vo formáte Little-endian.

Tabuľka 14.4: GPT záznam o partícií [3].

Rozsah v bajtoch	Popis	Základný údaj?
0-15	GUID typ partície	Nie
16-31	Unikátne GUID číslo	Nie
32-39	Začiatočná LBA adresa partície	Áno
40-47	Koncová LBA adresa partície	Áno
48-55	Atribúty partície	Nie
56-127	Meno partície (Unicode)	Nie

Označenie typov partícií je komplikovanejšie ako pri MBR a tvorí až 16 bajtov (vo formáte 4-2-2-2-6 bajtov) [15]. Pomerne známy je typ C12A7328-F81F-11D2-BA4B-00A0C93EC93B, ktorý reprezentuje EFI systémovú partíciu. Príklad GPT záznamu a jeho analýzu môžeme vidieť na obrázku 14.15 a obrázku 14.16.

Offset	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	ASCII
0000000000512	45	46	49	20	50	41	52	54	00	00	01	00	5C	00	00	00	EFI PART....\...
0000000000528	77	90	4A	FB	00	00	00	00	01	00	00	00	00	00	00	00	w.Jû..........
0000000000544	AF	6D	70	74	00	00	00	00	22	00	00	00	00	00	00	00	¯mpt...."....
0000000000560	8E	6D	70	74	00	00	00	00	EE	D2	C2	48	28	6B	DA	45	.mpt....îÒÂH(kÚE
0000000000576	8A	2D	8C	6C	1F	65	2C	5A	02	00	00	00	00	00	00	00	.-.l.e,Z.....
0000000000592	80	00	00	00	80	00	00	00	23	0A	16	57	00	00	00	00	........#..W....
0000000000608	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0000000000624	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0000000000640	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0000000000656	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0000000000672	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0000000000688	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0000000000704	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0000000000720	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0000000000736	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0000000000752	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0000000000768	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0000000000784	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0000000000800	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0000000000816	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0000000000832	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0000000000848	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0000000000864	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0000000000880	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0000000000896	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0000000000912	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0000000000928	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0000000000944	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0000000000960	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0000000000976	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0000000000992	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0000000001008	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....

Obr. 14.15: Ukážka GPT záznamu.

HPA

Host Protected Area alebo aj HPA bolo zadefinované v ATA 4 špecifikácii. Vkladá na koniec disku oblasť, ktorá je pre bežného používateľa neviditeľná. Pomocou príkazu IDENTIFY_DEVICE vieme štandardne zistiť veľkosť konkrétneho disku. Pri použití HPA to neplatí a nepodarilo by sa nám ju odhaliť. Je nutné použiť príkaz READ_NATIVE_MAX_ADDRESS [8]. Ak sú hodnoty týchto príkazov rôzne, tak sa nám podarilo odhaliť HPA oblasť. Niektoré nástroje (napríklad: Sleuthkit) vedia detegovať prítomnosť HPA.

Pre prístup do tejto oblasti vieme použiť príkaz SET_MAX_ADDRESS, kde zadáme vyššie zo získaných dvoch čísel. Z hľadiska forenznej analýzy je zaujímavé, že vieme nastaviť špeciálny bit tak, aby vykonaná zmena nebola permanentná (vieme využiť aj existujúce implementované riešenia, napríklad setmax[16]). Netreba sa však na to vždy spoliehať a je dobré mať urobenú zálohu dostupných údajov predtým, pretože môže dôjsť aj k strate všetkých údajov,

[16] https://www.win.tue.nl/~aeb/linux/setmax.c

GPT Header	000	
Signature (EFI PART)	000	45 46 49 20 50 41 52 54
Revision	008	00 00 01 00
Header size	012	92
Header CRC	016	77 90 4A FB
(reserved)	020	00 00 00 00
Current LBA	024	1
Backup LBA	032	1 953 525 167
First usable LBA	040	34
Last usable LBA	048	1 953 525 134
Disk GUID	056	EE D2 C2 48 28 6B DA 45 8A 2D 8C 6C 1F 65 2C 5A
Starting LBA of entr...	072	2
Number of entries	080	128
Entry size	084	128
CRC of partition arr...	088	23 0A 16 57
(reserved)	092	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00...

Obr. 14.16: Analyzovaný GPT záznam v programe Active Disk Editor.

ak nie je firmvér korektne implementovaný.

Niektoré hardvérové zariadenia s blokovaním zápisu vedia povoliť príkaz SET_MAX_ADDRESS, ak je správne nastavený bit, ktorý operáciu nerobí permanentnou.

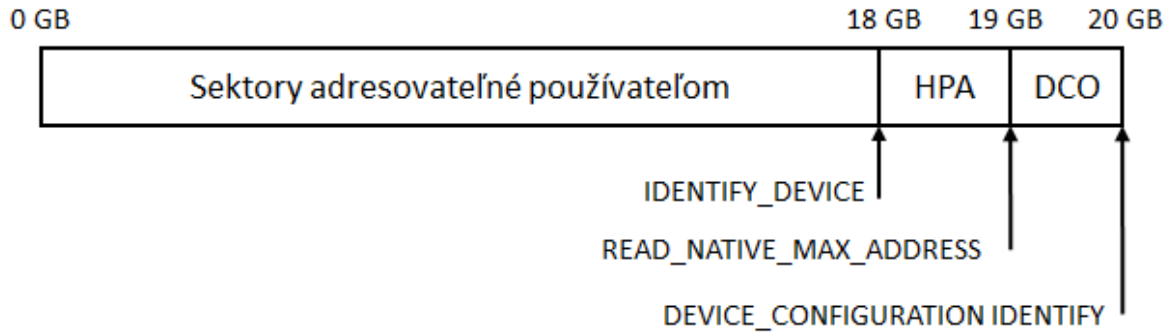
DCO

DCO (z angličtiny: “Device Configuration Overlay”) bolo zavedené v špecifikácii pre ATA 6. Použitie DCO nevylučuje možnosť použitia HPA, čím vieme dosiahnuť dva rôzne typy skrytých oblastí na disku. Pre zistenie prítomnosti potrebujeme použiť príkaz DEVICE_CONFIGURATION_IDENT Ak výsledok porovnáme s príkazmi IDENTIFY_DEVICE a READ_NATIVE_MAX_ADDRESS a hodnota je rôzna (viď. obrázok 14.17), tak sme našli DCO oblasť.

Na rozdiel od HPA, je odstránenie DCO permanentná a nezvratná operácia, ktorú realizujeme príkazom DEVICE_CONFIGURATION_RESET. Z tohto dôvodu je potrebné mať istotu, že chceme vykonať tento typ operácie a určite je potrebné mať dopredu urobené kópie ostatných oblastí [3].

14.6 Súborové systémy

Základnou a primárnou vlastnosťou súborového systému je ukladanie údajov na zariadenie (pevné disky, USB kľúče, pamäťové karty a iné) a ich opätovné sprístupnenie opračnému systému alebo používateľovi. Všetky ostatné poskytované vlastnosti sú sekundárne. Okrem toho vieme o ňom povedať:



Obr. 14.17: HPA a DCO oblasť.

- Súborový systém je nezávislý na operačnom systéme.
- Rôzne súborové systémy môžu byť podporované na rôznych operačných systémoch.

Pozostáva zo štrukturálnych a používateľských údajov. Štrukturálne údaje určujú spôsob ukladania a následnej reprezentácie údajov. Cieľom je, aby používateľ, či systém mohli pristupovať k uloženým údajom rýchlo, ľahko a efektívne. V priebehu času začali súborové systémy poskytovať aj ďalšie informácie, ktoré však neplnia jeho primárnu úlohu (napríklad žurnálovanie, čas prístupu k súboru a iné).

Z reálneho sveta vieme použiť analógiu s knižnicami, kde knihy tvoria „používateľské údaje“. Avšak, mať knižnicu plnú kníh je takmer až nepoužiteľné, pokiaľ nevieme efektívne nájsť konkrétnu knihu. Túto úlohu plnia „štrukturálne údaje“, ktoré hovoria o rozdelení kníh do kategórií a umiestnení týchto kategórií v priestore. Zároveň, v prípade prístupu iného používateľa (vypožičanie knihy), vedia poskytnúť informáciu o dočasnej neprístupnosti hľadanej knihy.

Ako sme už uviedli existujú dva typy údajov v súborových systémoch:

Primárne (esenciálne) – potrebné pre ukladanie a načítavanie súborov. Týmto údajom môžeme dôverovať.

Sekundárne (neesenciálne) – pre plnohodnotnejšie a pohodlnejšie použitie súborového systému. Je dobré ich mať, keďže poskytujú prídavné informácie (prístupové časy, tvorca súboru a iné). Týmto údajom by sme nemali bezvýhradne veriť, keďže môžu byť modifikované bez vplyvu na primárne vlastnosti operačného systému.

Prečo nemôžeme veriť sekundárnym údajom? Môžu byť ľahko meniteľné aj používateľom samotným. Zároveň, ak aj operačný systém vyžaduje nastavenie niektorých údajov (napríklad: žiadny z MAC časov nemôže byť v budúcnosti), tak nám môže stačiť pripojiť tento súborový systém k inému typu operačného systému. V tom prípade to už nebude požadovaný údaj (požadovaná kontrola tohto údaju bude chýbať), alebo údaj aktualizovaný výhradne operačným systémom. Takéto rozdiely sa vyskytujú aj medzi jednotlivými verziami OS Windows, ešte výraznejšie je to medzi OS Windows a jednotlivými linuxovými distribúciami.

14.6.1 Všeobecný súborový systém

Poznáme päť úrovni abstrakcie údajov v súborových systémoch (Obrázok 14.18):

1. **Úroveň súborového systému**: Poskytuje základné informácie o súborovom systéme. Platí tu pravidlo: Všetky sú rovnaké a zároveň každý je iný. Aj keď máme ten istý súborový systém, tak sa líši napríklad vo svojej celkovej veľkosti, veľkosti klastru alebo inom parametri. Definuje používané údajové štruktúry. Údaje na tejto úrovni môžeme chápať ako formu „mapy“ súborového systému, ktorá nám hovorí, kde a ako nájdeme jednotlivé údajové štruktúry.

2. **Úroveň obsahu**: Reprezentuje vlastný obsah súborov, ktorý je uložený v štandardizovaných jednotkách (bloky, klastre a i.). Zvyčajne tvorí najväčšiu časť súborových systémov.

3. **Úroveň metadát**: Opisné údaje o údajoch, ako napríklad kde sú uložené, aké sú veľké, prístupové časy k údajom. Nemusí obsahovať názov súboru a nenachádzajú sa v nej vlastné údaje tvoriace obsah súboru. Pri FAT súborovom systéme sa môže jednať napríklad o záznam súboru v rámci adresára. Pri NTFS sa môže jednať o MFT záznam, či inode štruktúru pri linuxových súborových systémoch (napr. Ext verzie 2 až 4).

4. **Úroveň názvov súborov**: Jedná sa o rozhranie použiteľné pre prácu človekom. Je veľmi podobná prekladu IP adries na doménové mená (radšej zadávame napríklad www.kinit.sk ako 37.9.175.131), kedy sa počítač postará o preklad doménového mena na správnu IP adresu. Podobne aj tu počítač k úrovni metadát pripája názov súboru, najčastejšie sa jedná o informácie nachádzajúce sa v štruktúrach určených pre adresáre.

5. **Aplikačná úroveň**: časť, ktorá plní sekundárne úlohy súborového systému, ktoré sú potrebné počas zápisu alebo čítania súboru. Môžu byť však užitočné pre lepšiu použiteľnosť, ako aj počas vyšetrovania (môže v nich zostať viac zostatkových dôkazov). Môžeme medzi ne radiť žurnálové systémy, používateľské kvóty, či prístupové práva.

V ďalšej podkapitole sa pozrieme na možnosti použitia forenznej analýzy na jednotlivé vrstvy abstrakcie súborového systému.

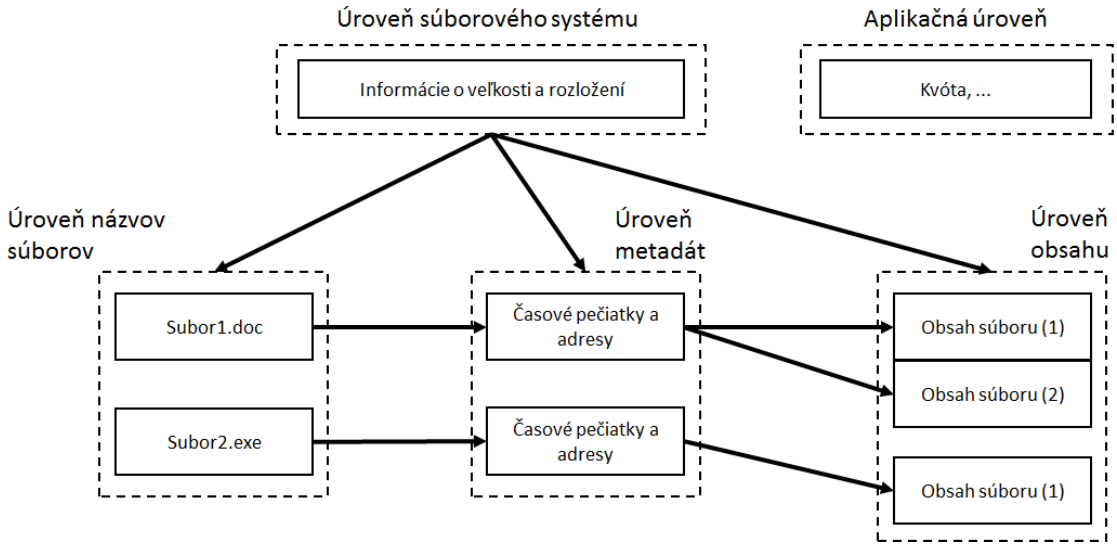
Analýza podľa vrstiev abstrakcie

Každá z vrstiev nám ponúka iné typy informácií, ktoré z nej vieme extrahovať. Zároveň, každá môže napomáhať podozrivému v schovávaní informácií a robiť tým pátranie zložitejším.

1) Úroveň súborového systému

Aplikovaním forenznej analýzy vieme identifikovať o aký konkrétny súborový systém sa jedná, čím je špecifický, kde a akým spôsobom má uložené údaje. Môžeme identifikovať tiež jeho verziu.

Pri analýze súborového systému na zväzku treba pamätať, že súborový systém nemusí využívať celý priestor na pamäťovom médiu. Najčastejšie (nie zámerne) môže nastať situácia, kedy súborový systém spája dokopy viacero sektorov do jednej adresovateľnej jednotky a celkový počet sektorov zväzku nie je deliteľný bezo zvyšku touto adresovateľnou jednotkou. V



Obr. 14.18: Úrovne abstrakcie súborového systému.

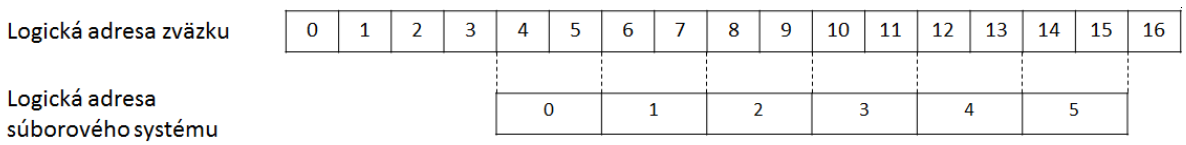
zostávajúcom priestore (pri vedomom nastavení aj v rozsahu niekoľko gigabajtov) môžu byť ukryté informácie, či už zámerne, alebo ako pozostatok predchádzajúceho používania zväzku v inej konfigurácií. Nevyužitý priestor zväzku sa obvykle nachádza na jeho konci.

2) Úroveň obsahu

Údaje sú ukladané v rámci sektorov, alebo údajových jednotiek (viacero spojených sektorov dokopy, ich pomenovanie záleží od konkrétneho súborového systému). Každý z nich môže mať viacero adries, minimálne sú to dve:

- Fyzická adresa: počítaná od začiatku fyzického média.
- Logická adresa: počítaná od začiatku zväzku.

Na obrázku 14.19 vidíme, že sektor 16 nám tvorí nevyužitý priestor (spomínané v úrovni súborového systému). Prvé sektory (v tomto prípade 0-3 adresy zväzku) zvyknú tvoriť základné štruktúry súborového systému. Až od adresy 4 začína prvá logická adresa súborového systému. Je dôležité ju vedieť lokalizovať, pretože od tohto bodu ďalej (ak nie je súborovým systémom určené inak) nájdeme obsah samotných súborov.



Obr. 14.19: Logická adresa zväzku a logická adresa súborového systému [3].

Údaje sa štandardne ukladajú od začiatku obsahovej časti. Pri dlhodobom používaní zväzku môže dochádzať k tzv. „fragmentácií“, kedy nevieme nájsť dostatočný počet voľných údajových jednotiek za sebou a tak musíme súbor uložiť na viacero rôznych miest na disku. Na toto sa používajú rôzne alokačné stratégie pre hľadanie dostupných údajových jednotiek. Tomuto sa nebudeme hlbšie venovať v rámci tejto knihy, ale je potrebné na to pamätať pri analýze.

Viacero súborových systémov vie identifikovať zlé údajové jednotky a označiť ich za poškodené, aby sa s nimi viac nepracovalo. Bolo to potrebné najmä pri starších typov diskov, ktoré nemali dobrú kontrolu konzistencie. Ak máme k dispozícií súborový systém, ktorý má túto funkcionalitu, tak údajové jednotky označené ako poškodené by mali byť jednou z prvých vecí, ktoré skontrolujeme. Útočník totiž vie označiť aj korektné údajové jednotky za chybné a tým ich vyradí z používania. Málokedy sa robí ďalšia kontrola poškodených častí disku. Ukryté údaje sa dostávajú mimo „hľadáčik“ viacerých forenzných nástrojov, ale správne nástroje pre akvizíciu údajov zobrazujú správu o chybných sektoroch (alebo údajových jednotkách), ktoré sú dostupné pre manuálnu kontrolu.

Vieme použiť viacero techník analýzy:

Prezeranie údajových jednotiek – ak vieme začiatok obsahovej časti a vieme veľkosť jednej údajovej jednotky, tak sa vieme posúvať po zväzku a kontrolovať obsah aj týmto pomerne jednoduchým spôsobom. Vieme kde sa nachádzajú údaje a zisťujeme o aké údaje sa jedná.

Hľadanie na logickej úrovni súborového systému – zadávame kľúčové frázy, ktoré sa postupne vyhľadávajú po jednotlivých údajových jednotkách. Vieme, čo chceme nájsť, ale nevieme či a kde sa to na zväzku nachádza. Slabinou tohto spôsobu je fragmentácia. Ak hľadáme kľúčovú frázu, ktorá sa nachádza v súbore a prechádza viacerými údajovými jednotkami, tak v dôsledku fragmentovania sa nemusia nachádzať za sebou a takéto vyhľadávanie zlyhá.

Vyšetrovanie nealokovaných sektorov alebo údajových jednotiek – zameriame sa len na tie časti zväzku, o ktorých súborový systém tvrdí, že nie sú alokované. Môžeme nájsť množstvo údajov, ktoré boli zmazané (či už úmyselne alebo neúmyselne).

Kontrola konzistencie – využívame pri nej vstupy z úrovne metadát. Napríklad: všetky údaje na disku musia mať práve jedny metadáta (ak sa nejedná o špecifický typ odkazu). Môžeme ju použiť aj na kontrolu chybovosti sektorov, ktoré majú svoj obsah štandardne vyplnený nulami. Ak nájdeme sektor, ktorý je označený za chybný, ale je vyplnený inými údajmi, tak sa môže jednať o skryté údaje.

Vyšetrovanie môžu skomplikovať techniky, ktoré sa zameriavajú na skrývanie dôkazov. Najčastejším spôsobom je prepísanie nealkovaných jednotiek pomocou samých núl, jednotiek alebo náhodnými údajmi. V prípade náhodných údajov je na tejto úrovni abstrakcie nemožné zistiť, či boli údaje zámerne poškodené špecializovaným nástrojom. Zistiť to vieme, až použitím metód z vyšších úrovní abstralcie súborového systému. Výhodou môže byť, ak sa podozrivý spoľahne na funkcie operačného systému, ktoré sa nie vždy musia správať tak, ako očakáva. Napríklad:

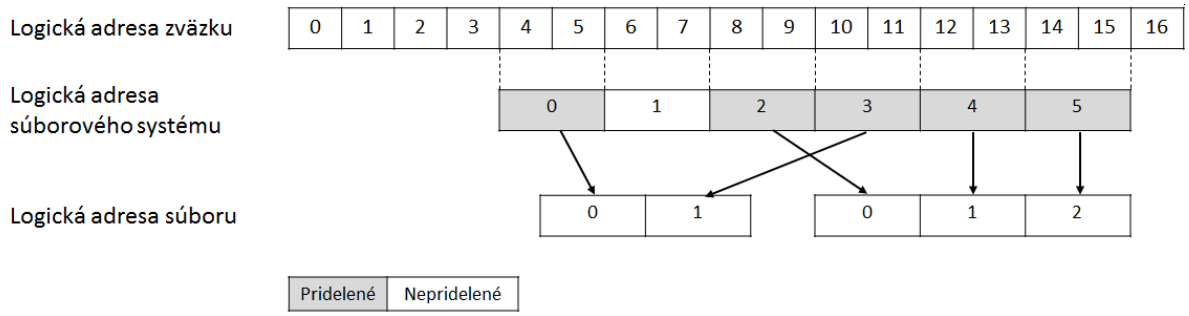
- Ak zvolíme prepísanie súboru samými nulami a následne ho dáme zmazať, tieto kroky sa nemusia odohrať v tomto poradí aj na úrovni operačného systému. Ten si môže zapamätať

vo vyrovnávacej pamäti, že má prepísať obsah súboru, ale toto môže zrušiť, keď zistí, že by mal meniť obsah už neexistujúceho súboru.

- Podobne ako v predchádzajúcom prípade, ak chceme prepísať nealokované údajové jednotky (už zmazaný súbor), tak to operačný systém nemusí vykonať, keďže by mal prepisovať časti zväzku, ktoré sa aj tak nepoužívajú.
- Pri prepisovaní obsahu vychádzame z toho, že operačný systém prepíše existujúce údajové jednotky. Operačný systém však môže rozhodnúť o alokovaní nových údajových jednotiek, kde zapíše napríklad požadované nuly a pôvodný obsah zostane nedotknutý.

3) Úroveň metadát

Pri tejto úrovni začíname pracovať s ďalším typom adresovania a to logickými adresami súborov. Ako môžeme vidieť na obrázku 14.20, logické adresovanie súborov má svoj základ logickom adresovaní súborového systému. V predchádzajúcich častiach sme spomínali fragmentáciu súborov na rôzne časti na disku. S takto rozdeleným súborom by sa nám nedalo pracovať, preto ho potrebujeme mať na vyššej úrovni abstrakcie zložený do jedného celku. Môžeme vidieť, že aj keď súbory sú na disku rozdelené do rôznych údajových jednotiek, ktoré za sebou nenasledujú, tak samotný súbor vždy číslujeme od jeho nultej dátovej jednotky (relatívny štart súboru) a sekvenčne pokračujeme až po jeho koniec.



Obr. 14.20: Logické adresovanie súborov [3].

Metadáta sú zvyčajne ukladané spoločne v jednej časti, ktorá je určená súborovým systémom.

Nevyužitý priestor

Ako sme už spomínali v predchádzajúcich kapitolách, tak údajové jednotky nemusia byť využité celé pre uloženie konkrétneho súboru. Platí pravidlo, že určite sú prepísané tie sektory z údajovej jednotky, ktoré obsahujú aspoň jeden bajt ukladaného súboru. Ostatné sektory v údajovej jednotke môžu zostať nedotknuté. V starších operačných systémoch dochádzalo aj k prepísaniu s údajmi z operačnej pamäte, čím sa mohli získať ďalšie zaujímavé dôkazy.

Obnova zmazaných súborov na úrovni metadát

Metadáta nám pomáhajú určiť, ktoré údajové jednotky vytvárajú súbor a v akom poradí. Pri zmazaní súboru sa môže časť týchto údajov prepísať alebo sa len pridá príznak o tom, že sa

môžu opätovne použiť. V závislosti od operačného systému môže byť obnovovanie zmazaných súborov úplne jednoduché a stačí sa pozrieť na tieto údaje a získať obsah zmazaného súboru.

Pri obnove zmazaných súborov pomocou metadát musíme mať na pamäti, že mohlo dôjsť k viacerým prípadom. Za všetky vyberáme tieto:

- Súbor bol zmazaný, jeho metadáta boli zneplatnené. Jeho obsah bol neskôr prepísaný novým súborom, ale využila sa iná časť pamäte pre uloženie metadát nového súboru. Pôvodné metadáta sú stále k dispozícii na disku, ale už ich nevieme použiť pri obnove zamazaného súboru, ktorého obsah bol prepísaný.

- Súbor bol zmazaný, jeho metadáta boli zneplatnené. Metadáta boli prepísané metadátami nového súboru, ale pôvodný obsah súboru zostal nedotknutý. Obsah sa síce na disku naďalej nachádza, ale nevieme ho obnoviť jednoduchým spôsobom na úrovni metadát. Vieme kontrolovať nealokovaný priestor, hľadať sektory s údajmi a pokúsiť sa ich pospájať dokopy.

- Súbor bol zmazaný, jeho metadáta boli zneplatnené. Vytvorí sa nový súbor s novými metadátami, pričom pôvodne metadáta sa zachovajú, prepíše sa len obsah súboru. Nový súbor zmažeme. Jeho metadáta prepíšeme ďalším novým súborom, ktorý bude mať uložený svoj obsah niekde inde na disku ako pôvodný súbor. Týmto sme došli do situácie, kedy metadáta zo zmazaného súboru ukazujú na obsah iného zmazaného súboru, ku ktorému nám už neexistujú metadáta. Nemusíme vedieť rozlíšiť, že zmazaný obsah súboru nepatrí k zneplatneným metadátam.

Týmto spôsobom vieme získať viacero metadát ukazujúcich na rovnakú údajovú jednotku, pričom žiadne z metadát nemusia byť správne a viažuce sa k údajom na disku. Problém sa dá ešte viac skomplikovať, ak používame v čase rovnaké názvy súborov (pri vyššej úrovni abstrakcie) alebo rovnaké údajové typy súborov.

Kompresia a „riedke“ súbory

Súborový systém môže automaticky komprimovať súbory. Z pohľadu aplikácie, ktorá zapisuje údaje sa môže jednať o transparentný proces a nemusí si byť vedomá, že jej údaje sú komprimované. Komprimované údaje by mali byť pred vyšetrovaním dekomprimované. Komprimácia môže byť použitá nie len na úrovni obsahu súborov, ale aj na úrovni samotných súborov.

Pri tzv. „riedkych súboroch“ (z angličtiny: “sparse files”), ktoré obsahujú množstvo núl, sa nemusia zapisovať údajové jednotky, ktoré sú vyplnené len nulami. Niektoré súborové systémy zapíšu nulu do oblasti, kde sa zapisuje adresa údajovej jednotky. Ak žiadny súbor nemôže obsahovať takúto adresu, tak je jasné, že sa jedna o údajovú jednotku plnú núl.

Ďalšou výzvou na tejto úrovni môže byť šifrovanie (aj heslo aj použitý algoritmus). Opäť platí, že by sme mali dešifrovať všetky údaje pri vyšetrovaní, aby sme ich vedeli správne analyzovať. Šifrovanie sa môže viazať na:

Obsah súborov – metadáta zostávajú nedotknuté.

Zväzky – šifrované sú aj metadáta súborov. Niekedy však nie je šifrovaný celý zväzok, kde sa nachádza operačný systém.

Pri vyšetrovaní sa na úrovni metadát používa viacero techník analýzy:

Prehliadanie metadát – zisťovanie prídavných údajov (MAC časy, veľkosť, umiestnenie) o súboroch. Jedná sa o bežnú činnosť súčasných analytických nástrojov.

Logický pohľad na súbor – na základe metadát sa vieme pozrieť na aktuálny obsah súboru. Prehliadame tie údajové jednotky, na ktoré ukazujú metadáta.

Vyhľadávanie na logickej úrovni súborov – je podobné hľadaniu na logickej úrovni súborového systému, ale vďaka správnemu prepojeniu údajových jednotiek môže vyhľadávanie fungovať aj na disku s fragmentovanými súbormi.

Prehľadávanie nealokovaného priestoru – ak zostali zachované metadáta po zmazaných súboroch, tak s nimi môžeme pracovať takmer ako s nezmazanými súbormi.

Vyhľadávanie na základe rôznych atribútov v metadátach – môžeme zúžiť vyhľadávanie na špecifický časový interval, na súbory vytvorené konkrétnym používateľom, súbory s nastavením konkrétnych prístupových práv a iné.

Kontrola konzistencie – nachádza sa každý vytvorený súbor v adresári? Preverujeme, či údajové jednotky používané súbormi sú alokované, snažíme sa identifikovať skryté údaje.

Na tejto úrovne abstrakcie je viacero sofistikovanejších možností ako zaviesť vyšetrovateľa alebo len skryť údaje. Tak ako pri predchádzajúcej úrovni vieme prepísať metadáta nulami, ale toto robí túto metódu jednoducho detekovateľnú. Nemá logiku nájsť takto „ostrovček“ núl v skupine metadát s rôznym zastúpením núl a jednotiek. Pokročilejšie je použitie náhodného zoskupenia núl a jednotiek. Ideálne je však použiť náhodné údaje pre jednotlivé položky (prístupové časy, prístupové práva), ktoré sa nijako neviažu k pôvodnému súboru. Najpokročilejšou metódou je presunutie nepoužitých metadát na koniec, prostredníctvom vymieňania s platnými údajmi. Po takomto vymieňaní môžu byť metadáta zmazaných súborov prepísané nulami a už to nebude podozrivé. Jedná sa však o časovo náročnú metódu.

4) Úroveň názvov súborov

Ako vyplýva z názvu, tak k úrovni metadát pridávame názov súboru. Výhodou je, že práca so súbormi sa stáva zrozumiteľnejšia aj pre ľudí. Adresáre a súbory sa obvykle chápu spoločne, líšia sa len svojim obsahom, kde adresáre obsahujú definované údajové štruktúry pre vnorené adresáre, či súbory. Pre väčšinu súborových systémov (a všetky najrozšírenejšie) platí, že musí existovať koreňový adresár, ktorý obsahuje iné priečinky a súbory. Každý súbor aj priečinok v súborovom systéme musí mať vo svojej ceste zahrnutý aj koreňový adresár.

Hlavnou úlohou je nájdenie pozície koreňového adresára, aby sme vedeli ďalej vykonávať analýzu jednoduchým spôsobom.

Tak ako sme popísali komplikácie pri prepisovaní údajov na úrovni metadát, rovnako sa situácia komplikuje aj spojenie metadát s názvom súboru, ktorý môže tiež podliehať prepisovaniu pri mazaní a vytváraní súborov. Niektoré súborové systémy však zlučujú úroveň metadát

a názvov súborov do jednej údajovej štruktúry, teda tento typ komplikácie odpadá. Na tejto úrovni vieme použiť napríklad tieto metódy analýzy:

Vypísanie názvov súborov a priečinkov v súborovom systéme – môžeme vypísať všetky súbory, na základe prístupovej cesty, časti mena alebo koncovky.

Vyhľadávanie mien súborov. Hľadá sa časť mena, koncovky – môžeme použiť metadáta pre hľadanie mien súborov.

Kontrola konzistencie – zisťuje sa, či každý názov súboru má priradené metadáta. Nemôže existovať platný názov súboru bez toho, aby k nemu existovali metadáta a mal prepojenie na samotný obsah súboru.

Možnosti pre zmazanie sú pomerne jednoduché. Stačí premenovať súbor. Treba však poznať správanie a štruktúry súborového systému. Pri premenovaní sa môže nový názov uložiť na koniec štruktúry a pôvodný názov zostane nedotknutý. V takomto prípade môžeme preorganizovať štruktúru názov. Tento prístup je náročný, má však veľmi dobré výsledky.

5) Aplikačná úroveň

Jediná úroveň, ktorá nie je nevyhnutná pre základnú činnosť súborového systému. Dokáže však zrýchliť činnosť súborového systému alebo ho učiniť stabilnejším. Najbežnejšou aplikáciou je žurnálovanie. Ak počas procesu zapisovaniu na disk dôjde k neštandardnému stavu (pád OS, výpadok napájania a iné), môže sa dostať súborový systém dostať do nekonzistentného stavu. Počas vytvárania nových súborov môžu byť vytvorené aj kompletné časti niektorých úrovní (existujú metadáta, názov súbor, samotný obsah súboru), ale nemusia byť navzájom prepojené. Samozrejme, niektorá z vytváraných častí môže byť neúplná alebo môže úplne chýbať.

Z tohto dôvodu operačné systémy na začiatku vykonávajú kontrolu súborového systému a hľadajú takéto nekonzistencie. Pri väčších súborových systémoch môže ísť o časovo náročný proces. Použitie žurnálu umožňuje túto kontrolu výrazne zrýchliť a aj opraviť niektoré z chybných záznamov.

Žurnál je súbor, ktorý ako taký je zoznam budúcich zmien v súborovom systéme. Môže sa jednať o vytváranie nového súboru, vrátane jeho obsahu. Najskôr sa vytvorí popis týchto činností, spolu s platnými údajmi a až potom sa začne súbor reálne vytvárať na disku. Kontrola súborového systému je tým výrazne zrýchlená a stačí skontrolovať, či zmeny, ktoré sú zapísané v žurnály, boli aj zrealizované. Ak sa ich nepodarilo zrealizovať, sú dve platné stratégie:

1. Dokončiť činnosti zaznamenané v žurnály.
2. Zahodiť všetky zmeny. Reverzne odstrániť všetky realizované zmeny nedokončenej operácie.

Žurnál je zaujímavý z hľadiska vyšetrovania a môže obsahovať informácie o súboroch, ku ktorým už nie je možné sa dostať, môže obsahovať čas zmazania, či aktualizovania vyšetrovaných súborov. Pri súborových systémoch, ktoré mažú metadáta (napr. Ext3, Ext4), vieme získať aj názvy zmazaných súborov.

Samozrejme, žurnálovací systém má len limitovanú kapacitu a preto obsahuje len malé časové okno z hľadiska používania súborového systému. V princípe vieme rozdeliť žurnály na tri základné typy:

1. **So spätným zápisom** – ukladajú sa len údaje o metadátach, ktoré však môžu byť na disk zapísané skôr. Najmenej spoľahlivý spôsob.

2. **Usporiadaný** – Najskôr sa uložia metadáta do žurnálu, po zrealizovaní zápisov na disk sa označia ako zrealizované.

3. **Úplný žurnál** – Metadáta aj dáta (obsah súboru) sú najskôr zapísané do žurnálu, až potom sa zapíšu na disk. Je to najstabilnejší stav, avšak z hľadiska výkonu najhorší, pretože na disk sa reálne zapisuje dvakrát (najskôr do žurnálovacieho súboru, potom do cieľovej lokality).

Ďalšie techniky forenznej analýzy použiteľné na tejto úrovní sú:

Filtrovanie súborov podľa ich aplikačného určenia – sledujú sa primárne hlavičky a pätičky súborov, z ktorých sa zisťujú známe typy súborov. Umožňuje to rýchlejšiu manipuláciu so súbormi.

Filtrovanie podľa typov súborov – nemusíme nutne filtrovať len podľa jednej koncovky, ale môžeme filtrovať celé skupiny, ako napríklad obrázky, dokumenty a iné.

Kontrola konzistencie prípony súboru a jeho reálneho obsahu

Medzi najčastejšie spôsoby, ako skomplikovať vyšetrovanie na tejto úrovni je prepisovanie žurnálovacieho súboru (buď zmazanie, alebo zapísanie nepodstatných údajov).

Pri práci so súbormi môže dôjsť k nahradeniu údajov v hlavičke a pätičke za údaje iného typu súboru, čím sa súbor nedostane medzi tie, ktoré majú byť analyzované (dokument, ktorý sa tvári ako obrázok môže byť prehliadnutý, ak hľadáme len dokumenty). Pomerne jednoduchou technikou je zmena prípony na „txt“ alebo inú podobnú, ktoré vlastne nemajú žiadnu hlavičku, či pätičku. Použité nástroje môžu tieto súbory prehliadnuť a nerobiť ani kontrolu obsahu súboru oproti jeho vnútornej štruktúre.

14.6.2 FAT

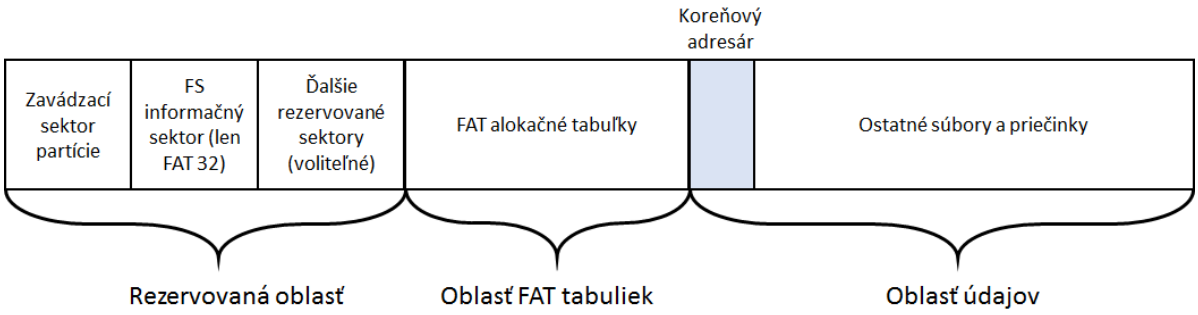
FAT (z angličtiny: “File Allocation Table”) patrí k najjednoduchším súborovým systémom, ktorý bežne podporujú operačné systémy. Historicky bol primárnym súborovým systémom v rámci MS DOS a starších verziách OS Windows (verzie 9x), neskôr bol nahradený súborovým systémom NTFS. V dnešnej dobe sa používa primárne na USB kľúčoch a pamäťových kartách, čiastočne aj pre virtuálne disky (v špeciálnych prípadoch). Je však otázkou času, kedy pôjde výrazne do úzadia aj na týchto zariadeniach vzhľadom na ich neustále rastúcu kapacitu.

Princíp

Zhluk blokov sa nazýva aj v tomto súborovom systéme cluster. FAT v súčasnosti existuje v troch základných verziách:

1. FAT12
2. FAT16
3. FAT32

Primárne sa odlišujú počtom bitov, ktoré je možné použiť na adresáciu clusterov. FAT32 zaviedlo drobné zmeny, ale vo všeobecnosti je možné vyjadriť základnú štruktúru podľa obrázku 14.21.



Obr. 14.21: Štruktúra súborového systému FAT [28].

FS (z angličtiny: "File system") informačný sektor, ktorý je typický prvok pre FAT32, treba brať s rezervou. Jedná sa o nepovinnú časť a aj keď je použitá, tak operačný systém sa ňou nemusí riadiť a ani ju aktualizovať. Z tohto dôvodu sa touto časťou nebudeme bližšie zaoberať. Dôležité je vedieť, že je ukončený sériou 0xAA550000.

Existuje špeciálna alokačná tabuľka (od nej odvodený aj názov celého súborového systému), ktorá eviduje využitie jednotlivých clusterov. Platí, že každý použitý cluster ukazuje na jednu z týchto možností:

1. Na ďalší cluster.
2. Ukončenie zreťazenia clusterov (end-of-cluster-chain): 0xfff (FAT12), 0xffff (FAT16), 0xffffffff (FAT32).

Týmto spôsobom je možné ukladať súbory, ktoré presahujú veľkosť jedného clusteru.

Významné štruktúry

Rezervovaná oblasť

Vychádzajúc z obrázku 14.21 je rezervovaná oblasť rozdelená na tri časti:

- Boot sektor partície.
- FS Informačný sektor (len pri FAT32).
- Ďalšie rezervované sektory (voliteľná časť).

Budeme sa primárne venovať sektoru pre zavedenie partície (z angličtiny: "boot sector"), ktorý je najdôležitejší pri orientácií vo FAT súborovom systéme. V tabuľke 14.5 vidíme popis jednotlivých parametrov. 3.-10. bajt obsahuje takzvané magické číslo (alebo aj masku) 0x4D 53 44 4F 53 35 2E 30 ("MSDOS5.0"), vďaka ktorému vieme určiť, že sa jedná o FAT súborový systém.

Tabuľka 14.5: Popis boot sektora pre FAT súborový systém [28].

Bajtový posun v rámci sektora pre zavedenie partície	Dĺžka v bajtoch	Rozsah v bajtoch	Obsah
0x0	3	0-2	Základná inštrukcia pre skok na zavádzač operačného systému (ak je partícia na to určená).
0x3	8	3-10	OEM (napr. 0x4D 53 44 4F 53 35 2E 30).
0xB	2	11-12	Počet bajtov na sektor: 512, 1024, 2048, 4096.
0xD	1	13-13	Počet sektorov na cluster.
0xE	2	14-15	Počet rezervovaných sektorov (rezervovaná oblasť).
0x10	1	16-16	Počet alokačných tabuliek (štandardne dve: primárna a kópia).
0x11	2	17-18	Maximálny počet záznamov v koreňovom priečinku.
0x13	2	19-20	Celkový počet sektorov vo FAT zväzku. Ak je hodnota nula, tak je číslo väčšie ako dva bajty a celková veľkosť sa nachádza na bajtoch 32-35.
0x15	1	21-21	Typ média, deskriptor (0xF8 – pevný disk, 0xF0 – odobrateľný).
0x16	2	22-23	Počet sektorov obsadených FAT súborovým systémom. Ak sa tu nachádza 0, tak to reprezentuje FAT32.
0x18	2	24-25	Počet blokov na stopu.
0x1A	2	26-27	Počet hláv.
0x1C	4	28-31	Počet sektorov pred začiatkom partície.
0x20	4	32-35	Celkový počet sektorov použitých vo FAT zväzku.
0x24	476	36-511	V tejto časti sa odlišuje FAT12/16 a FAT32.

Oblasť FAT tabuliek

O správnu prácu s obsahom súborov: jeho nájdenie a spájanie clusterov do celku sa stará FAT tabuľka. Obsahuje všetky clustere súborového systému, ktoré nadobúdajú jednu z týchto hodnôt:

- Adresa nasledujúceho clusteru, ktorý je použitý pre uloženie obsahu daného súboru.
- 0 (0x0000 pre FAT16) – nepoužitý alebo prázdny cluster.
- -9 (0xFFF7) – chybný cluster
- -1 (0xFFFF) – posledný cluster v zreťazení daného súboru.

Adresy clusterov sa začínajú číslovať od 2. Prevody medzi sektorovým a clusterovým adresovaním sú pomerne jednoduché:

- Z clusterovej adresy na sektorovú adresu:

$$(\mathrm{C}-2) \times \mathrm{počet\_sektorov\_v\_clusteri} + \mathrm{sektorová\_adresa\_clusteru\_2}$$

- Zo sektorovej adresy na clusterovú adresu:

$$\frac{\mathrm{S} - \mathrm{sektorová\_adresa\_clusteru\_2}}{\mathrm{počet\_sektorov\_clusteri}} + 2$$

Ako lokalizovať miesto, kde sa nachádza údajová časť FAT súborového systému?

Majme napríklad FAT systém, o ktorom sme zistili, že:

- začína na sektore 32,
- počet rezervovaných sektorov je 8,
- počet FAT tabuliek je 2,
- počet sektorov pre jednu FAT tabuľku je 248.

Z tohto vyplýva, že údajová časť musí začínať:

- $32 + 8 + 2 \times 248 = 536$ sektor

V prípade FAT12 a FAT16 je potrebné ešte pripočítať veľkosť koreňového adresára (512 záznamov * 32 B na záznam = 32 sektorov, pri veľkosti sektora 512 B). Ak chceme získať posun v bajtoch od začiatku partície, tak musíme výsledné číslo ešte vynásobiť veľkosťou sektora (napríklad: 512 B).

Ako lokalizovať presné miesto clusteru vo FAT tabuľke?

Nehovoríme tu o obsahu samotného clusteru a kde sa nachádza v údajovej časti FAT systému, ale len o jeho mieste vo FAT tabuľke. Platí, že cluster sa snažíme nájsť v prvej FAT tabuľke (v opačnom prípade je ešte potrebné posunúť sa na konkrétnu nasledujúcu tabuľku).

Vieme, že FAT tabuľka začína za začiatkom FAT súborového systému a po jeho rezervovanej časti. Majme:

- Začiatok FAT systému na 32 sektore.
- Veľkosť rezervovanej oblasti 8 sektorov.
- Chceme zistiť presné miesto (resp. jeho offset) pre cluster 0x08D3 vo FAT tabuľke. Cluster 0x08D3 ukazuje na cluster 0x08D4 (little endian reprezentácia je D408), viď. obrázok 14.22.

Pre získanie presného posunu potrebujeme zistiť posun (offset) FAT tabuľky, pri veľkosti sektora 512B:

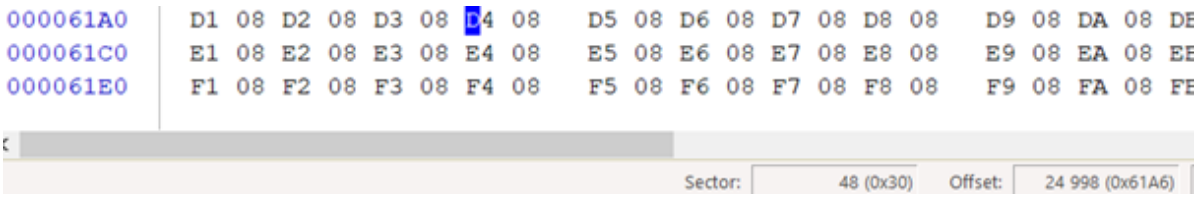
$$(32 + 8) \times 512 = 20480 = 0x5000$$

Teraz vieme, kde presne začína FAT tabuľka a už nám stačí len vynásobiť cluster počtom bajtov, ktorými je reprezentovaný. Napríklad, pre FAT16 sú to 2 bajty na jeden cluster. Posun hľadaného cluster 0x8D4 je:

$$\text{Posun\_FAT\_tabulky} + \text{Cluster} \times \text{Pocet\_bytov\_na\_cluster}$$

$$0x5000 + 2 \times 0x08D4 = 0x61A6$$

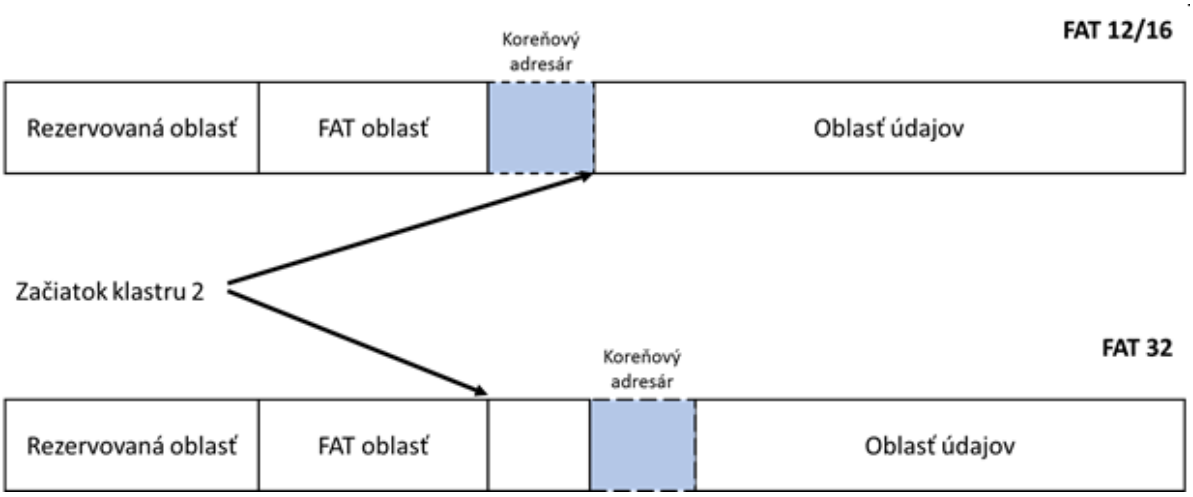
Výsledok si môžeme overiť aj v spodnej časti obrázu 14.22.



Obr. 14.22: Ukážka FAT tabuľky.

Koreňový adresár a záznamy v adresároch

Adresáre v súborových systémoch vytvárajú stromové štruktúry pre správne zaradenie je vždy potrebné vedieť miesto, kde sa nachádza koreňový priečinok (z angličtiny: "root directory"). Ako môžeme vidieť na obrázku 14.23, záleží od konkrétnej verzie FAT, kde sa nachádza koreňový adresár. Kým pre FAT12 a FAT16 je to hneď za samotnými FAT tabuľkami, pri FAT32 môže byť umiestnený kdekoľvek (adresa jeho clusteru je uvedená v tzv. "boot" sektore). Výhoda zmeny lokality tkvie v tom, že sa zmenšilo obmedzenie na počet záznamov, ktoré môže obsahovať koreňový adresár.



Obr. 14.23: Umiestnenie koreňového adresára pre FAT12/16 a FAT32 [3].

Dĺžka jedného záznamu v adresári má 32 bajtov a má štruktúru znázornenú v tabuľke 14.6. Z príkladu na obrázku 14.24 vyberieme niektoré význačné časti:

- Jedná sa o alokovaný záznam (nultý bajt je rôzny od 0x00 a 0xE5) a spolu s ďalšími desiatimi bajtmi vytvára názov „Pokus“. Tento názov nezaberá celých 11 bajtov, preto sú za ním doplnené 0x20, pre ukončenie reťazca.
- Nasleduje bajt 0x10, vďaka ktorému vieme, že sa jedná o podadresár.
- Bajty 14 – 15 hovoria o čase vytvorenia. Jedná sa o reprezentáciu pomocou little endian, teda reťazec D155 reprezentuje hodnotu je 0x55D1. Tieto dva bajty sa rozdelia na bity podľa tejto schémy (typickej pre FAT, 01010-101110-10001):
  - 5 bitov pre hodiny – $01010_2 = 10$ hodín.
  - 6 bitov pre minúty – $101110_2 = 46$ minút.
  - 5 bitov pre sekundy – $10001_2 = 17$. V tomto prípade sa nejedná o 17 sekúnd. Ako vidíme, k dispozícií pre sekundy máme len 5 bitov. Najväčšie číslo, ktoré vieme v tomto rozsahu vyjadriť je 31, čo je výrazne menej ako 59 sekúnd. Aby sme dokázali ukladať sekundy, čo najbližšie k reálnemu stavu, tak muselo prísť ku kompromisom. FAT vie ukladať len párny počet sekúnd. Binárnu hodnotu (v tomto prípade 10001_2) je potrebné vynásobiť dvojkou a tak získame výsledný počet sekúnd, v tomto prípade 34.
  - Výsledný čas vytvorenia je: 10 hodín, 46 minút a 34 sekúnd.
- Bajty 16 – 17 reprezentujú dátum vytvorenia. Opäť je potrebné previezť hodnotu 634E z little endian na šestnástkové číslo 0x4E63. Schéma pre dátum je takáto (100111-0011-00011):
  - 7 bitov pre roky – $1000111_2 = 39$ rokov. Z dôvodu malého bitového rozsahu pre roky prišlo aj tu k návrhu na optimalizáciu. Stanovil sa počiatočný rok 1980, ku ktorému sa pripočíta hodnota z tejto časti. V tomto prípade $1980 + 39 = 2019$.

  - 4 bity pre mesiace – $0011_2 = 3$. mesiac (marec).
  - 5 bitov pre dni – $00011_2 = 3$. deň.
  - Výsledný dátum vytvorenia je 3. marca 2019.

- Bajty 20 – 21 a 26 – 27 reprezentujú adresu prvého clustera pre daný súbor. Prvá dvojica reprezentuje hornú časť adresy (0000) a druhá dvojica spodnú časť adresy (4014), obe sú reprezentované pomocou little endian. V tomto prípade sa jedna o adresu clusteru 0x00001440. Prevod z adresy clusteru na sektorovú adresu je tento:

```
(Cluster - 2) x pocet_sektorov_v_clusteri +
   sektorova_adresa_clusteru_2
```

$$(\text{Cluster} - 2) \times \text{pocet\_sektorov\_v\_clusteri} + \text{sektorova\_adresa\_clusteru\_2}$$

  - Sektorovú adresu clusteru 2 získame posunom od začiatku FAT oblasti. Je potrebné preskočiť rezervovanú časť, časť určenú pre FAT tabuľky a v prípade FAT12 a FAT16 aj časť, ktorú zaberá koreňový adresár:

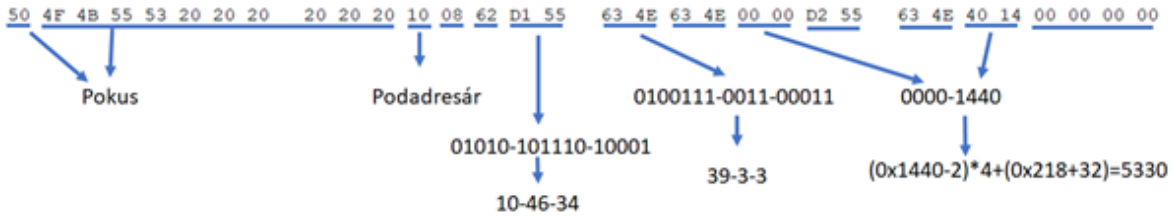
```
Zaciatok_FAT + Rezervovane_sektory +
Pocet_FAT_Tabuliek x Pocet_sektorov_pre_FAT_tabulky +
Velkost_korenoveho_adresara_v_sektoroch
```

$$\begin{aligned}\text{Zaciatok\_FAT} &+ \text{Rezervovane\_sektory} + \\ &+ \text{Pocet\_FAT\_Tabuliek} \times \text{Pocet\_sektorov\_pre\_FAT\_tabulky} + \\ &+ \text{Velkost\_korenoveho\_adresara\_v\_sektoroch}\end{aligned}$$

  - V tomto prípade, ak vieme, že máme 4 sektory v jednom clusteri:

$$(0x1440 - 2) \times 4 + (0x218 + 0x20) = 0x5330$$

- Na konci (posledné štyri bajty) je veľkosť súboru. V prípade priečinkov je vyplnená hodnota 0.



Obr. 14.24: Príklad záznamu v adresári.

Každý adresár musí obsahovať dva záznamy pre priečinky:

- "." – adresár, v ktorom sa nachádzame.
- ".." – rodičovský adresár.

Vďaka tomu vieme vždy v každom priečinku získať adresu tohto priečinka a vieme sa rekurzívnym spôsobom dostať do koreňového adresára. Umožňujte to efektívnejšiu prácu s adresárovou štruktúrou.

Tabuľka 14.6: Štruktúra záznamu pre súbor/podadresár v adresári [3].

Bajtový posun v rámci záznamu adresára (hex)	Dĺžka v bajtoch	Rozsah v bajtoch	Obsah
0x0	1	0-0	Prvý znak mena súboru v ASCII a alokačný stav (0xE5 alebo 0x00 pre nealokovaný stav, 0x2E pre adresár)
0x1	10	1-10	2. až 11. znak mena súboru v ASCII
0xB	1	11-11	Atribúty súboru (0x01 pre režim iba na čítanie, 0x02 pre skrytý súbor, 0x04 pre systémový súbor, 0x08 pre záznam obsahujúci názov zväzku na disku, 0x10 pre záznam popisujúci podadresár, 0x20 pre archív, 0x40 a 0x80 pre nepoužité)
0xC	1	12-12	Rezervované
0xD	1	13-13	Čas vytvorenia (desatiny sekúnd)
0xE	2	14-15	Čas vytvorenia (hodiny, minúty a sekundy)
0x10	2	16-17	Dátum vytvorenia
0x12	2	18-19	Dátum prístupu
0x14	2	20-21	Dva vrchné bajty z adresy prvého clusteru (0 pre FAT12 a FAT16)
0x16	2	22-23	Čas zápisu (hodiny, minúty a sekundy)
0x18	2	24-25	Dátum zápisu
0x1A	2	26-27	Spodné dva bajty z adresy prvého clustera
0x1C	4	28-31	Veľkosť súboru (0 pre adresáre)

Dlhé názvy súborov (štruktúra Long File Name)

Postupom času sa ukázalo, že formát pre názov súboru: 8 znakov pre meno a 3 pre príponu (tzv. schéma "8.3") je nedostatočný. Rovnako obmedzenie na ASCII znaky má svoje obmedzenia pri jazykových mutáciách, ktoré využívajú špeciálne znaky. Tento výrazný nedostatok FAT rieši špeciálna štruktúra Long File Name (LFN). Nachádza sa medzi záznamami o súboroch v adresári, hneď nad klasickou 8.3 schémou (Tabuľka 14.7).

Tabuľka 14.7: Spôsob ukladania rôznych schém pre názvy súborov.

2	LFN2
1	LFN1
0	Schéma 8.3

LFN zavádza podporu tzv. "Unicode" kódovania znakov a dĺžku názvu zväčšuje na 255 znakov. Štruktúra je daná podľa tabuľky 14.8. Každý LFN záznam má dĺžku 32 bajtov a pre podporu dlhých názvov je potrebné zreťaziť viacero týchto štruktúr. Toto rieši prvý bajt, ktorý určuje poradové číslo záznamu. Poradové číslo je zároveň na binárnej úrovni v logickom súčte:

- s číslom 0x40, v prípade, že sa jedná o posledný záznam,
- s číslom 0xE5, ak je záznam nealokovaný (napríklad pri zmazanom súbore).

Ako vidíme, tak jeden LFN záznam podporuje celkovo 13 znakov (26 bajtov) uložených pomocou Unicode kódovania.

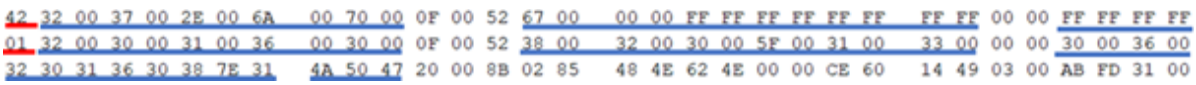
Tabuľka 14.8: Štruktúra LFN [28].

Posun v bajtoch (v rámci LFN záznamu) v šestnásťkovej sústave	Dĺžka v desiatkovej sústave (v bajtoch)	Rozsah v desiatkovej sústave (v bajtoch)	Obsah
0x0	1	0-0	Poradové číslo, začína sa s 1 a rastie pre každý LFN záznam až po posledný záznam, nad ktorým je použitý logický súčet (OR) s hodnotou 0x40. Nepridelené súbory majú prvý záznam v logickom súčte s hodnotou 0xE5
0x1		10 1-10	5 znakov mena súboru (kódovanie Unicode)
0xB	1	11-11	Atribúty typu súboru (0x0F – priečinok)
0xC	1	12-12	Rezervované
0xD	1	13-13	Kontrolná suma
0xE	12	14-25	6 znakov mena súboru (kódovanie Unicode)
0x1A	2	26-27	Rezervované
0x1C	4	28-31	2 znakov mena súboru (kódovanie Unicode)

Z dôvodu podpory Unicode sa v niektorých nástrojoch, ktoré majú ASCII zobrazovanie znakov zobrazuje kombinácia znak + bodka (napr. „2.0.1.6.“ pre „2016“).

Na príklade uvedenom na obrázku 14.25 vidíme príklad pre dlhý názov súboru. V poslednom riadku v každej trojici sa nachádza štruktúra 8.3 a názov súboru je 201608~1.jpg. Vidíme, že pre celý názov súboru potrebujeme dva LFN záznamy. Prvý záznam má svoj prvý bajt “0x01”, druhý záznam (najvyšší) má poradové číslo 0x02, keďže sa jedná zároveň o posledný zázname, tak je v logickom súčte s číslom 0x40, preto je uvedená hodnota 0x42.

Postupne z prvého záznamu prečítame znaky „2.0.1.6.0.8.2.0._.1.3.0.6.“ a z druhého „2.7...j.p.g.“, teda celý názov súboru bol 20160820_130627.jpg.



Obr. 14.25: Príklad štruktúry LFN.

Vytváranie a vymazanie súborov

Vytváranie súborov vo FAT súborovom systéme je pomerne jednoduché a skladá sa z týchto krokov:

1. Skontroluje sa veľkosť voľného miesta a jedinečnosť mena súboru.
2. Alokuje sa príslušný počet clusterov, ktorý je daný vzťahom:

$$\text{počet\_clusterov} = \left\lceil \frac{\text{veľkosť súboru}}{\text{veľkosť clusteru}} \right\rceil$$

   Vyberajú sa len nealokované clustre (označené 0 – napr. 0x0000 v prípade FAT16) a vyhýba sa chybným clusterom (napr. 0xFFF7 pre FAT16) v alokačnej tabuľke.
3. Vytvorí sa nový záznam v tabuľke adresára, ktorý tvorí názov súboru, jeho veľkosť a označenie prvého clusteru v zreťazení.
4. Vytvorí sa zreťazenie alokovaných clusterov v alokačnej tabuľke. Každý cluster ukazuje na nasledujúci s výnimkou posledného, ktorý obsahuje 0xFFFF (pre FAT16).

Vymazanie súborov je rýchly proces:

1. V názve súboru sa prvý znak nahradí znakom 0xE5 („σ“, niektoré nástroje zobrazujú aj vo forme „_“).
2. Vymaže sa zreťazenie clusterov vo FAT tabuľke.

Proces mazania súboru je veľmi rýchly, vďaka jeho jednoduchosti. Reálne nedochádza k zmazaniu obsahu súboru. Ak súbor nebol na zväzku fragmentovaný, tak jeho obnova je pomerne triviálna:

1. Znak 0xE5 nahradíme prvým znakom zo štruktúry pre dlhé meno súboru. Týmto vieme obnoviť pôvodný názov súboru. Ak táto štruktúra nebola použitá, môžeme použiť ľubovoľný bežný ASCII znak pre názov súboru (najčastejšie: a-z, A-Z, 0-9) tak, aby nevznikla duplicita s iným názvom súboru.
2. Zistíme veľkosť súboru v clusteroch. Veľkosť súboru vyčítame zo záznamu v tabuľke adresára pre obnovovaný súbor. Použijeme rovnaký vzorec ako pri vytváraní súboru.
3. Prvý cluster zo zreťazenia nájdeme v tabuľke adresára, v zázname obnovovaného súboru. Do FAT tabuľky doplníme do neho číslo ďalšieho clusteru. Takto postupne obnovíme celé zreťazenie a do posledného clusteru zapíšeme 0xFFFF (pre FAT16).

Pri tomto type obnovy musí byť splnených viacero podmienok:

- Súbor nebol fragmentovaný (rozptýlený) vo zväzku.
  - Nevedeli by sme povedať s istotou, ktorý cluster nasleduje ako ďalší v zreťazení.

- Záznam zmazaného súboru nebol prepísaný.
  - Nevedeli by sme povedať, že sa tam súbor reálne nachádzal. Nevedeli by sme jeho pôvodnú veľkosť, začiatok zreťazenia clusterov ani, časť jeho názvu.
- Všetky pôvodne použité clustre zostali neobsadené.
  - Pôvodný obsah súboru bol zmazaný. Pri opatrnom postupe sa nám môže podariť obnoviť aspoň časť súboru.
  - Pri dlhšom používaní súborového systému môže dôjsť k prepísaniu obsahu časti clusterov novým súborom. Ak tento súbor zmažeme, tak nemusíme vedieť rozlíšiť, či sa jedná o obsah pôvodne zmazaného súboru alebo novo zmazaného súbory. Pre určité typy súborov vieme použiť nástroje, ktorými vieme zistiť, či nenastal takýto prípad (napríklad kontrola stavu clusterov vo FAT tabuľke).

Ako vyplýva z uvedených podmienok, tak najlepšie výsledky pri obnove súborov môžeme dosiahnuť na nefragmentovanom zväzku a čo najbližšie (z hľadiska počtu vykonaných operácií nad zväzkom) k bodu zmazania súborov.

14.6.3 NTFS

V čase prestávala stačiť pomerne jednoduchá štruktúra FAT súborových systémov, zároveň vznikali nové požiadavky. Medzi nimi boli bezpečnosť (rôzni používatelia a ich prístupové práva), ale aj stabilita súborového systému ako takého. V tomto kontexte bol predstavený spoločnosťou Microsoft nový súborový systém NTFS (z angličtiny: “New Technology File System”).

V porovnaní s FAT zavádza tieto hlavné novinky [28]:

- Komplexné štruktúry súborového systému.
- Pomenovania súborov do dĺžky 255 znakov.
- Šifrovanie.
- Bezpečnosť a prístupové zoznamy.
- Žurnálovanie.

MFT záznamy

Dochádza k veľkému filozofickému posunu a každá časť NTFS je považovaná za súbor. Pri FAT súborovom systéme boli napríklad úvodné hlavičky alebo samotné FAT tabuľky vo forme vyhradených sektorov v rámci súborového systému. Toto pri NTFS zaniká všetky jeho štruktúry sú zároveň súbormi. Záznamy o všetkých súboroch sa nachádzajú v tzv. „$MFT súbore“ (známe aj ako „MFT záznamy o súboroch“). Medzi niektoré zo základných NTFS súborov patria tie uvedené v tabuľke 14.9.

Každý MFT záznam je dlhý 1024 bajtov a začína konštantou “FILE” alebo “BAAD” v závislosti od toho, či sa jedná o korektný súbor alebo zlý záznam. MFT záznamy môžu tvoriť až okolo 12,5 % miesta na zväzku.

Tabuľka 14.9: NTFS – základné súbory.

Záznam v $MFT súbore	Meno súboru	Popis
0	$MFT	Záznamy všetkých súborov v súborovom systéme, vrátane seba samého.
1	$MFTMirr	Obsahuje obvykle kópiu prvých štyroch záznamov $MFT.
2	$LogFile	Obsahuje záznamy o zmene metadát súborového systému.
3	$Volume	Obsahuje informácie o zväzku (názov, ID, verziu a i.).
4	$AttrDef	Zoznam mien, čísel a opisov atribútov.
5		Koreňový adresár súborového systému.
6	$Bitmap	Reprezentuje obsadenosť jednotlivých clusterov v súborovom systéme (0 – voľný, 1 – obsadený).
7	$Boot	Zavádzací sektor a zavádzací kód súborového systému. Obvykle sa nachádza na začiatku súborového systému.
8	$BadClus	Clustre, ktoré obsahujú chybné sektory.
9	$Secure	Bezpečnosť a kontrola prístupov k súborom alebo skupinám súborov. Šetrí sa réžia oproti stavu, kedy by boli tieto údaje pri jednotlivých súboroch samostatne.
10	$UpCase	Tabuľka veľkých písmen vo formáte Unicode. Zabezpečuje necitlivosť súborového systému na veľké a malé písmena v názvoch súborov.
11	$Extend	Obsahuje rôzne rozšírenia súborového systému.
12-23	.....	Rezervované pre $MFT rozšírenia záznamov.

V rámci MFT záznamov sa nachádza viacero vnorených štruktúr (ktoré definujú rôzne vlastnosti súboru), zostávajúci priestor môže byť použitý pre uloženie obsahu samotného súboru. Musí sa však jednať o súbor s pomerne malou dĺžkou (maximálne 700 bajtov). V opačnom prípade sa nachádza v iných častiach zväzku a ich miesto je určené parametrom "Data run" v atribúte $DATA. Ku každému súboru môže existovať viacero parametrov "Data run", ktoré vlastne definujú clustre (ich za sebou idúce počty), v ktorých je uložený samotný obsah súboru. V porovnaní s FAT tabuľkou nám stačí vedieť pre každý "Data run" počiatočný cluster a celkový počet clusterov v tomto intervale, čím sa minimalizuje réžia.

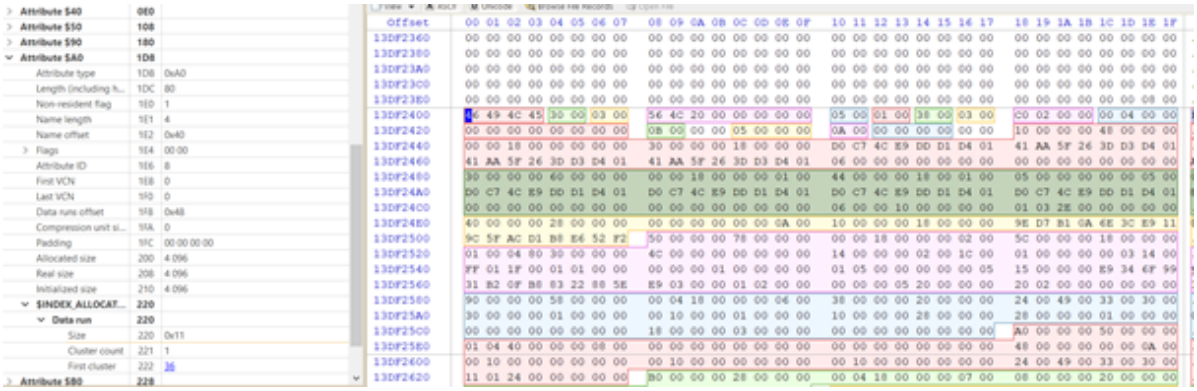
MFT atribúty

MFT atribúty ukladajú ďalšie metadáta o konkrétnom súbore. V tabuľke 14.10 uvádzame základné atribúty a ich význam. Úplný zoznam atribútov je možné nájsť na [35].

Každý z týchto atribútov je tvorený štruktúrou rôznych parametrov (napr. vyššie spomenutý "Data run" pre $INDEX_ALLOCATION, či $DATA), ktorým sa kvôli rozsahu tejto knihy nebudeme venovať. Viac informácií k nim je možné nájsť napríklad v [1]. Ukážku analýzy súboru si môžete pozrieť na obrázku 14.26.

Tabuľka 14.10: MFT atribúty.

Identifikátor	Meno atribútu	Popis
16 ($10)	$STANDARD_INFORMATION	Všeobecné informácie, MAC časy, ID vlastníka, príznaky súboru a iné.
48 ($30)	$FILE_NAME	MAC časy, meno súboru, odkaz na rodičovský adresár.
128 ($80)	$DATA	Nachádza sa v ňom obsah súboru. Podľa veľkosti súboru záleží, či je to priamo v MFT zázname alebo v inej časti zväzku.
144 ($90)	$INDEX_ROOT	Používaný pre adresáre. Obsahuje informácie o podadresároch a súboroch, ktoré sa v ňom nachádzajú.
160 (A0)	$INDEX_ALLOCATION	Používaný ak je počet súborov a podpriečinkov v adresári priveľký a nevojde do MFT záznamu.

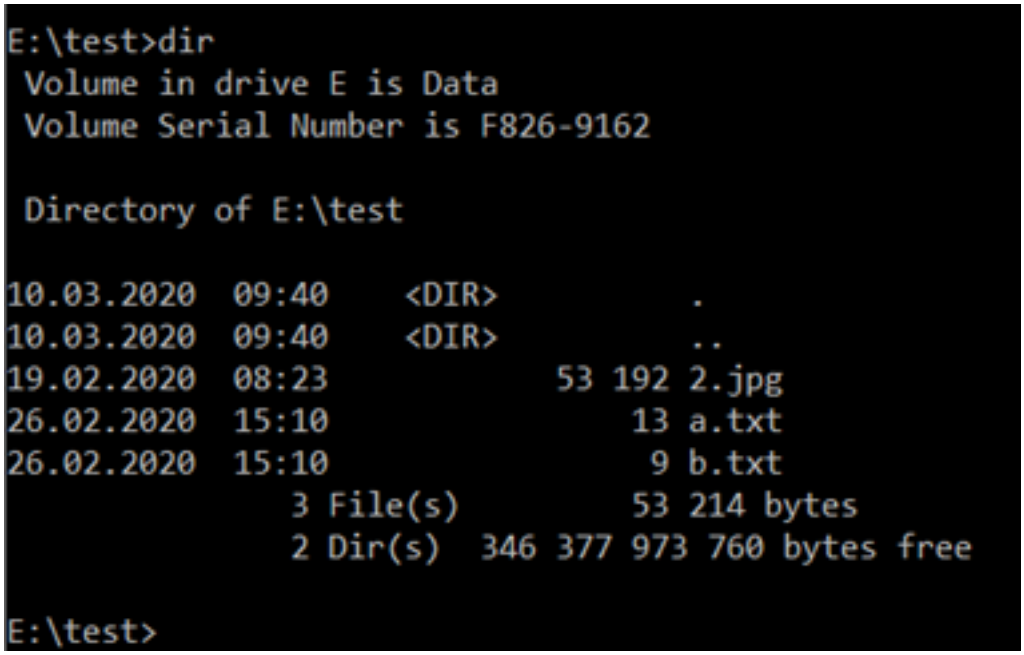


Obr. 14.26: Ukážka analýzy súboru v NTFS.

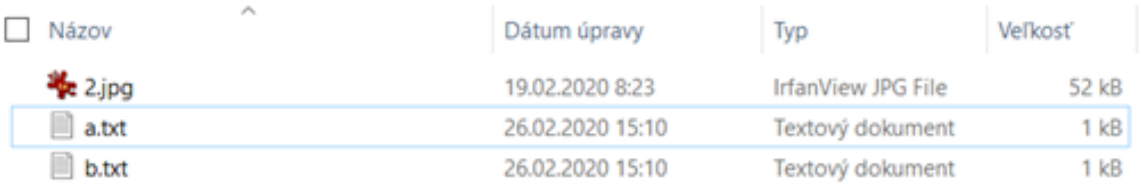
Alternatívne toky údajov

Zaujímavou novou funkciou v NTFS, z pohľadu forenznej analýzy, je pridanie alternatívnych tokov údajov (z angličtiny: “Alternate Data Streams”). Umožňuje pridávať rôzne prídavne toky údajov k existujúcemu súboru, dokonca až celé súbory. Po verziu Windows Vista bolo možné vykonávať spustiteľné aplikácie, ktoré boli celé týmto spôsobom pridané k iným súborom. Táto funkcionalita bola často zneužívaná rôznym malvérom, ktorý sa takto dokázal skrývať. V prípade, že sa pridal k súborom v chránených adresároch (napr. System32), tak pre antivírové riešenia bolo nemožné odložiť súbor do karantény.

Veľkou výhodou z pohľadu útočníka je, že použitie tejto funkcionality sa nedá odhaliť použitím štandardných metód, napríklad zobrazenie v priečinku použitím príkazu *dir* bez prepínačov (Obrázok 14.27) alebo v štandardnom náhľade s použitím Prieskumníka (Obrázok 14.28). V oboch prípadoch vidíme, že súbory pôsobia štandardne a nebudia žiadne podozrenie.



Obr. 14.27: Zobrazenie obsahu adresára v príkazovom riadku.



Obr. 14.28: Zobrazenie obsahu adresára pomocou Prieskumníka.

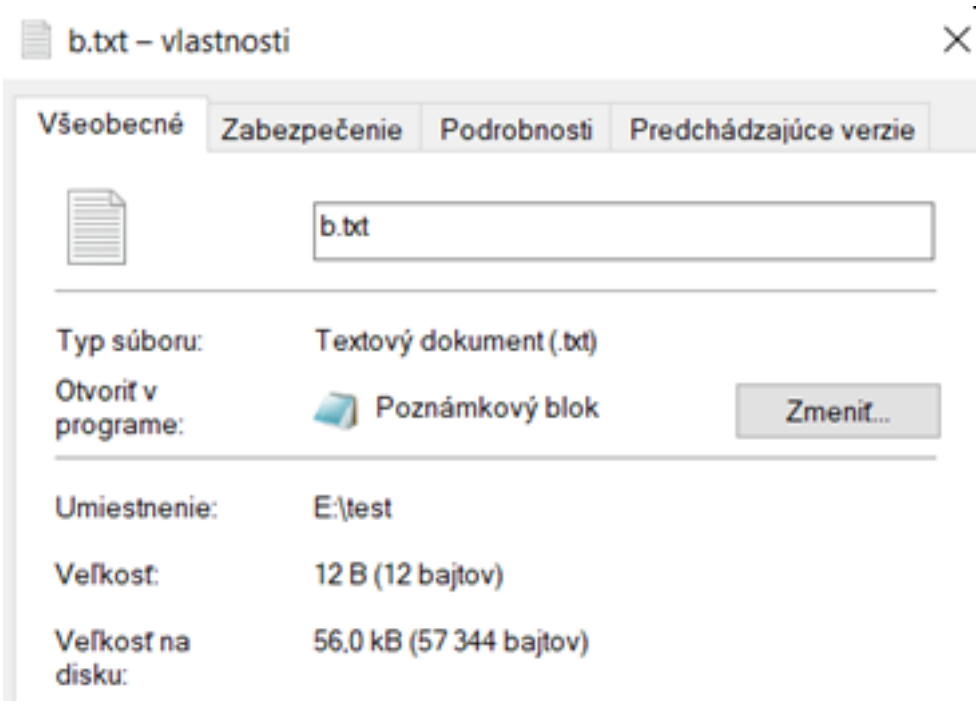
Ak si však dáme zobraziť vlastnosti niektorého zo súborov (napr. súbor „b.txt“ na obrázku 14.29), vidíme pomerne veľký nesúlad medzi jeho reálnou veľkosťou a veľkosťou na disku. Toto je len indikátorom niečoho podozrivého. Bežne sa môže stať, ak je súbor menší ako veľkosť clustera, že sa tieto veľkosti líšia (platí to aj pre väčšie súbory a fragmentovaný systém). Určite nám to vie pomôcť pri určovaní podozrivých súborov.

Ak máme podozrenie, že niektoré súbory v danom priečinku obsahujú alternatívne toky údajov, použijeme príkaz „*dir /R*“, ktorý ich dokáže zobraziť (Obrázok 14.30). Z obrázku vidíme, že súbory reálne obsahujú viac informácií ako sa mohlo na prvý pohľad zdať a identifikovali sme dokopy päť alternatívnych tokov údajov. Vidíme dokonca, že väčšina z nich je väčšia ako bola pôvodná veľkosť súborov.

Ako odhaliť tento skrytý obsah a ako bol vôbec vytvorený?

Vytvoriť alternatívny tok údajov je veľmi jednoduché, stačí v príkazovom riadku v danom adresári zavolať príkaz:

```
Echo "text" meno_suboru:nazov_alternativneho_toku_udajov
```



Obr. 14.29: Zobrazenie vlastností súboru.

Odhalenie jeho obsahu je rovnako jednoduché a môžeme použiť napríklad príkaz:

```
More < nazov_suboru:nazov_alternativneho_toku_udajov
```

Príklad takéhoto vytvorenia alternatívneho toku údajov a zobrazenie jeho obsaju môžeme vidieť na obrázku 14.31.

Vytváranie a mazanie súborov

Vytváranie súborov v NTFS súborovom systéme prebieha takto:

1. Kontrola voľného miesta na zväzku a alokovanie potrebného počtu clusterov. Ak sa jedná o malý súbor (do 700 bajtov), ktorý môže byť umiestnený v samotnom MFT zázname, nie je potrebné alokovať žiadne clustre.
2. Nájde sa voľný MFT záznam, ktorý môže byť priradený k vytváranému súboru.
3. Vyplnia sa základné údaje MFT záznamu (vrátane $STANDARD_INFORMATION, $FILE_NAME, $DATA a iné potrebné parametre).
4. Ak sa jedná o súbor do 700 bajtov, tak sa celý jeho obsah bude nachádzať v atribúte $DATA. V opačnom prípade sa tu budú nachádzať informácie o tom, kde sa nachádza obsah súboru (použitím tzv. “Data run”). V súbore $Bitmap sa vyznačia príslušné clustre ako obsadené. Po tomto kroku sa zapíše obsah vytváraného súboru.
5. Nájde sa koreňový adresár (MFT záznam číslo 5). Postupne sa prehľadá adresárová štruktúra na miesto, kde sa má súbor nachádzať. Vytvorí sa nový záznam (tzv. „INDX

```
E:\test>dir /R
 Volume in drive E is Data
 Volume Serial Number is F826-9162

 Directory of E:\test

10.03.2020  09:40    <DIR>          .
10.03.2020  09:40    <DIR>          ..
19.02.2020  08:23            53 192 2.jpg
                                186 2.jpg:Zone.Identifier:$DATA
26.02.2020  15:10                13 a.txt
                                  0 a.txt:dp:$DATA
                                 15 a.txt:tajomstvo:$DATA
26.02.2020  15:10                 9 b.txt
                                 26 b.txt:dp:$DATA
                            139 691 b.txt:drobnost:$DATA
               3 File(s)         53 214 bytes
               2 Dir(s)  346 377 973 760 bytes free

E:\test>
```

Obr. 14.30: Podrobný výpis obsahu adresára cez príkazový riadok.

```
E:\test>echo "forenzna analyza" > a.txt:ads

E:\test>more <a.txt:ads
"forenzna analyza"
```

Obr. 14.31: Vytvorenie a zobrazenie alternatívneho toku údajov.

záznam“), ktorý sa zapíše do rodičovského adresára (do $INDEX_ROOT alebo $INDEX_ALLOCATION).

6. Po vytvorení každého kroku sa vytvorí záznam v súbore $LogFile.

Pri mazaní súboru sa uplatní takmer opačné poradie:

1. Cez koreňový adresár sa nájde umiestnenie súboru. Po nájdení rodičovského záznamu sa z tohto odstráni záznam o súbore („INDX záznam“).

2. MFT záznam súboru sa nastaví ako zmazaný (použije sa zmena príznaku vo “Flags”) a stane sa prístupným pri vytváraní nových súborov.

3. Ak sa obsah súboru nachádza výhradne v rámci MFT záznamu, pokračuje sa na ďalší krok. Ak sa nachádza mimo tento záznam, tak sa z parametra $DATA zistia jednotlivé lokality clusterov (pomocou parametrov "Data run"). Tieto sa nastavia v súbore $Bitmap ako voľné a prístupné pre ďalšie zápisy.

4. Po vytvorení každého kroku sa vytvorí záznam v súbore $LogFile.

Obnovovanie súboru sa inšpiruje postupom vymazávania. Vychádzame z toho, že MFT záznam nebol prepísaný iným záznamom:

1. Prehľadávame MFT a hľadáme tie, ktoré majú nastavený príznak, že sú dostupné. V rámci týchto MFT záznamov hľadáme ten, ktorý ma požadovaný názov (ak obnovujeme všetky zmazané súbory, toto porovnanie vynechávame).

2. Nastavíme príznak o používaní MFT záznamu na obsadený (napr. ako alokovaný súbor).

   a) Ak bol súbor menší ako 700 bajtov pokračujeme na ďalší krok.

   b) Ak bol súbor väčší ako 700 bajtov, pozrieme sa do atribútu $DATA a v časti "Data run" nájdeme adresy potrebných clusterov. Tie porovnáme so stavom v súbore $Bitmap. Ak sú všetky označené ako voľné, môžeme ich opätovne alokovať (označiť ako obsadené). Ak však niektoré z nich nie sú voľné, tak medzitým došlo k prepísaniu týchto clusterov iným súborom a nie je možné obnoviť celý obsah zmazaného súboru.

3. V MFT zázname nájdeme rodičovský adresár (číslo jeho MFT záznamu).

   a) Ak rodičovský adresár nebol zmazaný, môžeme v ňom obnoviť alebo opätovne vytvoriť záznam o súbore.

   b) Ak rodičovský adresár bol zmazaný, môžeme obnovovaný súbor vytvoriť inde v rámci existujúcej stromovej štruktúry adresárov.

V prípade, že chceme zmazané súbory obnoviť na iné miesto, napríklad v situácii, keď kontrolujeme zväzok a nájdené zmazané súbory chceme obnoviť napríklad na USB kľúč, môžeme niektoré kroky modifikovať:

1. Nájdeme MFT záznamy zmazaných súborov a skontrolujeme, či všetky ich clustre stále neboli prepísané.

2. Vytvoríme nový MFT záznam na novom médiu (USB kľúč) podľa pravidiel pre vytváranie súborov.

3. Skopírujeme parametre zmazaných súborov z MFT záznamu (napr. časové pečiatky, veľkosť, atribúty) do nového MFT záznamu alebo ich uložíme do samostatného súboru.

4. Z pôvodných "Data run" alebo priamo z $DATA skopírujeme obsah súboru do novej štruktúry.

14.6.4 EXT

Rozšírený súborový systém (z angličtiny: "Extended File System") – EXT patrí medzi najviac používané súborové systémy pre operačný systém Linux. Pôvodne bol založený na Unix súborovom systéme (z angličtiny: "Unix File System" – UFS). V súčasnosti existujú tri používané verzie:

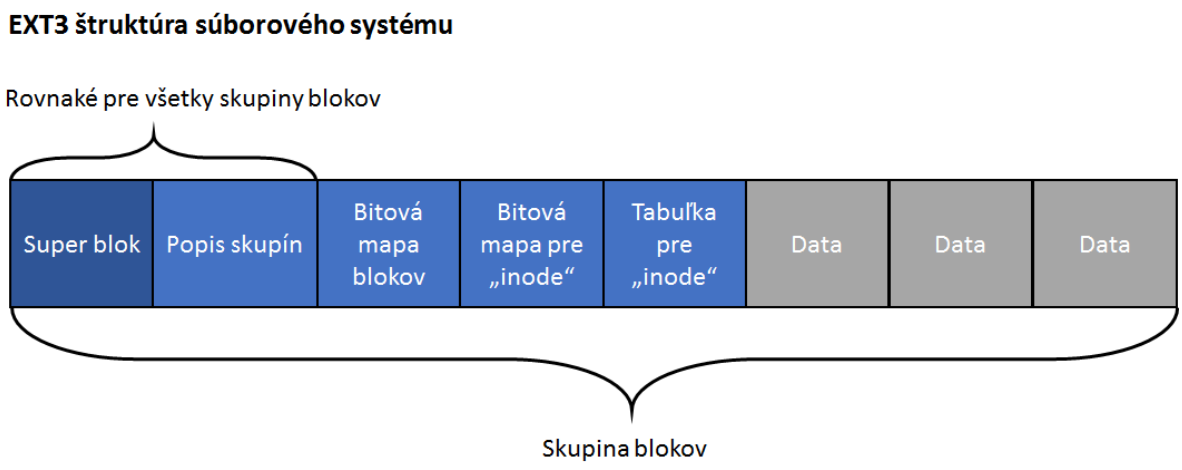
EXT2 – aj v súčasnosti bežný pre partície, ktorých obsah sa moc často nemení.

EXT3 a EXT4 – obe verzie používajú už žurnálovací systém a sú výrazne viac používané ako EXT2.

S EXT4 súborovým systémom sa zaviedli viaceré významné zlepšenia v porovnaní s predchádzajúcimi generáciami a to najmä:

- Presnosť MAC časov na úrovni nanosekúnd.
- Podpora času vytvorenia.
- Predĺžil sa maximálny možný dátum do 25. 4. 2514.
- Vytváranie veľkých Inode štruktúr (viac nižšie).
- Vyšší počet podadresárov a súborov v priečinku.

Pre označenie najmenšej adresovateľnej jednotky (cluster) sa používa pojem blok a platí tu známe pravidlo, že OS Linux považuje všetko za súbor (súbor, priečinok, soket, ...). V ďalších častiach si postupne prejdeme význačné štruktúry (Obrázok 14.32).



Obr. 14.32: EXT štruktúra [3].

Superblok (Superblock)

Začína sa na 1024. bajte od začiatku a je dlhý presne 1024 bajtov. Začína sa magickým číslom (konštantou) 0xEF53. Jedná sa o kľúčový prvok, ktorý popisuje parametre súborového systému, veľkosti a správanie jednotlivých štruktúr (Tabuľka 14.11). Pre zvýšenie spoľahlivosti sa obvykle nachádza na začiatku každej skupiny blokov (z angličtiny: "Block group").

Tabuľka 14.11: Výbrané parametre Superbloku.

Meno	Popis
Block size	Veľkosť bloku
Inode count	Celkový počet inode-ov
Block count	Celkový počet blokov
Filesystem Features	Špeciálne vlastnosti súborového systému
Free blocks	Počet voľných blokov
Free inodes	Počet voľných inode-ov
Inodes per group	Počet inode-ov na jednu skupinu
Blocks per group	Počet blokov na jednu skupinu
Volume name	Meno zväzku
Last write time	Posledný čas zápisu
Last mount time	Čas posledného pripojenia súborového systému
Last moun on	Miesto posledného pripojenia súborového systému
Mount count	Počet pripojení súborového systému

Vidíme, že už z tejto úvodnej štruktúry vieme získať viacero zaujímavých informácií, aj o samotnom súborovom systéme, aby sme ho vedeli správne prehľadávať. Vieme získať aj informácie zaujímavé pre vyšetrovanie. Vieme zistiť, kedy došlo k poslednej zmene v rámci súborového systému, ale aj kedy bol posledný krát pripojený, čo nám môže pomôcť potvrdením alebo vyvrátením danej hypotézy počas vyšetrovania. Príliš nízky počet pripojení súborového systému môže ukazovať na to, že v nedávnej dobe mohlo dôjsť k formátovaniu zväzku a reinštalovaniu operačného systému.

Skupina blokov (Block Group)

Skupiny blokov rozdeľujú súborový systém na niekoľko rovnakých častí. Každá skupina obsahuje:

- kópiu superbloku,
- bitové mapy obsadenosti blokov a inode-ov,
- tabuľku inode-ov,
- počet voľných inode-ov a blokov
- opis skupiny (z angličtiny: "Group descriptor"), ktorý definuje vlastnosti skupiny blokov,
- obsah samotných súborov.

Štruktúru a parametre jednotlivých skupín môže výrazne ovplyvniť použitie parametrov *flex_group* a *sparse_super* (uvedené neskôr).

Inody a Extenty

Inode reprezentuje metadáta k uloženému súboru. Pri EXT2 a EXT3 má veľkosť 128 bajtov, EXT4 v súčasnosti používa 156 bajtov, ale alokuje rovno 256 bajtov, ktoré umožňujú ďalšie rozširovanie do budúcnosti. Podobne ako v iných pokročilých súborových systémoch aj tu sa ukladajú MAC časy, typ súboru, miesto uloženia obsahu súboru na zväzku, prístupové zoznamy (ACL), prístupové práva (zápis, čítanie, vykonávanie) pre používateľa, skupinu, či ostatných.

Ak potrebujeme lokalizovať inode postupujeme týmito krokmi:

- Identifikácia skupiny: (Inode číslo -1) / (Počet inode-ov na skupinu blokov).
- Index v rámci skupiny: (Inode číslo -1) modulo (Počet inode-ov na skupinu blokov).
- Posun (z angličtiny: “offset”) v tabuľke pre inode-y: Index * (Veľkost inode-u).

Aj keď inode-y obsahujú množstvo príznakov a parametrov, tak je potrebné k nim pristupovať opatrne, keďže niektoré z nich nie sú v súčasnosti podporované operačnými systémami.

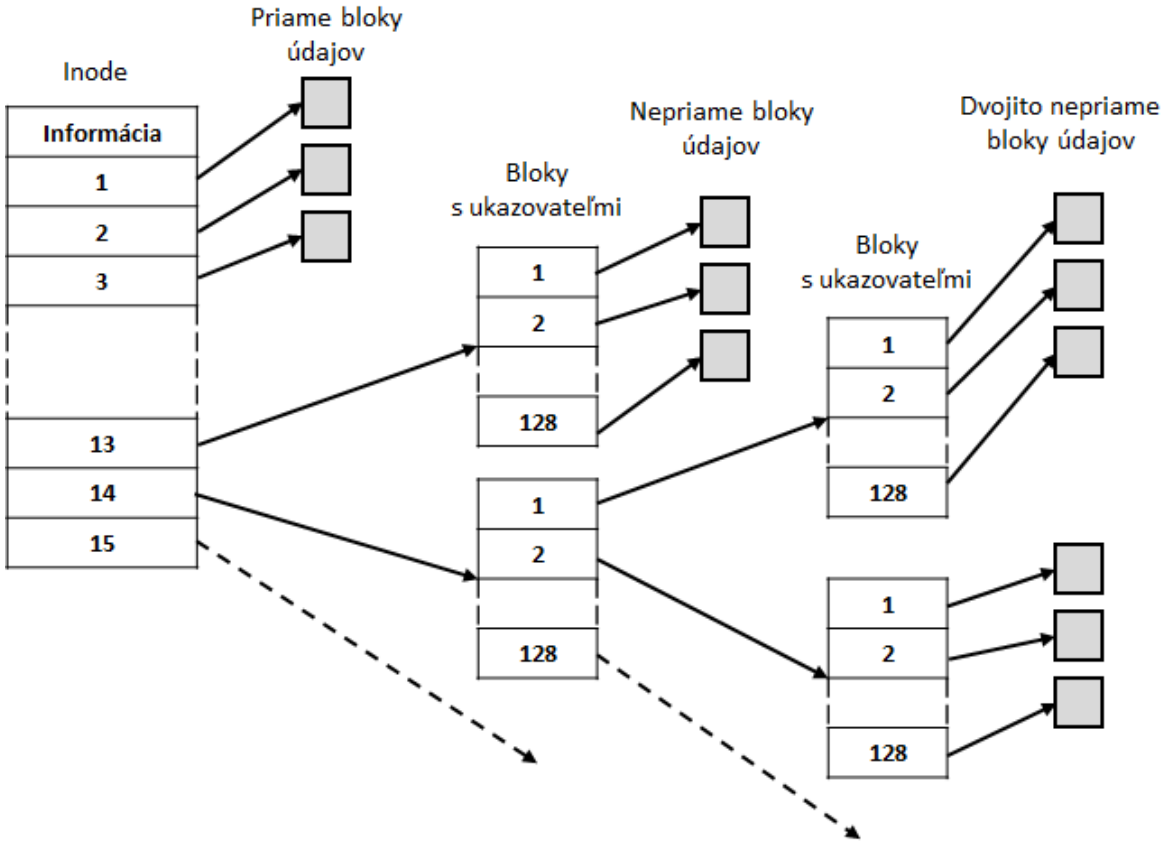
Zaujímavým je spôsob adresovania na obsah súboru. V štruktúre sa nachádza na obrázku 14.33:

- 12 priamych ukazovateľov na bloky (clustre) na obsah disku (z angličtiny: “Direct Data Blocks”).
- 1 nepriamy ukazovateľ na bloky (z angličtiny: “Indirect Data Blocks”).
- 1 dvojito nepriamy ukazovateľ na bloky (z angličtiny: “Double indirect Data Blocks”).
- 1 trojito nepriamy ukazovateľ na bloky (z angličtiny: “Triple indirect Data Blocks”).

Ak uvažujeme veľkosť bloku 8192 bajtov (8 KB) a veľkosť jedného záznamu pre blok 8 bajtov, tak maximálnu kapacitu vypočítame nasledovne:

$$Celková\_kapacita = 8192 \times (12 + 1024 + 1024 \times 1024 + 1024 \times 1024 \times 1024)$$

Vidíme, že EXT je efektívne navrhnutý na prácu s menšími súbormi. Pri väčších súboroch dochádza pravidelne k prerušovaniu medziblokom s ďalšími ukazovateľmi. Z tohto dôvodu bola v rámci EXT4 zavedená nová štruktúra, tzv. *“Extent”*, ktorá nahrádza tento spôsob adresovania. Jedná sa o stromovú štruktúru, ktorej prvé štyri záznamy môžu byť uložené na mieste pôvodnej adresnej schémy v rámci inode-u. Je možné vytvárať stromovú štruktúru až do piatej úrovne. Extenty fungujú na podobnom princípe ako “Data run” v NTFS, ukazujú na prvý blok danej časti obsahu súboru a potom rozsah za sebou idúcich blokov (teda štartovací blok + dĺžka intervalu).



Obr. 14.33: Reprezentácia inode štruktúr [19].

Adresáre

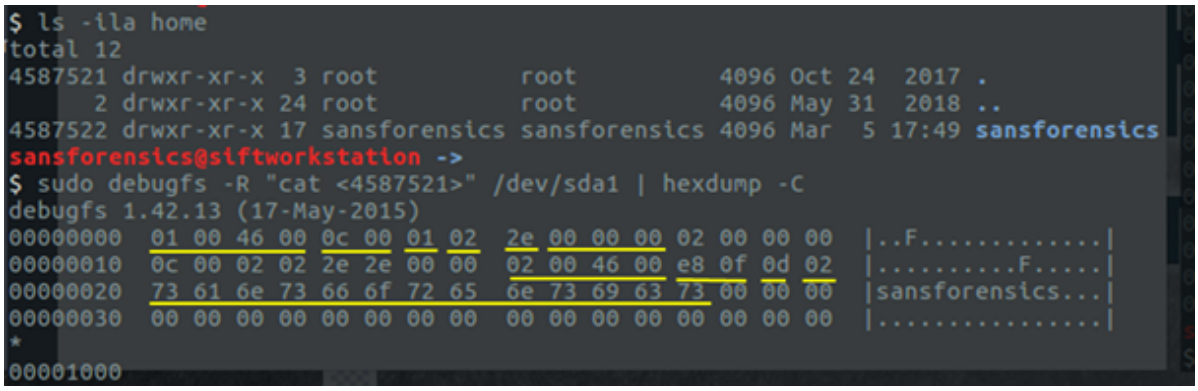
Pomáhajú spájať mená súborov s inode-ami. Ku každému adresáru sa pristupuje ako k súboru. Základná štruktúra môže byť pomocou parametra *Filetype feature* (vo *Filesystem feature*) rozšírená (Tabuľka 14.12). Je to možné vďaka tomu, že maximálna dĺžka mena súboru je 255 znakov, ale v pôvodne štruktúre sú na to vyhradené až dva bajty (teoretická maximálna dĺžka 65535 znakov). Z tohto dôvodu sa jeden bajt odčlenil na reprezentovanie typu súboru. Nejedná sa o kritickú zmenu, keďže typ súboru vieme identifikovať aj z inode-u príslušného súboru, ale zjednoduší to prehľadávanie.

Ak spojíme predchádzajúce znalosti, tak na obrázku 14.34 vidíme, že jednoduchým pridaním prepínačov k príkazu *ls* vieme získať aj inode číslo súborov v priečinku (napr. 4587522 pre "sansforensics"). Zaujímavé sú jednotlivé zápisy v tomto priečinku ako môžeme vidieť na nižšej časti obrázka. Treba počítať s tým, že tieto údaje sú uvedené vo formáte little endian. Vidíme inode číslo (prvé 4 bajty), nasledované dĺžkou záznamu (0x000C), dĺžkou mena (0x01), typom súboru (0x02), menom súboru (0x2E – ".") a zarovnaním zvyšku názvu na násobok štyroch bajtov. Podobne si vieme pozrieť druhý záznam. Zaujímavosťou tretieho záznamu je, že ak si všimneme jeho dĺžku, tak je pomerne veľká (0x0FE8 – 4072), vzhľadom na to, že jeho meno je pomerne krátke (0x0D – 13 znakov – "sansforensics"). Celé tajomstvo tkvie v tom, že posledný záznam v priečinku je dorovnaný do konca prideleného bloku (v tomto prípade je

Tabuľka 14.12: Základná a rozšírená štruktúra adresárov.

Meno	Dĺžka (Dĺžka v rozšírenej štruktúre) v bajtoch	Nachádza sa v základnej štruktúre?	Popis
Inode	4	Áno	Číslo Inode-u
Rec len	2	Áno	Dĺžka záznamu
Name len	2 (1)	Áno	Dĺžka mena
File type	1	Nie	Typ súboru (napr. 0x01 štandardný súbor, 0x02 adresár, 0x06 socket, 0x07 symbolický odkaz)
Name	maximálne 255	Áno	Názov súboru

blok o veľkosti 4096 bajtov).



Obr. 14.34: Zistenie inode-u k priečinku a jeho obsahu.

Rozširujúce vlastnosti súborového systému

Pomocou parametra *System Features* viem významne ovplyvňovať správanie systému. Rozširujúce vlastnosti vieme rozdeliť do troch základných kategórií:

1. **Kompatibilné vlastnosti**. Súborový systém s takýmito vlastnosťami môže byť pripojený k operačnému systému aj na čítanie aj na zápis. Vlastnosti, ktoré môžu mať vplyv na rozloženie dát:

   a) *Resize inode*: Miesto na viac pre rozšírenie v budúcnosti v *Group Desriptor Table*.

2. **Nekompatibilné vlastnosti**. Súborový systém by nemal byť pripojený ani v režime čítania, ak tieto vlastnosti nie sú podporované operačným systémom. Parametre, ktoré môžu mať vplyv na rozloženie dát:

a) *Flexible block groups*: K viacerým skupinám blokov sa pristupuje ako k jednej logickej skupine. Všetky bitové mapy a tabuľky inode-ov sa nachádzajú v prvej skupine blokov.

b) *64-bit mode*: Má nepriamy vplyv z dôvodu nárastu veľkosti niektorých štruktúr.

c) *Extents*: Použitie extentov pre adresovanie obsahu súborov miesto zastaranej blokovej schémy.

d) *Filetype*: Záznamy v adresároch obsahujú pridanú informáciu o type súborov, ktoré sa v nich nachádzajú.

3. **Vlastnosti kompatibilné len v režime čítania**. Súborový systém s takýmito vlastnosťami môže byť pripojený k operačnému systému len v režime čítania. Parametre, ktoré môžu mať vplyv na rozloženie dát:

a) *Sparse super*: Kópia superbloku sa nachádza len v skupine číslo 0 a potom v každej skupine, ktorej číslo je mocninou 3, 5 alebo 7.

b) *Extra isize*: informuje o prítomnosti inode-ov a väčšou veľkosťou. Môžu poskytovať ďalšie informácie pri vyšetrovaní.

Správanie sa EXT súborového systému

Problematickou vlastnosťou z hľadiska forenznej analýzy je nulovanie (vymazanie) obsahu potrebných metadát v inode štruktúre a inode tabuľkách. Strácame tým možnosť jednoduchého plnohodnotného obnovenia súborov.

Súbory vieme obnoviť tzv. „dolovaním“, v tomto prípade len na základe prechádzania súborového systému so snahou identifikovať hlavičky a pätičky typických súborov (napr. jpg, pdf, docx a iné).

Pre získanie mien súborov, ktoré boli v súborovom systéme zmazané vieme prejsť záznamy jednotlivých priečinkov a prehľadávať tie časti, kde sa nachádzajú ich posledné záznamy, ktoré vypĺňajú zvyšok bloku vyhradeného pre daný priečinok (Obrázok 14.34). Za názvom posledného súboru môžeme nájsť ponechané zvyšky, ale aj celé názvy zmazaných súborov. Iné prístup spočíva v tom, že hľadáme aj celé zmazané priečinky a to tým, že využijeme známu vlastnosť EXT súborového systému. Každý priečinok má identické prvé dva názvy súborov (“.” a “..” – ukazovateľ na seba samého a na rodičovský priečinok). S využitím toho, že vieme dĺžku takéhoto záznamu (Obrázok 14.34), viem prehľadávať celý diskový priestor. Ak narazíme na dva takéto za sebou idúce záznamy v nealokovanom priestore, tak je veľká pravdepodobnosť, že sa nám podarilo nájsť záznamy zo zmazaného priečinka.

Takto vieme získať mená zmazaných súborov, avšak neexistuje žiadny spoľahlivý spôsob, ako by sme ich vedeli spojiť so súbormi, ktoré sa nám podarilo nájsť. Veľkou pomocou v tomto môžu byť záznamy, ktoré sa nachádzajú v žurnálovacom súbore.

Podobne ako existujú pre NTFS alternatívne toky údajov (ADS), tak niečo podobné existuje aj pri EXT4 súborovom systéme. Nazývajú sa rozšírené atribúty (z angličtiny: “extended attributes”). Rozšírené atribúty môžu zlepšovať vlastnosti súborového systému aj iným spôsobom (napr. zoznamy prístupov – ACL). My a zameriame len na tú časť, ktorá sa podobá na ADS. Pre nastavenie skrytého textu používame tento príkaz:

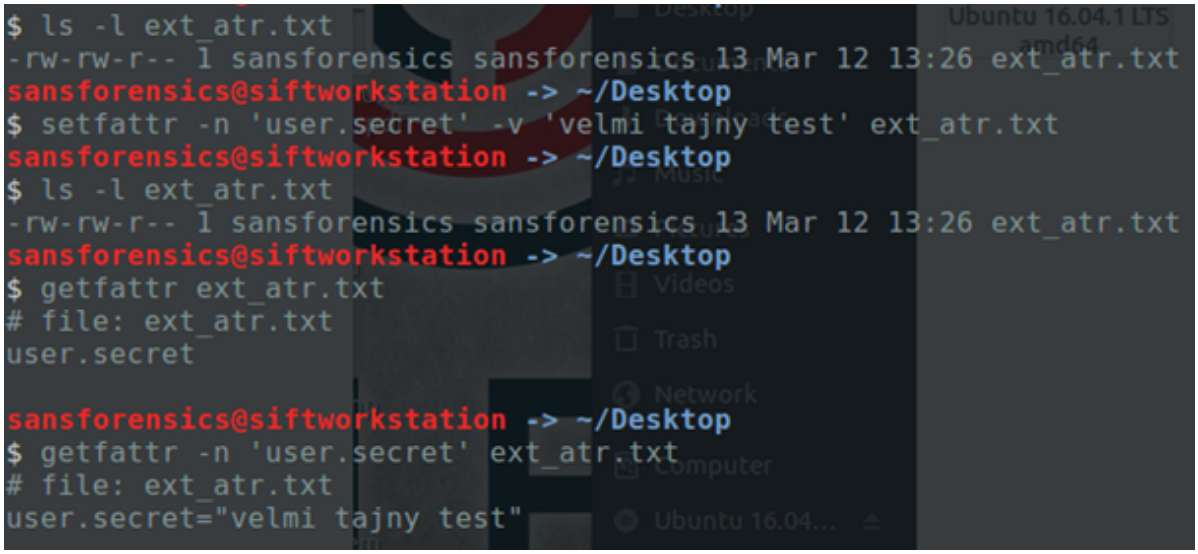
```
setfattr -n 'user.meno' -v 'hodnota' meno_suboru
```

Odhalenie vieme realizovať dvojkrokovo:

1. Príkazom *getfattr meno_súboru* získame výpis všetkých rozšírených atribútov.
2. Príkazom *getfattr -n 'user.meno' meno_súboru* vypíšeme hodnotu atribútu.

Ako môžeme vidieť na obrázku 14.35, tak veľkosť súboru sa nemení ani v prípade pridania skrytého textu cez rozšírený atribút (použitie príkazu *ls* pred a po pridaní textu). Vidíme postupnosť príkazov pre pridanie a vypísanie hodnoty takéhoto atribútu. Keďže takéto prehliadanie každého súboru samostatne by bolo náročné a dosť nepraktické, pri hľadaní môžeme upraviť príkaz getfattr tak, aby prehľadal všetky súbory v priečinku:

```
getfattr *
```



Obr. 14.35: Príklad použitia rozšírených atribútov.

14.6.5 APFS

APFS ((z angličtiny: "Apple File System") je proprietárny súborový systém od spoločnosti Apple, určený pre macOS High Sierra (10.13), iOS 10.3, watchOS 3.2, tvOS 10.2 a ich neskoršie verzie. Jedná sa o tretiu generáciu súborových systémov spoločnosti Apple (po HFS a HFS+), pričom konverziu z HFS+ je možné urobiť za bežnej prevádzky (z angličtiny: "on-the-fly"). V dobe písania tejto kapitoly patrí tento súborový systém k tým najmenej zdokumentovaným a sú známe len niektoré jeho špecifikácie. Kvôli jeho rozšíreniu na určité typy zariadení však pridávame aj jeho, aspoň základný popis.

K významným zmenám, ktoré zaviedol APFS (oproti HFS, či HFS+) patrí zavedenie nanosekundovej podpory pre časové pečiatky pre zmenu a prístup k súborom. Dosiahlo sa to vďaka 64-bitovému rozsahu tohto parametra a číslovanie podporuje od 1. 1. 1970 [37].

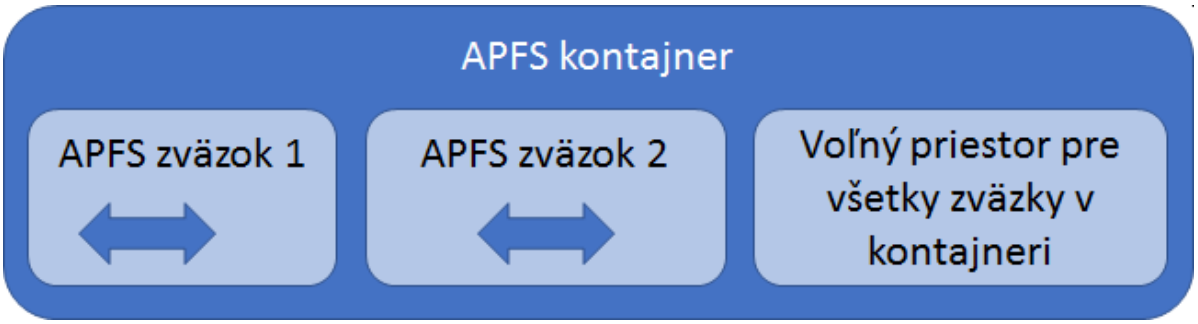
Medzi jeho význačné znaky patria [9]:

- Plná podpora 64-bitových štruktúr.
- Štandardne je kódovaný pomocou little endian.
- Cluster v tomto prípade nazývame blok (podobne ako pri EXT súborových systémoch).
- Jeden blok je obvykle tvorený 4096 bajtmi.
- Podporuje viac ako 9 kvintiliónov (2^{63}) súborov na jednom zväzku.
- Silné zameranie na bezpečnosť. Podporuje viacero šifrovacích kľúčov.
- Kopíruj pri zápise ("copy-on-write"). Každý blok je skopírovaný predtým ako sú aplikované zmeny. Teda existuje história pre všetky súbory, ktoré neboli prepísané a ich súborová štruktúra existuje.

Zavádza nový typ filozofie, kedy zväzky nemajú striktnú veľkosť, ale môžu v čase rásť alebo sa zmenšovať v závislosti od potreby. Sú združené v štruktúre Apple Container, ktorá môže presahovať aj na viac pevných diskov. Pre vytváranie viacerých zväzkov platí obmedzenie na aspoň 512 MB na jeden zväzok (t.j. aspoň 1024 MB pre dva zväzky).

Vďaka štruktúre Apple Container sa dosahuje jedná z inovatívnych vlastností APFS a tou je zdieľanie priestoru medzi jednotlivými zväzkami (z angličtiny: "space sharing"). Bežným prípadom je, že na jednom zväzku máme chýbajúcu kapacitu, kým iný má ešte dostatočné množstvo voľného miesta. APFS tento problém rieši tak, že uberie z kapacity zväzku, ktorý má dostatočne veľa miesta a pridá ju zväzku, ktorý ju momentálne potrebuje. Každý zväzok môže mať nastavenú svoju minimálnu kvótu. Pri tomto prístupe sa dá hovoriť o zväzkoch a zdieľanej voľnej kapacite medzi zväzkami (viď. obrázok 14.36).

Kým pre používateľa takéhoto systému je to výborná funkcionalita. Pre forenzného analytika to môže spôsobiť výrazné problémy. Ak sa po zmazaní súboru zmení veľkosť zväzku a uvoľnené bloky sú presunuté do iného zväzku, prípadne sú vrátené do celkovej voľnej kapacity, tak obnova zmazaných súborov sa stáva extrémne náročnou až nemožnou. Toto platí najmä, ak je každý zväzok šifrovaný iným šifrovacím kľúčom.



Obr. 14.36: Zdieľaný voľný priestor medzi zväzkami [9].

Kopírovanie pri zápise

APFS využíva špeciálny spôsob vytvárania kópií (klonov) súborov CoW ("copy-on-write" – kopírovanie pri zápise). Reálne nevytvára kópiu súboru, ale vytvorí pevný odkaz (z angličtiny: "hard link") na súbor, nový názov súboru a jeho metadáta. Vďaka tomuto prístupu je možné výrazne zvýšiť výkon súborového systému (stačí si predstaviť kopírovanie niekoľko gigabajtových súborov v iných súborových systémoch). Len s použitím tohto princípu by nám vznikal problém pri zmene obsahu jedného z takýchto súborov. Zmeny by sa prejavili aj vo všetkých ďalších súboroch, ktoré sú s danými blokmi previazané cez pevné odkazy. Tento problém sa rieši tak, že pri zmene obsahu súboru sa uložia len zmenené bloky a len pre tento súbor. Týmto sa vedia pôvodne identické súbory postupne odlišovať. Má to za následok veľkú úsporu miesta na zväzku, keďže sa ukladajú len zmenené alebo novovytvorené bloky.

Z pohľadu forenznej analýzy sa jedná o výhodnú vlastnosť, pretože nie je potrebné prehľadávať množstvo totožných súborov. Zväzok môže obsahovať menšie množstvo dát v porovnaní s inými súborovými systémami (menej dát na analýzu) alebo väčšie množstvo unikátneho obsahu.

„Snímky" zväzku

Štandardnou funkciou dnešných operačných systémov je vytváranie bodov pre obnovu systému v čase. APFS pomáha v tomto pomocou snímkou zväzku (z angličtiny: "Snapshot"), ktorý vnáša niekoľko prvkov originality a to najmä:

- Reálne sa nevytvára žiadna kópia dát. Bloky sú označená len na čítanie (read-only).

Všetky ďalšie zmeny spôsobia vytváranie nových blokov (tzv. „delta bloky"). Vďaka tomuto kroku je jednoduché vrátiť sa do pôvodného stavu, stačí odstrániť delta bloky. Prístup je možné použiť aj na obnovenie zmazaných súborov alebo ich častí.

Nevýhody z pohľadu forenznej analýzy

APFS je ľahko náchylný na zmeny. Aj pomerne malá aktivita môže viesť k prepísaniu veľkého množstva súborov. Pri experimentoch sa zistilo, že pripojením, či odpojením zväzku (z angličtiny: "mount" a "umount") zmenili 669 z pôvodne 10 000 zmazaných súborov.

Z toho vyplýva, že vypnutie počítača môže viesť k ešte väčším dôsledkom na stav zväzku. Z tohto dôvodu je výrazne odporúčaná akvizícia súborov na zapnutom ("živom") zariadení.

Ako už bolo spomínané vyššie, ďalším významným skomplikovaním pri vyšetrovaní je štandardne zapnuté šifrovanie objektov na zväzku. Po zmazaní objektu (súboru a jeho metadát) dochádza k jeho uvoľneniu zo zväzku do celkovej voľnej kapacity a môže byť extrémne náročné takýto objekt alebo jeho časť obnoviť.

14.7 Forenzná analýza „živej pamäte"

V predchádzajúcich kapitolách sme sa sústredili primárne na forenznú analýzu súborových systémov, ktoré sa štandardne nachádzajú na pevných diskoch, resp. pamätiach, ktoré sú stabilné pri strate napájania. V tejto časti sa budeme venovať vlastnostiam pamätí, ktoré pri

strate napájanie prichádzajú o uložené údaje. Kombináciou forenznej analýzy pevných diskov a operačnej pamäte získame dva najhodnotnejšie zdroje dôkazov.

14.7.1 Princípy

Operačná pamäť (RAM) je pamäť s náhodným prístupom, ktorá je v drvivej väčšine prípadov používaná CPU pre ukladanie údajov a programov, s ktorými pracuje.

Virtuálna pamäť je abstrakciou reálnej pamäte [43], s ktorou pracuje proces. Obsahuje aj zdrojový kód aj údaje. Pri práci s ňou je potrebné zabezpečiť preklad na reálnu adresu, ktorá sa môže nachádzať v operačnej pamäti alebo aj na pevnom disku (z angličtiny: “swap” alebo “pagefile”). Preklad sa uskutočňuje pomocou tabuľky stránok.

Čo sa v operačnej pamäti nachádza [27]?

- Bežiace procesy.
- Bežiace vlákna.
- Heslá a šifrovacie kľúče.
- Živé registre (OS Windows).
- Bežiace chatovacie aktivity a informácie o prihláseniach.
- Malware (vrátane rootkitov).
- Stav siete a pakety.
- Otvorené súbory, vrátane ešte neuložených súborov.
- Množstvo iných typov údajov.

Aké informácie vieme získať o procesoch?

- Celé meno a cestu k súboru, ku ktorému sa viaže daný proces.
- Argumenty z príkazového riadka, ktorým bol daný proces spustený.
- Identifikačné číslo procesu.
- Identifikačné číslo jeho rodiča. Na základe tohto vieme vytvárať stromy procesov a vieme identifikovať, či niektorý proces nespúšťal neštandardného potomka, napríklad ak by Poznámkový blok spúšťal z príkazového riadku bezpečnostné rozhranie s argumentmi pre nastavenie výnimky pre sieťovú komunikáciu. Procesy, ktoré nemajú rodiča sú podozrivé a vhodné na bližšie preverenie.
- Pracovný priečinok procesu.
- Názov okna v OS Windows.
- Súbory, ovládače, zariadenia, porty, a i., s ktorými proces pracuje.
- Zoznam načítaných modulov (ich mená, cesta k nim, veľkosť).

14.7.2 Výhody získavania údajov z operačnej pamäte

V zjednodušenom ponímaní sa berie, že na pevnom disku sa nachádza „všetko“ a to, čo treba sa presúva do operačnej pamäte, kde sa s daným programom a údajmi pracuje a výsledok sa opäť uloží na pevný disk. Prečo sa teda zaoberať samotnou analýzou operačnej pamäte, keď je to len nejaká forma medzičlánku? V prvom rade preto, že predchádzajúce vnímanie fungovania v počítači je chybné. Útočník môže využiť rôzne nedokonalosti súborového a operačného systému a už v dnešnej dobe existuje množstvo infiltrácií alebo aj útokov, ktoré sa nepotrebujú nikdy „dotknúť“ pevného disku a ich celé fungovanie je viazané na operačnú pamäť. Existujú prípady, kedy sa pred súdom bránili podozriví, že aktivitu na disku nerealizovali oni, ale muselo sa jednať o nejakú formu trójskeho koňa. Čo bez analýzy obrazu operačnej pamäte nebolo možné vyvrátiť.

Kým pevné disky v dnešnej dobe rastú do veľkosti rádovo terabajtov, tak pri operačných pamätiach hovoríme rádovo o gigabajtoch, pričom množstvo „šumu“ (nezaujímavých údajov z pohľadu vyšetrovania) je výrazne menší. Platí, že operačné pamäte vedia poskytnúť veľké množstvo zaujímavých údajov.

Rozdiely v získavaní údajov z pevného disku a z operačnej pamäte

Tak ako pri forenznej analýze súborových systémov, ani tu nemôžeme dôverovať operačnému systému [27], ktorý môže byť kompromitovaný. Z tohto dôvodu potrebujeme vykonávať analýzu v tzv. “offline” režime (vytvoríme si obraz, ktorý neskôr analyzujeme).

Ak zohľadníme prioritu danú nestálosťou údajov (strana 386, časť Nestálosť údajov), tak operačná pamäť má vyššiu prioritu pri zbere údajov a teda mala by byť vykonaná pred zberom údajov z pevného disku. Sledujú sa tým dva ciele:

1. Získanie údajov z pamäte skôr ako dôjde ich strate alebo prepísaniu.
2. Minimalizovať kontamináciu, ktorá vzniká spustením rôznych programov, ktoré zbierajú údaje z vyšetrovaného počítača.

Aj pri vytváraní obrazu samotnej operačnej pamäte dochádza za bežných okolností k jej skresleniu, pretože aj nástroj, ktorý realizuje vytvorenie obrazu sa do nej potrebuje nahrať. Je to prvok, s ktorým je potrebné počítať pri vyšetrovaní a treba ho mať zdokumentovaný. Ďalším rozdielom oproti pevným diskom je, že tu nevieme garantovať vytvorenie 100 % obrazu k bodu v konkrétnom čase. Údaje v operačnej pamäti sa veľmi rýchlo prepisujú a určite sa líši stav zo začiatku procesu zálohovania a z jeho konca. Nie je úplne korektný pojem obraz operačnej pamäte (i keď sa bežne používa), ale vhodnejším pojmom je obraz stránok pamäte, pre ktoré by mala platiť táto konzistencia.

Nejedná sa teda o základnú a opakovateľnú aktivitu. Pri každom jej vykonaní získame iný výsledný obraz operačnej pamäte, aj keď nevykonávame nad ňou žiadnu činnosť (postačuje činnosť procesov na pozadí). Nevieme povedať, že sa jedná o obraz operačnej pamäte s touto časovou pečiatkou. Môžeme povedať, že sa jedná o obraz operačnej pamäte vytvorený v časovom rozmedzí od spustenia procesu vytvárania obrazu až po jeho vyhotovenie.

Existuje však aj spôsob ako získať plnohodnotný obraz operačnej pamäte, ale je veľmi špecifický pre konkrétne situácie [27]:

1. Ak pracujeme s virtuálnym počítačom alebo serverom, tak vieme pozastaviť jeho vykonávanie a takto získať plnohodnotný obraz operačnej pamäte k danému okamihu.

2. Mať k dispozícií špecializovaný (a drahý) hardvér, ktorý obvykle už musí byť zapojený v počítači. V niektorých prípadoch je možné ho pripojiť aj za behu, ale hrozí riziko pádu systému.

3. Získanie údajov zo záznamoch o páde systému, prípadne hibernačných súborov.

Ako postupovať pri získaní obrazu operačnej pamäte?

Spôsob získania obrazu je do veľkej miery závislý od konkrétneho prostredia, v ktorom sa nachádzame. Môže to vyústiť do použitia rôznych metód. Vychádzajúc z obrázku 14.37, vidíme, že pripadá do úvahy niekoľko rôznych scenárov:

1. V najjednoduchšom prípade máme vyšetriť virtuálny počítač. Vtedy stačí pozastaviť vykonávanie a virtualizačný nástroj automaticky zastaví vykonávanie virtuálneho počítača a získame tým presný obraz operačnej pamäte.

2. Ak sa jedná o fyzický počítač, ktorý nie je zapnutý, tak máme k dispozícii obvykle už len to, čo sa nachádza na disku:

   a) Ak počítač len hibernuje, tak na disku nájdeme celý obraz operačnej pamäte.

   b) Ak je vypnutý, tak sa musíme spoľahnúť na súbory, v ktoré majú informáciu o operačnej pamäti z minulosti, ako napríklad: staršie súbory k hibernácií, súbory, do ktorých sa stránkovala operačná pamäť po prekročení jej kapacity (stránkovacie súbory), záznamy z pádov operačného systému (z angličtiny: “crash dump”).

   c) Ak je zapnutý, tak už v princípe nemáme jednoduché riešenia. Ak máme aspoň prístup ku kontu superpoužívateľa / administrátora, môžeme použiť softvérové nástroje, pričom potrebujeme zohľadniť viaceré parametre:

      i. Máme priamy prístup? Nejedná sa o server v serverovni bez klávesnice a obrazovky?

      ii. V akom formáte chceme vyhotoviť obraz?

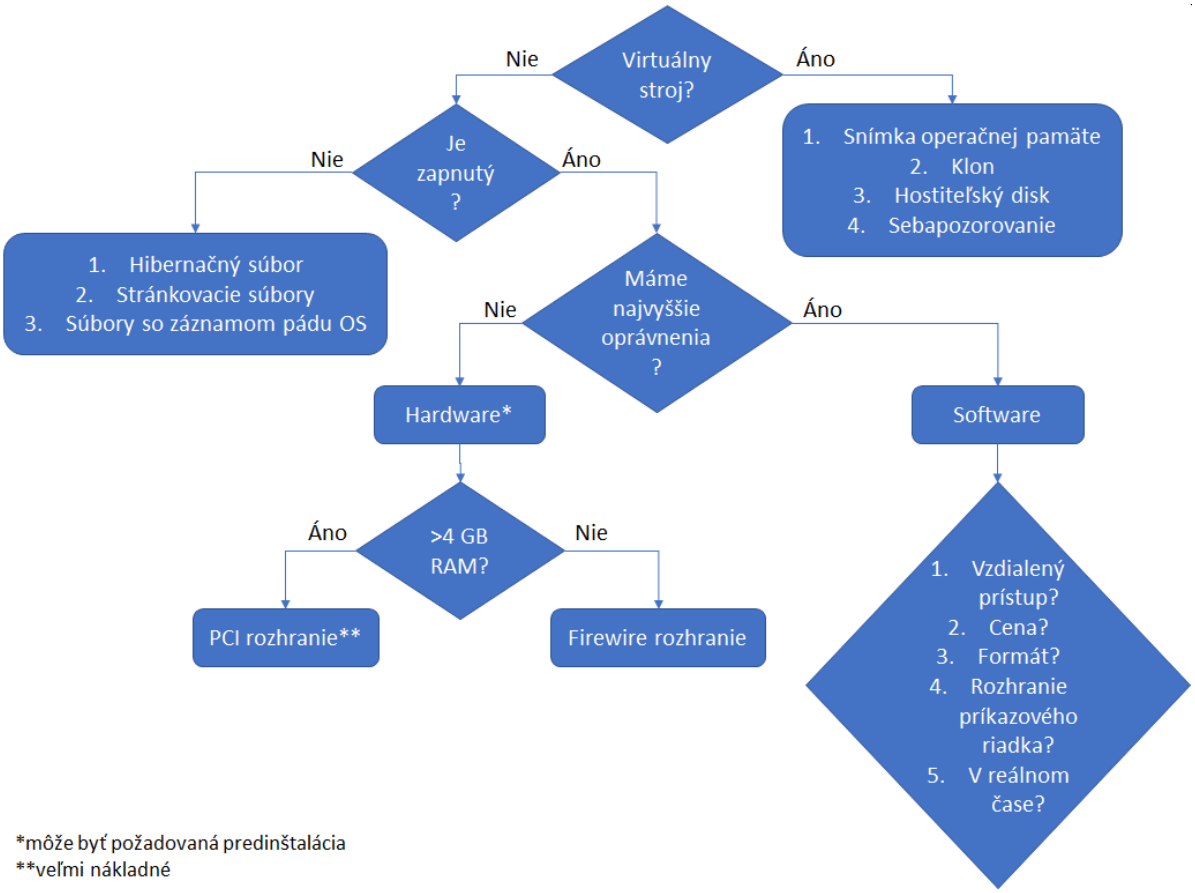
      iii. Použijeme nástroj z príkazového riadka (tzv. CLI) alebo s grafickým rozhraním (tzv. GUI).

      iv. Chceme vytvoriť celý obraz alebo nás zaujímajú len konkrétne časti?

   d) Ak nemáme prístup ku kontu superpoužívateľa / administrátora, môžeme použiť hardvér. Jeho veľkou výhodou je, že môžeme týmto spôsobom získať skutočný obraz pamäte (ak sa jedná o typ, ktorý pozastaví vykonávanie aktivít na procesore). Nevýhodou je, ak vyžaduje zapojenie do počítača, čo sa nemusí podariť bez jeho vypnutia (a tým by sme prišli o všetky údaje).

   e) Ak používame hardvér pre získanie obrazu RAM, môžeme použiť rozhranie firewire (do 4GB RAM) alebo PCI. Použitie tohto riešenia môže byť veľmi nákladné.

V prípade, že nemôžeme použiť žiadnu z uvedených metód, ale pre vyšetrovanie je kriticky dôležité získať údaje z operačnej pamäte, vieme použiť ešte útok zmrazením (z angličtiny: “Cold



Obr. 14.37: Rozhodovací strom pri získaní obrazu operačnej pamäte [27].

boot attack"). Je použiteľný na pamäte typu DRAM, ktoré po strate napájania strácajú uložené informácie rádovo v sekundách. DRAM sa skladá z buniek, ktoré sú vlastne kondenzátormi a pri nižších teplotách sa predlžuje doba ich vybitia. Ak by sme operačnú pamäť schladili napríklad tekutým dusíkom, vieme predĺžiť dobu vybitia na minúty až hodiny. Vieme postupovať dvoma spôsobmi:

1. Vybratie RAM pamätí do iného zariadenia a vytvorenie obrazu.
2. Reštart/zapnutie počítača. Cez BIOS zvolíme načítanie špeciálneho malého programu (nie operačného systému), ktorý vykoná zálohu operačnej pamäte. V tomto prípade treba počítať s prepísaním malej časti operačnej pamäte, potrebnej pre chod programu.

Riziká spojené so získavaním obrazu operačnej pamäte

Pri použití softvéru na získanie obrazu operačnej pamäte narážame na problém, že sa jedná o funkcionalitu, ktorá nie je štandardná a operačné systémy neposkytujú natívne mechanizmy pre jej podporu. Môže to viesť k neočakávaným stavom až pádu systému, to sa môže prejaviť nie len čisto z dôvodu použitia takého softvéru, ale môže k tomu prísť aj z dôvodu kombinácie so zle napísaným malware-om, ktorý sa v operačnej pamäti už nachádza. Je potrebné zvážiť

dôsledky takejto akvizície (jedná sa o kritický systém s dôsledkami na životné prostredie, zdravie, či život obyvateľov) a mať schválené vykonanie takejto aktivity.

Pri použití softvérových nástrojov nie je možné vytvoriť jednoznačný obraz operačnej pamäte, ale vieme hovoriť skôr o obraze pamäťových stránok. Môže tu však dôjsť k poškodeniu, a to v prípade, keď sa nad stránkou začala vykonávať kritická operácia (napr. aktualizovanie jej obsahu), ale kópiu stihneme zhotoviť skôr, ako sa táto operácia dokončila. Zálohovaná stránka z tohto dôvodu obsahuje nekonzistentné údaje, časť z nich obsahuje pôvodnú hodnotu a druhá časť už aktualizovanú.

Veľké riziko môžu predstavovať špeciálne typy malware-u, ktorý ak sa dostal do jadra operačného systému (z angličtiny: “rootkit”), tak môže ukrývať celé časti pamäte pre vyšetrovaním. Jedným z riešení je použitie útoku zmrazením (z angličtiny: “Cold boot attack”).

Útok zmrazením (Cold boot attack)

Ak máme podozrenie na špecifický typ malware-u alebo nedokážeme na zapnutom počítači vytvoriť obraz operačnej pamäte (nedostatočné práva, zamknutý počítač a iné), máme možnosť použiť špeciálnu metódu pre získanie obrazu. Je náročná aj na prípravu aj na znalosti a je použiteľná len na pamäte typu DRAM. Využíva sa skutočnosť, že jednotlivé pamäťové bunky sú tvorené kondenzátormi, ktoré v čase strácajú napätie, ktoré treba periodicky obnovovať, aby nedošlo k strate informácií. Za normálnych okolností hovoríme o jednotkách sekúnd, kedy sa kondenzátor vybije a informácia sa stratí. Ak však pamäť zmrazíme, tak dôjde k predĺženiu doby vybitia na minúty až hodiny. To nám vie poskytnúť dosť času na získanie obrazu operačnej pamäte [16]:

1. Zmrazíme moduly operačnej pamäte na čo najnižšiu teplotu (ideálne tekutým dusíkom).
2. Pripravíme si médium, na ktoré budeme zálohovať obraz pamäte.
3. Máme dve alternatívy:
   a) Ponechať pamäťové moduly v počítači. V takom prípade treba počítač reštartnúť a v BIOS-e nastaviť zavedenie systému z nášho média.
   b) Presunúť moduly do pripraveného počítača, ktorý bude zavádzať nami pripravený systém.
4. Po zapnutí a zavedení nášho malého programu (pozor, nie celého operačného systému) sa začne automaticky vytvárať obraz operačnej pamäte.

Je potrebné, aby sme nepoužívali žiadnu živú verziu operačného systému, ale špeciálne vytvorený program pre tento účel. Je to potrebné z dôvodu minimalizácie množstva zápisov do operačnej pamäte, čím by došlo k veľkému prepísaniu potenciálnych dôkazov.

Z vyššie uvedeného dôvodu vidíme, že pamäť typu DRAM patrí medzi nedôveryhodné, pretože sa nevieme spoľahnúť, že po vypnutí z nej údaje zmiznú. Môže to byť kritickým parametrom pri špeciálnych nasadeniach (napr. spravodajská činnosť).

14.7.3 Nástroje a formáty obrazu operačnej pamäte

Nástroje pre získanie alebo analýzu obrazu operačnej pamäte

Existuje viacero softvérových nástrojov, ktoré je možné použiť na získanie obrazu operačnej pamäte. Medzi úplne základne aj tu patrí nástroj *dd*, ktorý vieme použiť aj pre Windows (*dd if=\\.\PhysicalMemory of=memory.img*) alebo aj pre staršie verzie Linuxoc (*dd if=/dev/mem of=memory.img*). Prečo je použiteľný len pre staršie verzie Linuxu? Pretože operačná pamäť sa už v dnešnej dobe nemapuje k priečinkom /dev/mem, či /dev/kmem. Udialo sa tak z bezpečnostných dôvodov, takto mal totiž malware priamy prístup k časti operačnej pamäti).

Medzi iné nástroje, ktoré vieme použiť patria napríklad:

- Lime,
- Winen,
- FTK Imager,
- Redline,
- Fast Dump.

Keď už máme získaný obraz operačnej pamäte, tak rozpoznávame viacero nástrojov. Tieto majú za sebou istý historický vývoj a delíme ich na viacero generácií.

Nástroje nultej generácie

Bežne používané pred rokom 2004. Tvorené najmä kombináciou príkazov *strings* a *grep*, ktoré vedeli vypísať ASCII znaky z operačnej pamäte a nad nimi realizovať základnú formu filtrácie a vyhľadávania. Týmto spôsobom sme vedeli získať obrovské množstvo údajov (aj okolo 10 % pôvodnej veľkosti obrazu). Nevýhodou bolo, že neexistuje kontext nad týmito údajmi. Dá sa odpovedať otázka „Čo“ z 5WH otázok, ale nevieme spojiť túto informáciu s bežiacim procesom, či používateľom, ktorý túto aktivitu vykonal. Stále však vieme získať množstvo dobrých informácií, napríklad: správy na obrazovke, otvorené dokumenty, mená programov, heslá (za určitých podmienok), informácie ohľadne sieťového pripojenia.

Nástroje prvej generácie

Predstavuje rozšírenie predchádzajúcej generácie o získavanie základných štruktúr operačných systémov pri práci s operačnou pamäťou. Schopnosť analyzovať záznamy z pádov operačného systému.

Nástroje druhej generácie

Vznik prvých automatizovaných nástrojov, ktoré podporujú obvykle viacero operačných systémov. Typickým príkladom je výborný nástroj Volatility, ktorému sa budeme venovať aj neskôr.

Nástroje tretej generácie

Začal sa klásť dôraz na vizualizáciu, cloudové a virtualizačné riešenia. Zástupcami tejto generácie sú Microsoft LiveKd alebo Moon Sols LiveCloudKd.

Nástroj Volatility

Nástroj Volatily patrí medzi najvýznamnejšie voľne dostupné nástroje pre analýzu obrazu operačnej pamäte. Aj keď patrí k nástrojom tzv. „druhej generácie“, stále patrí medzi lídrov v tejto oblasti a vďaka širokej podpore dokáže vydávať nové aktualizácie extrémne rýchlo. Celý nástroj je vytvorený v programovacom jazyku Python a je modulárny, vďaka čomu ho je možné ľahko rozširovať a používať na väčšine platforiem. Zároveň, nie len, že je ho možné spustiť vo viacerých typoch operačných systémov, ale dokáže pracovať s obrazmi pamäte operačných systémov Windows, Linux, MAC OS a Android.

Volatility poskytuje rozhranie pre ovládanie cez príkazový riadok, ale existujú už aj pokusy o vytvorenie grafickej nadstavby [50].

Každá verzia každého operačného systému pristupuje k operačnej pamäti trochu inak a môže používať odlišné štruktúry. Pre korektnú analýzu je potrebné mať nastavený správny profil vo Volatility:

- Windows: pri tvorbe profilov sa spoliehame na hodnoty v štruktúre kdbg, ktorá je typická pre operačné systémy Microsoftu. Slúži jadru operačného systému na ladiace účely. Obsahuje zoznam bežiacich procesov a načítaných modulov jadra. Obsahuje tiež informácie o verzii, čo umožňuje napríklad rozlíšiť aj, či daný Windows má alebo nemá nainštalovaný tzv. Service pack. Sofistikovaný malware však vie meniť tieto hodnoty a obraz operačnej pamäte sa potom môže tváriť, ako keby patril k inej verzii OS Windows.

- Linux a Mac OS sú v tomto ohľade komplikovanejšie, pretože existuje veľké množstvo ich verzií, ktoré sa odlišujú verziou jadra, či jeho podverziami. V prípade operačného systému Linux sa môže jednať o viac ako 500 možností. Aj tu existuje možnosť stiahnuť si vlastný profil[17,18]. Odporúčaným postupom je však vytvoriť si vlastný profil na virtuálnom počítači, ktorý má rovnaké parametre ako vyšetrovaný. Návody pre vytvorenie profilu existujú aj pre Linux [44] aj pre Mac OS [45].

Okrem základného použitia [49] existuje viacero hutných výberov príkazov [46], [47], [10], ktoré sú užitočné pri zoznamovaní sa s týmto nástrojom, prípadne na základné vyšetrovanie. Na konci tejto kapitoly si ukážeme jednoduchý príklad vyšetrovania operačnej pamäte aj pomocou nástroja Volatility.

Príklady formátov obrazov operačnej pamäte

Existuje viacero možností ako sa vieme dostať k celej operačnej pamäti alebo jej časti. Niektoré z nich si uvedieme nižšie.

[17] https://github.com/volatilityfoundation/profiles
[18] https://www.osforensics.com/downloads/Collection.zip

„Surový obraz pamäte“

Čistý obraz operačnej pamäte, ktorý má najširšiu podporu medzi forenznými nástrojmi. Často sa používa zachovanie priestorovej integrity vytváraného obrazu. V prípade, ak sa nepodarí pristúpiť k niektorej časti alebo dôjde k problém počas kopírovania stránky, tak môže dôjsť k doplneniu tejto časti prázdnymi bajtmi. Je to dôležité z pohľadu zachovania relatívnej pozície údajov voči iným údajom. Takto vytvorený obraz neobsahuje žiadne prídavné štruktúry. V tom je zásadný rozdiel oproti špecializovaným prístupom pre uloženie obsahu operačnej pamäte. Tie môžu obsahovať ďalšie prídavné štruktúry, ktoré môžu mať vyplnené informácie pre ľahšiu prácu a obrazom pamäte.

Záznamy OS Windows o páde systému (z angličtiny: “Windows crash dumps”)

Vznikajú počas toho ako sa operačný systém dostane do nedefinovaného stavu a dôjde k jeho pádu (známe aj ako „modrá obrazovka smrti“ – BSOD). Počas tohto pádu sa ukladá obraz operačnej pamäte na disk. Môže sa jednať o plnohodnotný úplný obraz, alebo len o malý záznam. Najčastejšie je tvorený časťou operačnej pamäte, v ktorej sa nachádza jadro operačného systému (tzv. kernel) a prípadne časť, ktorá spôsobila pád systému [32]. Pre spracovanie inými nástrojmi (napríklad Volatility), sa musí jednať o úplný obraz [29].

Privodiť takýto stav operačného systému (v závislosti od verzie) sa dá aj pomocou aplikácie NotMyFault. Nevýhodou čiastočných obrazov je, že sú vhodné pre ladenie (z angličtiny: “debugging”) a nie pre forenznú analýzu.

Hibernačný súbor (hiberfil.sys)

Jedná sa o komprimovanú kópiu operačnej pamäte, ktorá má svoju hlavičku v OS Windows (PO_MEMORY_IMAGE). Pre komprimáciu sa používa Xpress kompresný algoritmus, ktorý existuje v súčasnosti v troch variantoch [31]. Vzhľadom na použitie kompresného algoritmu máme dve možnosti, ako pristupovať k práci s týmto súborom:

1. Pri každej operácií (napríklad výpis bežiacich procesov uložených v RAM) dôjde k rozbaleniu príslušnej časti pamäte a vykonaniu potrebnej operácie.

2. Pamäť najskôr celú rozbalíme a potom analyzujeme jej obsah.

Nevýhodou takto získaného obrazu je, že sa strácajú informácie o DHCP konfigurácií, ktorá je uvoľnená a aktívne spojenia sú ukončené. To môže spôsobiť neúplne informácie o sieťovej komunikácií.

Naopak, výhodou je, že tento súbor nie je obvykle nikdy zmazaný. Vymazáva sa len prvá stránka (jej hlavička) po obnovení systému z hibernácie. Teda, ak bol počítač aspoň raz hibernovaný, tak sa vieme dostať k nejakému historickému obrazu jeho operačnej pamäte.

Výstupy z virtualizačných nástrojov

Pomocou hypervízora vieme získať obvykle plnohodnotný obraz operačnej pamäte, keď dáme pozastaviť vykonávanie virtuálneho počítača. V niektorých prípadoch (napríklad Virtual box) nemusia automaticky ukladať celý obraz, ale je potrebné túto funkciu nastaviť, resp.

vytvoriť obraz manuálne. Môžeme získať aj rôzne zaujímavé údaje, napríklad VM Ware je schopný „zmraziť“ aj SSL/TLS spojenia. V závislosti od použitého virtualizačného nástroja môžeme získať obraz operačnej pamäte v rôznych formátoch.

14.7.4 Odporúčané postupy

Pri získavaní obrazu operačnej pamäte je dobré pamätať na odporúčané postupy, ako napríklad [27]:

- Byť minimálne invazívny. Zvoliť taký typ programu pre vytvorenie obrazu, ktorý zaberie čo najmenšiu časť v operačnej pamäti (minimalizovanie množstva prepísaných údajov). Aj dobre napísaná aplikácia s grafickým rozhraním môže mať menší dopad ako zle napísaná aplikácia v príkazovom riadku.
- Nepoužívať lokálny disk. Ak sa riadime prioritou nestálosti údajov, tak získavanie údajov z operačnej pamäti je pred získavaním údajov z pevného disku. Pri ukladaní na disk podozrivého počítača by sme mohli prepísať časti disku, kde sa nachádzali zmazané súbory. Ak by sme opomenuli aj tento fakt, tak nemenej dôležitá je skutočnosť, že by sme zasahovali do potenciálneho dôkazu. Tým by sme mohli spôsobiť jeho nepoužiteľnosť pred súdom. Miesto lokálnych pevných diskov sa preto odporúčajú externé pamäte (USB kľúče / disky, SD karty, a i.).
- Používať sterilizované média. Boli premazané spôsobom korektným pre použitie vo forenznej analýze. Treba pamätať na použitie vhodného súborového systému na externom pamäťovom médiu. Napríklad:
  - V dnešnej dobe je vo väčšine prípadov nevhodné používať súborový systém FAT (12, 16 aj 32), pretože umožňuje vytvárať súbory s maximálnou veľkosťou 4 GB. Bežná veľkosť operačnej pamäte je násobne väčšia. Lepšou alternatívou je použitie NTFS súborového systému.
  - Súborový systém by mal byť podporovaný operačným systémom vyšetrovaného počítača. Napríklad, nemá zmysel používať EXT4 na OS Windows, alebo EXT4 so špeciálnymi nastaveniami (napríklad flex_bg, extents), ktoré cieľový operačný systém nepodporuje.
- Výslednému obrazu operačnej pamäte zhotoviť odtlačok (z angličtiny: “hash”).
- Po zrealizovaní vyššie uvedených krokov je vhodné ešte skopírovať všetky súbory, ktoré obsahujú:
  - Záznamy o páde systému.
  - Hibernačné súbory.
  - Súbory, ktoré slúžia na odkladanie údajov operačnej pamäte na disk (napríklad, pre Windows sa jedná o pagefile.sys).

Pri získavaní obrazu pamäte (a najmä pri vyšetrovaní) treba pamätať na skutočnosť, že aj v operačnej pamäti môžeme uvoľniť obsah danej stránky a nemusí pritom prísť k zamazaniu jej údajov. Teda ako pri zmazaných súboroch, aj tu viem získať ďalšie informácie. Vzhľadom na

rýchlosť a veľkosť operačnej pamäte však treba počítať so skutočnosťou, že priemerná životnosť uvoľnených stránok je do päť minút.

14.7.5 Jednoduchý príklad analýzy obrazu operačnej pamäti

Uvedieme si jednoduchý príklad analýzy obrazu operačnej pamäti. Použijeme na to veľmi dobre zdokumentovaný prípad malwere-u Zeus [53]. Obraz operačnej pamäti infikovaného zariadenia (zeus.vmem) je pomerne jednoduché nájsť na internete [26].

Existuje množstvo podrobných návodov (napríklad [54]) ako identifikovať tento typ infekcie. My ho však použijeme primárne pre ukážku práce s operačnou pamäťou. Pre tento príklad sú potrebné len minimálne znalosti operačného systému Linux alebo Windows. V oboch prípadoch je potrebné skontrolovať si, či sú v systéme nainštalované nástroj Python a Volatility. Kapitola 14.7.5 je primárne určená pre analýzu v OS Linux.

Príkaz strings

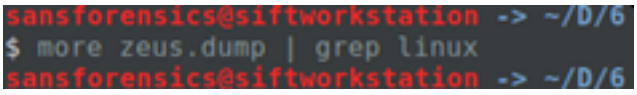
Ako sme spomínali vyššie, tak operačná pamäť síce obsahuje množstvo binárnych údajov, ktoré nie sú človeku ľahko čitateľné, ale obsahuje aj množstvo čitateľných znakov (tzv. ASCII znaky). Ak použijeme príkaz:

```
strings zeus.vmem > zeus.dump
```

Pri bližšom pozretí zistíme, že z pôvodného 137 MB obrazu operačnej pamäte sme získali 11,5 MB znakový výstup, s ktorým vieme ďalej pracovať. V ďalšom kroku je časté použitie kombinácie príkazov more a grep. Napríklad vieme využiť tieto možnosti

Jednoduché zistenie, či sa jedná o obraz operačne pamäte OS Linux. Na obrázku 14.38 vidíme, že sa pravdepodobne nebude jednať o operačný systém Linux, keďže sa nám nepodarilo nič nájsť.

```
more zeus.vmem | grep linux
```



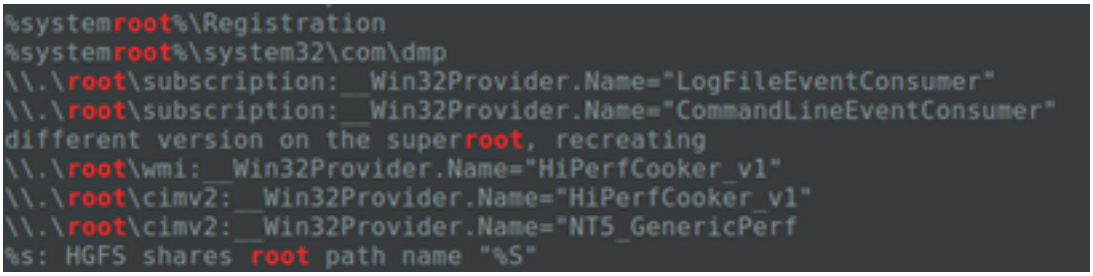
Obr. 14.38: Použitie príkazu a jeho výstup.

Z tohto dôvodu vyskúšame nájsť niečo typické pre Linux a tým je adresár „root", ktorého nejaká časť by sa mohla nachádzať v operačnej pamäti. Na obrázku 14.39 vidíme ukážku takého výpisu. Vidíme, že sme niečo našli, avšak vyzerá to tak, že sa bude jednať o obraz operačného systému Windows. Napovedá nám v tomto najmä reťazec „Win32".

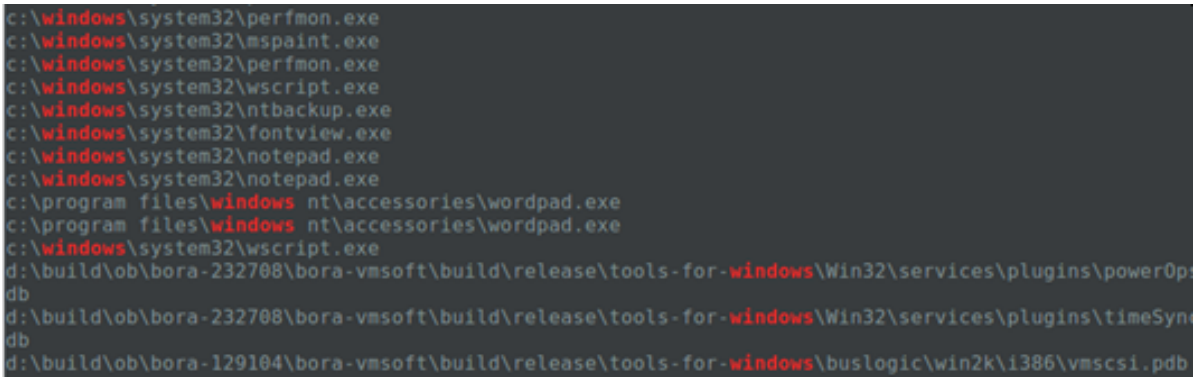
```
more zeus.vmem | grep root
```

Keďže sa nám vyšetrovaný obraz pamäte javí ako získaný z OS Windows, vyskúšame si to overiť ďalším príkazom. Na obrázku 14.40 máme časť výpisu a vidíme, že sa nám podarilo nájsť množstvo konštrukcií známych z tohto operačného systému.

```
more zeus.vmem | grep windows
```



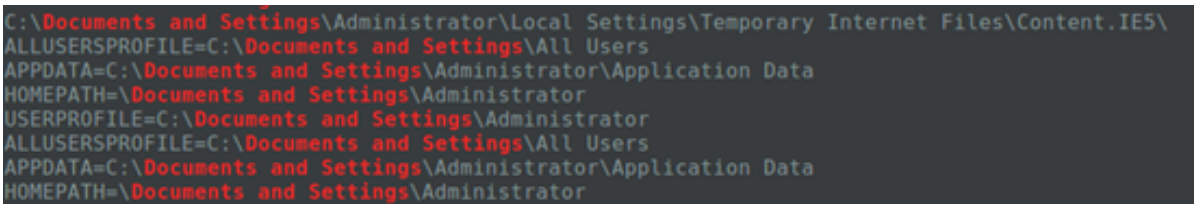
Obr. 14.39: Vypísanie reťazcov, ktoré obsahujú časť „root“.



Obr. 14.40: Hľadanie reťazca „windows“.

Keď sme zistili, že sa pravdepodobne jedná o OS Windows, tak sa môžeme pokúsiť nájsť používateľov v systéme. Je známe, že pre novšie verzie sa nachádzajú v priečinku „Documents and Settings“, teda sa ho pokúsime nájsť. Vidíme časť výpisu (Obrázok 14.41), na základe ktorého sa môžeme čiastočne domnievať, že pravdepodobne bude prihlásený Administrátor, keďže vidíme jeho meno v časti domovského adresára „HOMEPATH“.

```
more zeus.vmem | grep 'Documents and Settings'
```

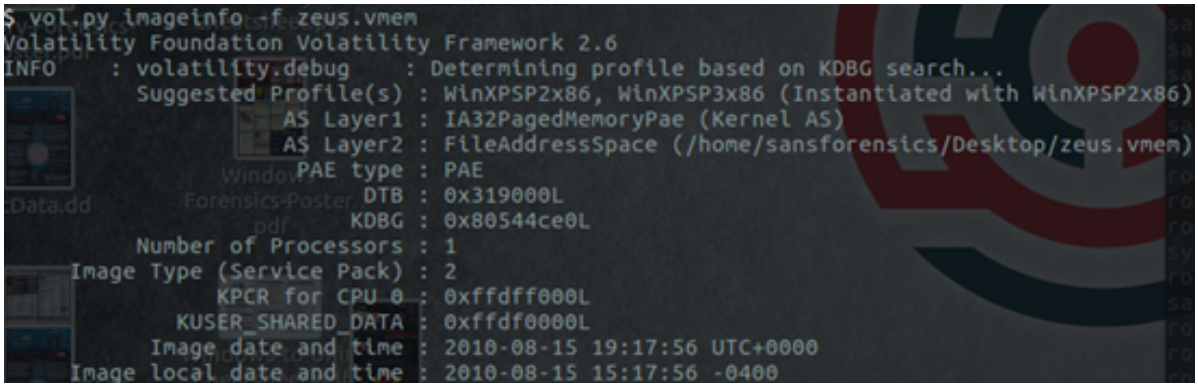


Obr. 14.41: Pokus o nájdete prihláseného používateľa.

Pre všetky vyššie zistenia je potrebné sa ich pokúsiť potvrdiť aj iným spôsobom. Keďže týmto spôsobom nemáme prístup k celej časti operačnej pamäte, tak väčšina zistení pomocou príkazov strings a grep zostáva v štádiu domnienok, ktoré je potrebné potvrdiť iným spôsobom.

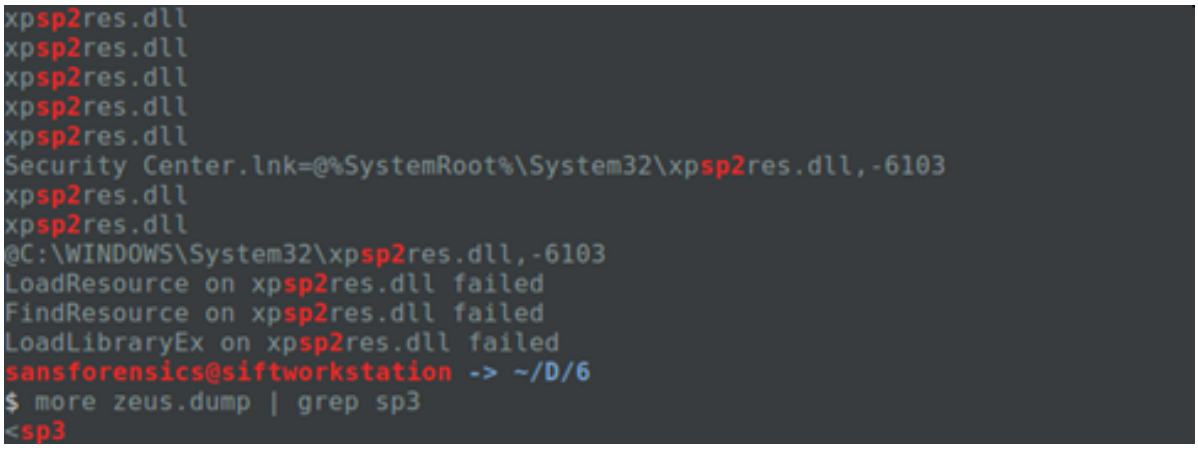
Nástroj Volatility

V predchádzajúcom prípade sme získali podozrenie, že nami analyzovaný obraz pamäte je z operačného systému Windows. Môžeme sa v tom utvrdiť použitím príkazu *imageinfo* v nástroji Volatility. Na obrázku 14.42 vidíme, že sa nám podarilo zistiť, že sa jedná určite o obraz operačnej pamäte OS Windows, konkrétne o verziu Windows XP, ktorá má nainštalovaný Service pack 2 alebo Service pack 3 (v časti *Suggested profile*). K dispozícií máme aj ďalšie informácie, za všetky sa môžeme pozrieť na „AS Layer 2“, kde môžeme vidieť, že sa jedná o 32 bitovú architektúru (“IA32. . . “).



Obr. 14.42: Zistenie profilu pre operačný systém Windows.

Na obrázku 14.43 opätovne môžeme použiť príkaz strings, kde najskôr hľadáme výskyt reťazca „sp2“ a následne „sp3“. Z nájdených výsledkov to vyzerá, že je nainštalovaný Service pack 2.



Obr. 14.43: Pokus o spresnenie, či je použitý Service pack 2 alebo 3.

Ak sme si už istý profilom, ktorý chceme používať, máme k dispozícií ďalšie príkazy nástroja Volatility. V rámci každého príkazu doplníme „*profile=WinXPSP2x86*“, čo nám zabezpečí prehľadávanie operačnej pamäte podľa štruktúr, ktoré používa Windows XP so Service pack 2. Ak sa chceme orientovať na výpis procesov, tak máme viacero možností:

- Príkaz *pslist* umožňuje základný výpis procesov. Prechádza špeciálnu štruktúru, v ktorej sú jednotlivé procesy zreťazené. Z tohto dôvodu nedokáže identifikovať skryté procesy alebo procesy, ktoré sa nenachádzajú v tejto štruktúre. V oboch prípadoch je to výrazne podozrivá situácia, hodná ďalšieho vyšetrovania. Máme k dispozícii viacero informácií o procesoch (Obrázok 14.44), ako sú posun vo virtuálnej pamäti (Offset), meno procesu (name), identifikačné číslo procesu a jeho rodičia (PID a PPID), počet vlákien a mnohé iné.

```
vol.py -f zeus.vmem --profile=WinXPSP2x86 pslist
```

```
sansforensics@siftworkstation -> ~/D/6
$ vol.py -f zeus.vmem --profile=WinXPSP2x86 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0x810b1660 System                    4      0     58      379 ------      0
0xff2ab020 smss.exe                544      4      3       21 ------      0 2010-08-11 06:06:21 UTC+0000
0xff1ecda0 csrss.exe               608    544     10      410      0      0 2010-08-11 06:06:23 UTC+0000
0xff1ec978 winlogon.exe            632    544     24      536      0      0 2010-08-11 06:06:23 UTC+0000
0xff247020 services.exe            676    632     16      288      0      0 2010-08-11 06:06:24 UTC+0000
0xff255020 lsass.exe               688    632     21      405      0      0 2010-08-11 06:06:24 UTC+0000
0xff218230 vmacthlp.exe            844    676      1       37      0      0 2010-08-11 06:06:24 UTC+0000
0x80ff88d8 svchost.exe             856    676     29      336      0      0 2010-08-11 06:06:24 UTC+0000
0xff217560 svchost.exe             936    676     11      288      0      0 2010-08-11 06:06:24 UTC+0000
0x80fbf910 svchost.exe            1028    676     88     1424      0      0 2010-08-11 06:06:24 UTC+0000
0xff22d558 svchost.exe            1088    676      7       93      0      0 2010-08-11 06:06:25 UTC+0000
0xff203b80 svchost.exe            1148    676     15      217      0      0 2010-08-11 06:06:26 UTC+0000
0xff1d7da0 spoolsv.exe            1432    676     14      145      0      0 2010-08-11 06:06:26 UTC+0000
0xff1b8b28 vmtoolsd.exe           1668    676      5      225      0      0 2010-08-11 06:06:35 UTC+0000
0xff1fdc88 VMUpgradeHelper        1788    676      5      112      0      0 2010-08-11 06:06:38 UTC+0000
0xff143b28 TPAutoConnSvc.e        1968    676      5      106      0      0 2010-08-11 06:06:39 UTC+0000
0xff25a7e0 alg.exe                 216    676      8      120      0      0 2010-08-11 06:06:39 UTC+0000
0xff364310 wscntfy.exe             888   1028      1       40      0      0 2010-08-11 06:06:49 UTC+0000
0xff38b5f8 TPAutoConnect.e        1084   1968      1       68      0      0 2010-08-11 06:06:52 UTC+0000
0x80f60da0 wuauclt.exe            1732   1028      7      189      0      0 2010-08-11 06:07:44 UTC+0000
0xff3865d0 explorer.exe           1724   1708     13      326      0      0 2010-08-11 06:09:29 UTC+0000
0xff3667e8 VMwareTray.exe          432   1724      1       60      0      0 2010-08-11 06:09:31 UTC+0000
0xff374980 VMwareUser.exe          452   1724      8      207      0      0 2010-08-11 06:09:32 UTC+0000
0x80f94588 wuauclt.exe             468   1028      4      142      0      0 2010-08-11 06:09:37 UTC+0000
0xff224020 cmd.exe                 124   1668      0 --------      0      0 2010-08-15 19:17:55 UTC+0000   2010-08-15 19:17:56 UTC+0000
```

Obr. 14.44: Vypísanie procesov.

- Veľmi podobný prístup a obmedzenia má aj príkaz *pstree*. Jediným zásadným rozdielom snaha o prehľadnejší výpis procesov tak, aby bolo intuitívne, ktorý proces má akého rodiča (Obrázok 14.45).

```
vol.py -f zeus.vmem --profile=WinXPSP2x86 pstree
```

- Aby sme vedeli identifikovať skryté procesy a procesy mimo štandardnej štruktúry, potrebujeme *psscan* (Obrázok 14.46). Tento príkaz sa pokúša nájsť hlavičku, ktorú používajú štruktúry, ktoré ukladajú informácie o procesoch. Vďaka tomu dokáže získať informácie o viacerých procesoch, vrátane tých, ktoré boli ukončené a už si mimo štandardného zreťazenia procesov.

```
vol.py -f zeus.vmem --profile=WinXPSP2x86 psscan
```

Podobne je to so sieťovými spojeniami, kde máme k dispozícii príkaz *connections*, ktorý zobrazí aktívne bežiace TCP spojenia. V tomto prípade (Obrázok 14.47) môžeme povedať, že vo vyšetrovanej pamäti neprebiehali žiadne TCP spojenia.

```
vol.py -f zeus.vmem --profile=WinXPSP2x86 connections
```

Na rozdiel od predchádzajúceho prístupu, príkaz *connscan* (Obrázok 14.48), ktorý sa snaží nájsť štruktúru typickú pre TCP spojenia. Vďaka tomu môže nájsť aj predchádzajúce realizované TCP spojenia, ktoré sú ešte naďalej uložené v operačnej pamäti. Vidíme posun do

```
sansforensics@siftworkstation -> ~/D/6
$ vol.py -f zeus.vmem --profile=WinXPSP2x86 pstree
Volatility Foundation Volatility Framework 2.6
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x810b1660:System                                      4      0     58    379 1970-01-01 00:00:00 UTC+0000
. 0xff2ab020:smss.exe                                 544      4      3     21 2010-08-11 06:06:21 UTC+0000
.. 0xff1ec978:winlogon.exe                            632    544     24    536 2010-08-11 06:06:23 UTC+0000
... 0xff255020:lsass.exe                              688    632     21    405 2010-08-11 06:06:24 UTC+0000
... 0xff247020:services.exe                           676    632     16    288 2010-08-11 06:06:24 UTC+0000
.... 0xff1b8b28:vmtoolsd.exe                         1668    676      5    225 2010-08-11 06:06:35 UTC+0000
..... 0xff224020:cmd.exe                              124   1668      0 ------ 2010-08-15 19:17:55 UTC+0000
.... 0x80ff88d8:svchost.exe                           856    676     29    336 2010-08-11 06:06:24 UTC+0000
.... 0xff1d7da0:spoolsv.exe                          1432    676     14    145 2010-08-11 06:06:26 UTC+0000
.... 0x80fbf910:svchost.exe                          1028    676     88   1424 2010-08-11 06:06:24 UTC+0000
..... 0x80f60da0:wuauclt.exe                         1732   1028      7    189 2010-08-11 06:07:44 UTC+0000
..... 0x80f94588:wuauclt.exe                          468   1028      4    142 2010-08-11 06:09:37 UTC+0000
..... 0xff364310:wscntfy.exe                          888   1028      1     40 2010-08-11 06:06:49 UTC+0000
.... 0xff217560:svchost.exe                           936    676     11    288 2010-08-11 06:06:24 UTC+0000
.... 0xff143b28:TPAutoConnSvc.e                      1968    676      5    106 2010-08-11 06:06:39 UTC+0000
..... 0xff38b5f8:TPAutoConnect.e                     1084   1968      1     68 2010-08-11 06:06:52 UTC+0000
.... 0xff22d558:svchost.exe                          1088    676      7     93 2010-08-11 06:06:25 UTC+0000
.... 0xff218230:vmacthlp.exe                          844    676      1     37 2010-08-11 06:06:24 UTC+0000
.... 0xff25a7e0:alg.exe                               216    676      8    120 2010-08-11 06:06:39 UTC+0000
.... 0xff203b80:svchost.exe                          1148    676     15    217 2010-08-11 06:06:26 UTC+0000
.... 0xff1fdc88:VMUpgradeHelper                      1788    676      5    112 2010-08-11 06:06:38 UTC+0000
.. 0xff1ecda0:csrss.exe                               608    544     10    410 2010-08-11 06:06:23 UTC+0000
 0xff3865d0:explorer.exe                             1724   1708     13    326 2010-08-11 06:09:29 UTC+0000
. 0xff374980:VMwareUser.exe                           452   1724      8    207 2010-08-11 06:09:32 UTC+0000
. 0xff3667e8:VMwareTray.exe                           432   1724      1     60 2010-08-11 06:09:31 UTC+0000
```

Obr. 14.45: Výpis procesov v stromovej forme.

```
$ vol.py -f zeus.vmem --profile=WinXPSP2x86 psscan
Volatility Foundation Volatility Framework 2.6
Offset(P)          Name                PID   PPID PDB        Time created                   Time exited
------------------ ---------------- ------ ------ ---------- ------------------------------ ------------------------------
0x00000000010c3da0 wuauclt.exe        1732   1028 0x06cc02c0 2010-08-11 06:07:44 UTC+0000
0x00000000010f7588 wuauclt.exe         468   1028 0x06cc0180 2010-08-11 06:09:37 UTC+0000
0x0000000001122910 svchost.exe        1028    676 0x06cc0120 2010-08-11 06:06:24 UTC+0000
0x000000000115b8d8 svchost.exe         856    676 0x06cc00e0 2010-08-11 06:06:24 UTC+0000
0x0000000001214660 System                4      0 0x00319000
0x000000000211ab28 TPAutoConnSvc.e    1968    676 0x06cc0260 2010-08-11 06:06:39 UTC+0000
0x00000000049c15f8 TPAutoConnect.e    1084   1968 0x06cc0220 2010-08-11 06:06:52 UTC+0000
0x0000000004a065d0 explorer.exe       1724   1708 0x06cc0280 2010-08-11 06:09:29 UTC+0000
0x0000000004b5a980 VMwareUser.exe      452   1724 0x06cc0300 2010-08-11 06:09:32 UTC+0000
0x0000000004be97e8 VMwareTray.exe      432   1724 0x06cc02e0 2010-08-11 06:09:31 UTC+0000
0x0000000004c2b310 wscntfy.exe         888   1028 0x06cc0200 2010-08-11 06:06:49 UTC+0000
0x0000000005471020 smss.exe            544      4 0x06cc0020 2010-08-11 06:06:21 UTC+0000
0x0000000005f027e0 alg.exe             216    676 0x06cc0240 2010-08-11 06:06:39 UTC+0000
0x0000000005f47020 lsass.exe           688    632 0x06cc00a0 2010-08-11 06:06:24 UTC+0000
0x0000000006015020 services.exe        676    632 0x06cc0080 2010-08-11 06:06:24 UTC+0000
0x00000000061ef558 svchost.exe        1088    676 0x06cc0140 2010-08-11 06:06:25 UTC+0000
0x0000000006238020 cmd.exe             124   1668 0x06cc02a0 2010-08-15 19:17:55 UTC+0000   2010-08-15 19:17:56 UTC+0000
0x0000000006384230 vmacthlp.exe        844    676 0x06cc00c0 2010-08-11 06:06:24 UTC+0000
0x00000000063c5560 svchost.exe         936    676 0x06cc0100 2010-08-11 06:06:24 UTC+0000
0x0000000006499b80 svchost.exe        1148    676 0x06cc0160 2010-08-11 06:06:26 UTC+0000
0x000000000655fc88 VMUpgradeHelper    1788    676 0x06cc01e0 2010-08-11 06:06:38 UTC+0000
0x00000000066f0978 winlogon.exe        632    544 0x06cc0060 2010-08-11 06:06:23 UTC+0000
0x00000000066f0da0 csrss.exe           608    544 0x06cc0040 2010-08-11 06:06:23 UTC+0000
0x0000000006945da0 spoolsv.exe        1432    676 0x06cc01a0 2010-08-11 06:06:26 UTC+0000
0x00000000069a7328 VMip.exe           1944    124 0x06cc0320 2010-08-15 19:17:55 UTC+0000   2010-08-15 19:17:56 UTC+0000
0x00000000069d5b28 vmtoolsd.exe       1668    676 0x06cc01c0 2010-08-11 06:06:35 UTC+0000
```

Obr. 14.46: Výpis aj ukončených a skrytých procesov.

pamäte (Offset), lokálnu a vzdialenú adresu (Local/Remote Address) a identifikátor procesu, ktorý toto spojenie používa.

```
vol.py -f zeus.vmem --profile=WinXPSP2x86 conscan
```

Príkaz *sockscan* prehľadáva všetky použité komunikačné sockety (koncový bod v počítačovej sieti), ktoré sa môžu viazať k TCP, UDP (alebo iným) protokolom. Môžeme vidieť (Obrázok 14.49), ktorý proces používa dané spojenie (PID), aký protokol je použitý (Protocol), dobu

```
$ vol.py -f zeus.vmem --profile=WinXPSP2x86 connections
Volatility Foundation Volatility Framework 2.6
Offset(V)  Local Address             Remote Address            Pid
---------- ------------------------ ------------------------ ---
sansforensics@siftworkstation -> ~/D/6
```

Obr. 14.47: Hľadanie aktívnych spojení.

```
$ vol.py -f zeus.vmem --profile=WinXPSP2x86 connscan
Volatility Foundation Volatility Framework 2.6
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------ ------------------------ ---
0x02214988 172.16.176.143:1054      193.104.41.75:80          856
0x06015ab0 0.0.0.0:1056             193.104.41.75:80          856
```

Obr. 14.48: Hľadanie reziduálnych spojení.

vzniku spojenia (Create Time) a iné.

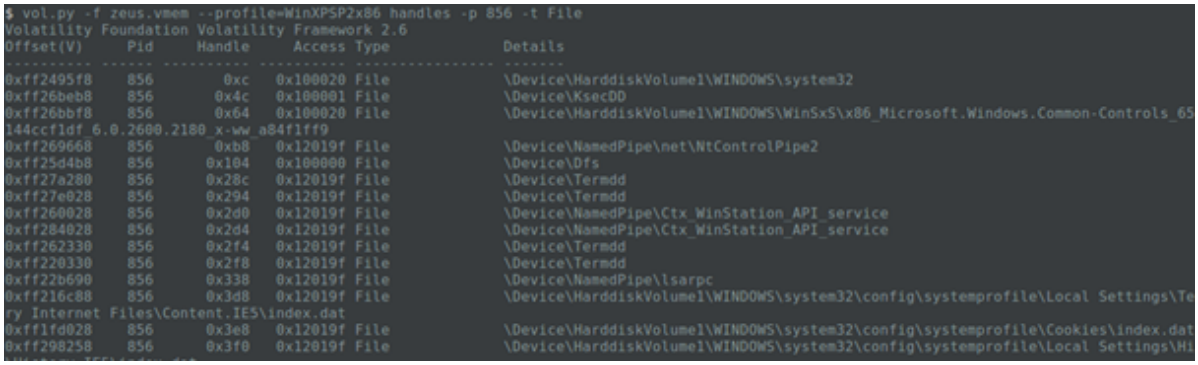
```
vol.py -f zeus.vmem --profile=WinXPSP2x86 sockscan
```

```
$ vol.py -f zeus.vmem --profile=WinXPSP2x86 sockscan
Volatility Foundation Volatility Framework 2.6
Offset(P)       PID   Port  Proto Protocol        Address         Create Time
---------- -------- ------ ------ -------------- --------------- -----------
0x007c0a20     1148   1900     17 UDP            172.16.176.143  2010-08-15 19:15:43 UTC+0000
0x01120c40        4    445     17 UDP            0.0.0.0         2010-08-11 06:06:17 UTC+0000
0x01131930     1088   1025     17 UDP            0.0.0.0         2010-08-11 06:06:38 UTC+0000
0x01134008        4      0     47 GRE            0.0.0.0         2010-08-11 06:08:00 UTC+0000
0x011568a8        4    138     17 UDP            172.16.176.143  2010-08-15 19:15:43 UTC+0000
0x0115f128      936    135      6 TCP            0.0.0.0         2010-08-11 06:06:24 UTC+0000
0x02daad28      216   1026      6 TCP            127.0.0.1       2010-08-11 06:06:39 UTC+0000
0x04863458        4    139      6 TCP            172.16.176.143  2010-08-15 19:15:43 UTC+0000
0x04864578     1028     68     17 UDP            172.16.176.143  2010-08-15 19:17:26 UTC+0000
0x04864a08        4    137     17 UDP            172.16.176.143  2010-08-15 19:15:43 UTC+0000
0x04a4be98        4   1033      6 TCP            0.0.0.0         2010-08-11 06:08:00 UTC+0000
0x04a51d28     1028   1058      6 TCP            0.0.0.0         2010-08-15 19:17:56 UTC+0000
0x04be7008        4    445      6 TCP            0.0.0.0         2010-08-11 06:06:17 UTC+0000
0x05dee200     1028    123     17 UDP            127.0.0.1       2010-08-15 19:15:43 UTC+0000
0x05e33d68     1148   1900     17 UDP            127.0.0.1       2010-08-15 19:15:43 UTC+0000
0x05f44008      688    500     17 UDP            0.0.0.0         2010-08-11 06:06:35 UTC+0000
0x05f48008     1028    123     17 UDP            127.0.0.1       2010-08-15 19:17:56 UTC+0000
0x06236e98     1028     68     17 UDP            172.16.176.143  2010-08-15 19:17:56 UTC+0000
0x06237b70      688      0    255 Reserved       0.0.0.0         2010-08-11 06:06:35 UTC+0000
0x06450478      856  29220      6 TCP            0.0.0.0         2010-08-15 19:17:27 UTC+0000
0x06496a20     1148   1900     17 UDP            127.0.0.1       2010-08-15 19:17:56 UTC+0000
0x069d5250      688   4500     17 UDP            0.0.0.0         2010-08-11 06:06:35 UTC+0000
```

Obr. 14.49: Prehľadávanie socketov.

Môžeme sa pozrieť s čím pracujú jednotlivé procesy pomocou príkazu *handles*. Keďže sa jedná o pomerne dlhý výstup, tak je dobré to zúžiť na konkrétny proces ("-p Číslo_procesu", napr. „-p 856“) a aj konkrétny typ objektu („-t Typ_procesu“, napr. „-t Port,File“), ktorý nás zaujíma. V tomto prípade (Obrázok 14.50) opäť vidíme posun v pamäti (Offset), aký proces používa konkrétny objekt (Pid) a v detailoch sa vieme dočítať viac informácií. Napríklad, kde sa daný súbor nachádzal na disku.

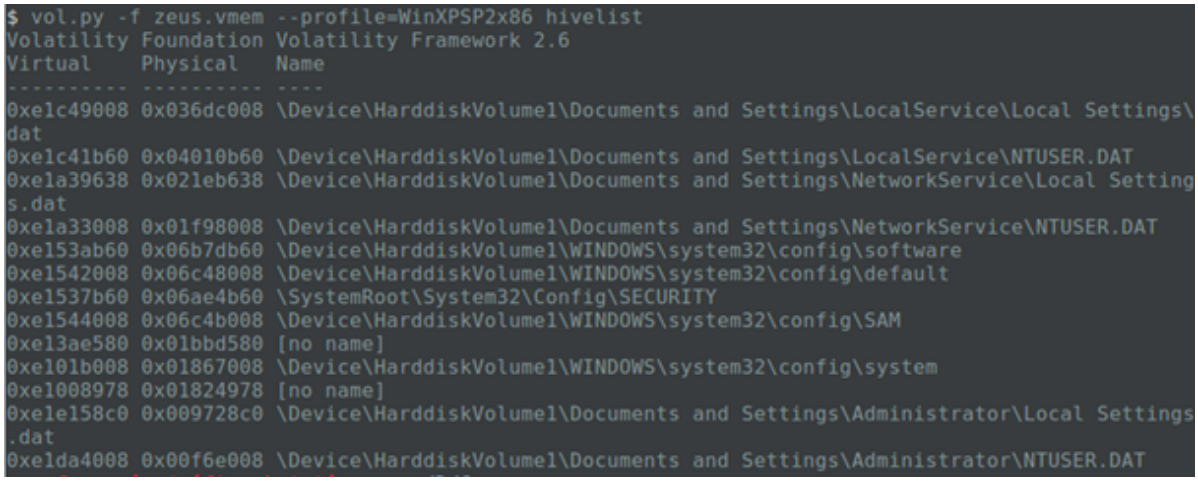
```
vol.py -f zeus.vmem --profile=WinXPSP2x86 handles -p 856 -t File
```



Obr. 14.50: Výpis súborov, s ktorými proces pracuje.

Je známe, že v OS Windows sa v operačnej pamäti nachádzajú aj registre. Pomocou príkazu *hivelist* sa k nim vieme dostať. Na obrázku 14.51 vidíme virtuálnu aj fyzickú adresu (prvé dva stĺpce), ktoré sú nasledované názvom registra.

```
vol.py -f zeus.vmem --profile=WinXPSP2x86 hivelist
```

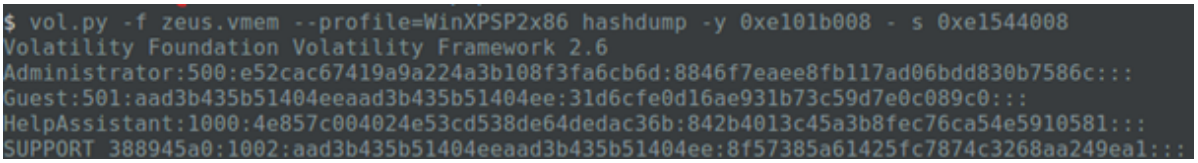


Obr. 14.51: Nájdene balíky registrov.

Ak vieme virtuálne adresy, tak máme viac možností, napríklad môžeme použiť príkaz *hashdump* (Obrázok 14.52), ktorý sa pokúsi nájsť všetky hodnoty vo forme hašov. Každým prepínačom v príkaze určujeme, o aký typ registra sa jedná (v tomto prípade -y reprezentuje register SYSTEM, -s register SAM). Následne vieme tieto hodnoty (hodnota „8846f7eaee8fb117ad06bdd830b7586c“ reprezentuje heslo účtu Administrator) vyskúšať prelomiť, napríklad pomocou stránky https://crackstation.net. Zistíme, že heslo administrátora bolo „password“.

```
vol.py -f zeus.vmem --profile=WinXPSP2x86 hashdump -y 0xe101b008
    - s 0xe1544008
```

Ak máme hlbšiu znalosť registrov a potrebujeme výpis len niekoľkých hodnôt, tak môžeme použiť príkaz *printkey* (Obrázok 14.53). Ak by sme potrebovali robiť hlbšiu analýzu registrov, tak sa odporúča exportovať registre do samostatného súboru (príkazom hivedump) a následne



Obr. 14.52: Výpis hodnôt, ktoré sú v tzv. „hash“ forme.

ich analyzovať v špecializovanom nástroji. Vidíme informácie o kľúčoch a ich hodnotách ako sú štandardne uložené v registroch operačného systému.

```
vol.py -f zeus.vmem printkey -K "Microsoft\backslash Windows NT\
    backslash CurrentVersion\backslash Winlogon"
```

Obr. 14.53: Vypísanie konkrétnej hodnoty z registrov.

Toto je len malá ukážka možností tohto nástroja. Samozrejmosťou sú exportovanie jednotlivých častí (napríklad procesov) pre ďalšiu analýzu, základná detekcie možných infiltrácií (*malfind*, *yara*), či dokonca k časti súborového systému, ktorý sa nachádza v operačnej pamäti (*mftparser*).

Literatúra

[1] A. Årnes. *Digital forensics*. John Wiley & Sons, 2017 (citované na stranách: 375, 380–382, 386, 390, 391, 393, 395–397, 440).

[2] N. Brownlee a E. Guttman. *Expectations for Computer Security Incident Response*. RFC 2350. RFC Editor, jún 1998. DOI: 10.17487/RFC2350. URL: https://www.ietf.org/rfc/rfc2350.txt (citované na strane 396).

[3] B. Carrier. *File system forensic analysis*. Addison-Wesley Professional, 2005 (citované na stranách: 398, 400, 408, 413, 417, 418, 420, 423, 425, 434, 436, 446).

[4] B. D. Carrier. „Volume analysis of disk spanning logical volumes“. Publik.: *Digital Investigation* 2.2 (jún 2005), s. 78–88. ISSN: 1742-2876. DOI: https://doi.org/10.1016/j.diin.2005.04.008. URL: http://www.sciencedirect.com/science/article/pii/S1742287605000368 (citované na strane 402).

[5] B. D. Carrier a E. Spafford. *Defining Event Reconstruction of Digital Crime Scenes*. 2004. URL: https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2004-37.pdf (cit. 14. 07. 2018) (citované na strane 377).

[6] Council of Europe. „Convention on Cybercrime (CETS N°.: 185)“. Publik.: *Chart of signatures and ratifications* (nov. 2001). URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 (citované na stranách: 391, 392).

[7] *dcfldd(1) - Linux man page*. 2006. URL: https://linux.die.net/man/1/dcfldd (cit. 03. 10. 2019) (citované na strane 407).

[8] *DCO and HPA*. 2013. URL: https://forensicswiki.xyz/wiki/index.php?title=DCO_and_HPA (cit. 10. 08. 2018) (citované na strane 419).

[9] A. Dewald a J. Plum. *APFS internals for forensic analysis*. Apr. 2018 (citované na stranách: 452, 453).

[10] A. Fortuna. *Volatility, my own cheatsheet (Part 3): Process Memory*. 2017. URL: https://www.andreafortuna.org/2017/07/10/volatility-my-own-cheatsheet-part-3-process-memory/ (cit. 12. 01. 2018) (citované na strane 461).

[11] C. P. Grobler a C. P. Louwrens. „Digital forensic readiness as a component of information security best practice“. Publik.: *IFIP International Information Security Conference*. Springer. 2007, s. 13–24 (citované na strane 393).

[12] GSMArena. *Counterclockwise: RAM capacity through the years*. 2018. URL: https://www.gsmarena.com/counterclockwise_ram_capacity_through_the_years-news-30756.php (cit. 05. 08. 2019) (citované na strane 388).

[13] Y. Gubanov a O. Afonin. „Recovering evidence from SSD drives in 2014: Understanding trim, garbage collection and exclusions“. Publik.: *Forensic Focus* 23 (sept. 2014) (citované na strane 401).

[14] Y. Gubanov a O. Afonin. „Why SSD drives destroy court evidence, and what can be done about it“. Publik.: *Forensic Focus* (2012) (citované na strane 401).

[15] *GUID Partition Table*. 2018. URL: https://en.wikipedia.org/wiki/GUID_Partition_Table (cit. 02. 08. 2018) (citované na strane 418).

[16] J. A. Halderman, S. D. Schoen, N. Heninger, W. Clarkson, W. Paul, J. A. Calandrino, A. J. Feldman, J. Appelbaum a E. W. Felten. „Lest We Remember: Cold-Boot Attacks on Encryption Keys“. Publik.: *Communications of the ACM* 52.5 (máj 2009), s. 91–98. ISSN: 0001-0782. DOI: 10.1145/1506409.1506429 (citované na strane 459).

[17] P. Henry. „Best practices in digital evidence collection“. Publik.: *SANS DFIR* 1 (2009) (citované na strane 398).

[18] W. J. Chisum a B. Turvey. „Evidence dynamics: Locard's exchange principle & crime reconstruction“. Publik.: *Journal of Behavioral Profiling* 1.1 (2000), s. 1–15 (citované na strane 380).

[19] *Inode pointer structure*. 2017. URL: https://en.wikipedia.org/wiki/Inode_pointer_structure (cit. 01. 10. 2018) (citované na strane 449).

[20] L. Johnson. *Computer incident response and forensics team management: Conducting a successful incident response*. Newnes, 2013 (citované na strane 377).

[21] G. Kessler. *GCK'S file signatures table*. 2020. URL: https://www.garykessler.net/library/file_sigs.html (cit. 30. 09. 2020) (citované na strane 389).

[22] G. C. Kessler. „An overview of steganography for the computer forensics examiner". Publik.: *Forensic Science Communications* 6.3 (jan. 2004), s. 1–27 (citované na strane 378).

[23] W. G. Kruse II a J. G. Heiser. *Computer forensics: incident response essentials*. Pearson Education, 2001 (citované na strane 382).

[24] S. Laliberte a A. Gupta. *The Role of Computer Forensics in Stopping Executive Fraud*. Okt. 2004 (citované na stranách: 381, 383).

[25] D. Lee. „Hash function vulnerability index and hash chain attacks". Publik.: *2007 3rd IEEE Workshop on Secure Network Protocols*. IEEE. 2007, s. 1–6 (citované na strane 385).

[26] M. Ligh, S. Adair, B. Hartstein a M. Richard. *Malware analyst's cookbook and DVD: tools and techniques for fighting malicious code*. Wiley Publishing, 2010. URL: https://github.com/mgoffin/malwarecookbook/blob/master/17/1/zeus.vmem.zip (citované na strane 464).

[27] M. H. Ligh, A. Case, J. Levy a A. Walters. *The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory*. John Wiley & Sons, 2014 (citované na stranách: 455, 456, 458, 463).

[28] X. Lin, X. Lin a Lagerstrom-Fife. *Introductory Computer Forensics*. Springer, 2018 (citované na stranách: 375, 405, 430, 431, 437, 439).

[29] C. Marcho. *Understanding Crash Dump Files*. 2008. URL: https://techcommunity.microsoft.com/t5/ask-the-performance-team/understanding-crash-dump-files/ba-p/372633 (cit. 19. 01. 2018) (citované na strane 462).

[30] R. McKemmish. *What is forensic computing?* Australian Institute of Criminology Canberra, 1999 (citované na strane 382).

[31] Microsoft. *[MS-XCA]: Xpress Compression Algorithm*. 2016. URL: https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-xca/a8b7cb0a-92a6-4187-a23b-5e14273b96f8 (cit. 19. 01. 2018) (citované na strane 462).

[32] Microsoft. *How to read the small memory dump file that is created by Windows if a crash occurs*. 2017. URL: https://support.microsoft.com/sk-sk/help/315263/how-to-read-the-small-memory-dump-file-that-is-created-by-windows-if-a (cit. 19. 01. 2018) (citované na strane 462).

[33] S. Mueller. *Upgrading and Repairing PCs: The ATA/IDE Interface*. 2013. URL: https://www.informit.com/articles/article.aspx?p=2028834&seqNum=2 (cit. 05. 12. 2018) (citované na strane 410).

[34] Národná rada Slovenskej republiky. *Zákon č. 69/2018 o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov*. 2018. URL: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/69/20190101 (citované na stranách: 391, 397).

[35] *NTFS File Types - NTFS.com*. 2018. URL: http://www.ntfs.com/ntfs-files-types.htm (cit. 03. 03. 2018) (citované na strane 440).

[36] G. Palmer a kol. „A road map for digital forensic research“. Publik.: *First digital forensic research workshop, Utica, New York*. 2001, s. 27–30 (citované na strane 377).

[37] J. Plum. *APFS filesystem format*. 2017. URL: https://blog.cugu.eu/post/apfs/ (cit. 10. 09. 2018) (citované na strane 452).

[38] *RAID*. 2019. URL: https://en.wikipedia.org/wiki/RAID (cit. 01. 10. 2019) (citované na strane 402).

[39] M. Reith, C. Carr a G. Gunsch. „An examination of digital forensic models“. Publik.: *International Journal of Digital Evidence* 1.3 (2002), s. 1–12 (citované na strane 383).

[40] F. Soviš. *Počítačová kriminalita a jej vyšetrovanie*. 2013. URL: https://www.csirt.gov.sk/doc/MFSRVzdelavanie/02Vzdelavanie2014/Prezentacie_veduci_zamestnanci_utvarov/PrezV_2014_02_Pocitacova_kriminalita.pdf (cit. 13. 07. 2018) (citované na stranách: 377, 379, 392).

[41] P. Stelfox. *Criminal investigation: An introduction to principles and practice*. Routledge, 2013 (citované na strane 377).

[42] S. J. Tan. *User Interface for Intel® SATA Motherboard Signal Quality Test (MSQT) Setup*. White Paper 323096. Intel, dec. 2009. URL: https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/sata-mqst-setup-paper.pdf (citované na strane 400).

[43] A. S. Tanenbaum a H. Bos. *Modern operating systems*. Pearson, 2015 (citované na strane 455).

[44] The Volatility Foundation. *Linux volatilityfoundation / volatility*. 2018. URL: https://github.com/volatilityfoundation/volatility/wiki/Linux (cit. 10. 01. 2018) (citované na strane 461).

[45] The Volatility Foundation. *Mac volatilityfoundation / volatility*. 2018. URL: https://github.com/volatilityfoundation/volatility/wiki/Mac#creating-a-profile (cit. 10. 01. 2018) (citované na strane 461).

[46] The Volatility Foundation. *Volatility Cheat Sheet*. 2014. URL: https://github.com/volatilityfoundation/volatility/raw/gh-pages/docs/VolatilityCheatSheet.pdf (cit. 12. 01. 2018) (citované na strane 461).

[47] C. Tilbury. *Memory Forensics Cheat Sheet v.2.0*. 2017. URL: https://digital-forensics.sans.org/media/volatility-memory-forensics-cheat-sheet.pdf (cit. 12. 01. 2018) (citované na strane 461).

[48] J. E. Tomyako. *Computers in Spaceflight: The NASA Experience*. 1987. URL: https://history.nasa.gov/computers/Ch2-5.html (cit. 03. 02. 2020) (citované na strane 387).

[49] *Volatility Usage volatilityfoundation / volatility*. 2017. URL: https://github.com/volatilityfoundation/volatility/wiki/Volatility-Usage (cit. 10. 01. 2018) (citované na strane 461).

[50] *Volatility Workbench – a GUI for the Volatility memory forensics*. 2017. URL: https://www.osforensics.com/tools/volatility-workbench.html#Overview (cit. 03. 03. 2017) (citované na strane 461).

[51] M. Y. C. Wei, L. M. Grupp, F. E. Spada a S. Swanson. „Reliably Erasing Data from Flash-Based Solid State Drives.“ Publik.: *FAST*. Zv. 11. 2011, s. 8–8 (citované na strane 401).

[52] *What are SCSI standards, interfaces, and connectors?* Indiana University. 2018. URL: https://kb.iu.edu/d/aiqw (cit. 10. 09. 2018) (citované na strane 400).

[53] Wikipedia. *Zeus (malware)*. 2016. URL: https://en.wikipedia.org/wiki/Zeus_(malware) (cit. 01. 02. 2018) (citované na strane 464).

[54] M. Willing. *Volatility Memory Forensics | Basic Usage for Malware Analysis*. 2011. URL: https://www.evild3ad.com/956/volatility-memory-forensics-basic-usage-for-malware-analysis/ (cit. 01. 02. 2018) (citované na strane 464).

Kapitola 15

Kybernetická bezpečnosť na úseku obrany štátu

Ján Hochmann

15.1 Úvod

Celkový trend vývoja bezpečnostnej situácie vo svete má zhoršujúci charakter. Vývoj svetovej politiky, bezpečnosti a ekonomiky v podmienkach ich mnohostrannosti a zložitosti nepriniesol do súčasnej doby žiadne jednoznačné pozitívne riešenia, práve naopak bezpečnostné situácia sa zhoršuje. V záujme obranných aktivít Európske únie (ďalej len „EÚ“), Organizácie severoatlantickej zmluvy (NATO) a ďalších nadnárodných organizácií (napr. Organizácia pre bezpečnosť a spoluprácu v Európe (OBSE), ktorá je najväčšou regionálnou bezpečnostnou organizáciou na svete dohliadajúcou nad svetovými konfliktami (ktorú v roku 2019 viedlo aj slovenské predsedníctvo), deklarovaných v strategických dokumentoch EÚ, je preto riešiť narastúce problémy so zabezpečeným dôležitých aktív proti zneužitiu alebo zničeniu a zabezpečiť tak podmienky pre zachovanie a rozvoj jednotného digitálneho trhu a bezpečnosti občanov, a to najmä chrániť kritické siete a informačné systémy a poskytovať kľúčové služby v oblasti kybernetickej obrany a ochrany. Z toho plynúce požiadavky na zabezpečenie objektov obrannej infraštruktúry v dôležitých oblastiach hospodárstva, kde obranná infraštruktúra predstavuje pozemky, stavby, budovy a zariadenia, telekomunikačné, energetické a dopravné systémy, informačné siete (ďalej len „objekty obrannej infraštruktúry“) a zásoby štátnych hmotných rezerv, ktoré slúžia v čase vojny alebo vojnového stavu na zabezpečenie obrany štátu[1], vrátane požiadaviek nahlasovania a riešenia kybernetických bezpečnostných incidentov, sú obsiahnuté v aktoch EÚ, medzinárodných zmluvách a dohovoroch, ako aj všeobecne záväzných právnych predpisoch na národnej úrovni.

Na úseku obrany štátu sa jedná najmä o sektory energetiku, dopravnú infraštruktúru a to cestnú dopravu, lodnú dopravu, leteckú dopravu a železničnú dopravu, obranu štátu, financie, elektronické komunikácie, informačné systémy a siete, priemysel, zdravotníctvo, vodné a potravinové zdroje a ďalšie čiastkové sektory dôležité pre obranu štátu, v ktorých je operačné riziko kľúčovou súčasťou prísnej regulácie a dohľadu nadnárodných organizácií, (napr.: Európsky systém finančného dohľadu (ESFS), Európske spoločenstvo pre atómovú energiu (Euroatom),

[1] § 26 zákona č. 319/2002 Z. z.

Európska agentúra pre bezpečnosť sietí a informácií (ENISA), ako aj ďalšie). Súčasťou zabezpečenia bezpečnosti prevádzky dôležitých objektov a prvkov (ďalej len „aktív“) sú aj postupy a bezpečnostné opatrenia vzťahujúce sa na všetky priestory, zariadenia, personál a operácie vrátane výroby, distribúcie, transportu, používania, skladovania a likvidácie nebezpečných zariadení, výrobkov a materiálov, rádiových a telekomunikačných systémov, sietí a počítačových systémov. Požiadavky a postupy aplikované na rôznych úrovniach v jednotlivých sektoroch verejnej správy a mimo nej, zahŕňajú aj zoznamy hrozieb a rizík, oznamovanie všetkých bezpečnostných incidentov, ich analýzu, návrhy bezpečnostných opatrení, dohľad a kontrolu. Prioritou EÚ je mať schopnosť autonómne zabezpečiť obranu a ochranu svojich aktív, a tak reagovať na zhoršujúcu sa bezpečnostnú situáciu vo svete.

15.2 Nadnárodný kontext a národné záujmy

Vzhľadom na to, že lokálne, resp. jednorazové zavedenie bezpečnostných opatrení samé osebe nepostačuje na zaistenie dlhodobo udržateľnej úrovne bezpečnostného systému EÚ, ktorý je postavený na bezpečnostných systémoch jednotlivých členských štátov, je potrebné udržateľnosť riešiť systematicky a zohľadňovať aj netechnické aspekty vplývajúce na bezpečnosť a obranu členských štátov až do úrovne jednotlivých organizácií, ich systémov, sietí, ľudských zdrojov a ich odborných spôsobilostí. Záujmom, ale aj povinnosťou každého členského štátu, nevynímajúc Slovenskej republiky, je preto vytvoriť jednotný rámec kybernetickej obrany nadväzujúci na bezpečnostné požiadavky EÚ a NATO v súlade s článkom 3 Washingtonskej zmluvy, stať sa ich plne integrovanou súčasťou, a tak sa podieľať na budovaní počiatočných európskych vojenských štruktúr. Na základe tohto smerovania, požiadavka na vytvorenie rámca riadenia kybernetickej bezpečnosti v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu bola zohľadnená aj v Akčnom pláne realizácie Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020 (uznesenie vlády č. 94/2016) a reflektuje na súčasné právne úpravy na národnej úrovni. Obsah tejto kapitoly je preto smerovaný najmä na rozpracovanie tých najdôležitejších otázok

a) inštitucionálneho riadenia kybernetickej bezpečnosti v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu,

b) zodpovednosti za riadenie kybernetickej bezpečnosti v čase mieru, núdzového a výnimočného stavu, prechodu do vojnového stavu a stavu vojny podľa ústavného zákona č. 227/2002 Z. z. o bezpečnosti štátu v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu a

c) zabezpečenia bezpečnostného dohľadu nad obrannou infraštruktúrou a dôležitými aktívami štátu, t. j. objektov osobitnej dôležitosti (ďalej len „OOD“), ďalších dôležitých objektov (ďalej len „ĎDO“) a prvkov kritickej informačnej infraštruktúry (ďalej len „prvkov KII“).

15.3 Legislatíva a strategické dokumenty

Právna úprava informačnej a kybernetickej bezpečnosti je v Slovenskej republike fragmentovaná medzi viaceré všeobecne záväzné právne predpisy. Pre účely dosiahnutia cieľa rozpracovaného v nasledujúcich častiach tejto kapitoly sa však jedná o predpisy zamerané, resp. aj dotýkajúce

sa **kybernetickej obrany**, ktoré vymedzujú kompetenčné rozloženie právomocí na úseku kybernetickej obrany. Sú to predovšetkým:

a) Ústava Slovenskej republiky (460/1992 Zb.)[2]

b) Ústavný zákon č. 227/2002 Z. z. o bezpečnosti štátu v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu[3]

c) Zákon č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy (Kompetenčný zákon)[4]

d) Zákon č. 319/2002 Z. z. o obrane Slovenskej republiky

e) Zákon č. 198/1994 Z. z. o Vojenskom spravodajstve

f) Zákon č. 321/2002 Z. z. o ozbrojených silách

Ďalšie súvisiace právne predpisy a dokumenty sú uvedené v prílohe na strane 488.

15.4 Definície a pojmy

Pre účel dodržania kompatibility kapitoly so súčasnými právnymi úpravami je v dokumente použitá odborná terminológia ustanovená v jednotlivých právnych predpisoch. Textácie definícií/pojmov s referenciami na ustanovenia zdrojových právnych predpisov sú uvedené vo výkladovom slovníku na strane 491.

15.5 Subjekty riadenia na úseku kybernetickej obrany štátu

Súčasný právny rámec riadenia bezpečnosti štátu vychádza z **ústavného zákona č. 227/2002 Z. z. o bezpečnosti štátu v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu**, podľa ktorého rozhodujúce právomoci v tejto oblasti majú ústavné orgány, ktorými sú prezident Slovenskej republiky (ďalej len „prezident“), Národná rada Slovenskej republiky (ďalej len „národná rada“) a Vláda Slovenskej republiky (ďalej len „vláda“).

15.5.1 Právomoci prezidenta

Prezident **vypovie vojnu** na základe rozhodnutia **„národnej rady“** len za podmienky, že Slovenská republika je napadnutá cudzou mocou, ktorá jej vypovedala vojnu alebo ktorá bez vypovedania vojny narušila jej bezpečnosť, alebo za podmienky, že vypovedaním vojny Slovenská republika plní záväzky vyplývajúce z členstva v organizácii vzájomnej kolektívnej bezpečnosti alebo z medzinárodnej zmluvy o spoločnej obrane proti napadnutiu, pričom vypovedanie vojny sa vzťahuje na celé územie Slovenskej republiky. V čase vojny možno v nevyhnutnom rozsahu a na nevyhnutný čas v závislosti od priebehu udalostí obmedziť základné práva a slobody a uložiť povinnosti na celom území Slovenskej republiky alebo na jej časti, a to najviac

[2] https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/1992/460/20210101
[3] https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2002/227/20201229
[4] https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2001/575/20201001

v rozsahu čl. 2 odseku 3, citovaného ústavného zákona. Prezident podľa odseku 4 má aj ďalšie právomoci.

Prezident môže **vyhlásiť vojnový stav** na návrh vlády, a to len za podmienky, že Slovenskej republike bezprostredne hrozí vypovedanie vojny alebo bezprostredne hrozí napadnutie cudzou mocou bez vypovedania vojny. Vyhlásenie vojnového stavu sa vzťahuje na celé územie Slovenskej republiky. V čase vojnového stavu možno v nevyhnutnom rozsahu a na nevyhnutný čas obmedziť základné práva a slobody a uložiť povinnosti v závislosti od priebehu udalostí na celom území Slovenskej republiky alebo na jej časti, a to najviac v rozsahu podľa článku 3 odseku 3 citovaného ústavného zákona. Prezident na návrh vlády má podľa odseku 4 aj ďalšie právomoci.

Prezident môže **vyhlásiť výnimočný stav** na návrh vlády, a to len za podmienky, že došlo alebo bezprostredne hrozí, že dôjde k teroristickému útoku, k rozsiahlym pouličným nepokojom spojeným s útokmi na orgány verejnej moci, drancovaním obchodov a skladov alebo s inými hromadnými útokmi na majetok alebo dôjde k inému hromadnému násilnému protiprávnemu konaniu, ktoré svojím rozsahom alebo následkami podstatne ohrozuje alebo narušuje verejný poriadok a bezpečnosť štátu, ak ho nemožno odvrátiť činnosťou orgánov verejnej moci a ak je znemožnené účinné použitie zákonných prostriedkov. Výnimočný stav možno vyhlásiť len na postihnutom alebo na bezprostredne ohrozenom území, ktorým môže byť aj celé územie Slovenskej republiky. Výnimočný stav možno vyhlásiť v nevyhnutnom rozsahu a na nevyhnutný čas, najdlhšie na 60 dní. Ak vzniknú nové okolnosti bezprostredne súvisiace s dôvodmi, pre ktoré bol výnimočný stav vyhlásený, možno výnimočný stav predĺžiť v nevyhnutnom rozsahu a na nevyhnutný čas, najviac o ďalších 30 dní. Výnimočný stav nemožno vyhlásiť na potlačenie štrajku, o ktorom rozhodol príslušný odborový orgán, alebo výluky, o ktorej rozhodol zamestnávateľ v súlade s predpismi o kolektívnom vyjednávaní, ani na znemožnenie alebo na rozpustenie verejného zhromaždenia občanov v súlade s predpismi upravujúcimi právo na zhromažďovanie, ak na ňom alebo v súvislosti s ním nedôjde ku konaniu, ktoré spĺňa podmienky podľa prvej vety.

V čase výnimočného stavu možno v nevyhnutnom rozsahu a na nevyhnutný čas podľa závažnosti ohrozenia obmedziť základné práva a slobody a uložiť povinnosti na postihnutom alebo na bezprostredne ohrozenom území, ktorým môže byť aj celé územie Slovenskej republiky, a to najviac v rozsahu článku 4 odseku 4 citovaného ústavného zákona. Prezident podľa odseku 5 má aj ďalšie právomoci.

15.5.2 Právomoc a zodpovednosť vlády

Vláda môže **vyhlásiť núdzový stav**, a to len za podmienky, že došlo alebo bezprostredne hrozí, že dôjde k ohrozeniu života a zdravia osôb, a to aj v príčinnej súvislosti so vznikom pandémie, k ohrozeniu životného prostredia alebo k ohrozeniu značných majetkových hodnôt v dôsledku živelnej pohromy, katastrofy, priemyselnej, dopravnej alebo inej prevádzkovej havárie; núdzový stav možno vyhlásiť len na postihnutom alebo na bezprostredne ohrozenom území, ktorým môže byť aj celé územie Slovenskej republiky. Núdzový stav možno vyhlásiť v nevyhnutnom rozsahu a na nevyhnutný čas, najdlhšie na 90 dní. Núdzový stav vyhlásený z dôvodu ohrozenia života a zdravia osôb v príčinnej súvislosti so vznikom pandémie možno v nevyhnutnom rozsahu a na nevyhnutný čas predĺžiť najviac o ďalších 40 dní, a to aj opakovane. S predĺžením núdzového stavu musí vysloviť **súhlas národná rada**, a to do 20 dní od prvého

dňa predĺženého núdzového stavu. Ak národná rada nevysloví súhlas, predĺžený núdzový stav zanikne dňom neschválenia návrhu vlády na vyslovenie súhlasu s predĺžením núdzového stavu, inak uplynutím lehoty podľa tretej vety na vyslovenie takéhoto súhlasu. **Súhlas národnej rady** je potrebný aj v prípade opätovného vyhlásenia núdzového stavu, ak od skončenia predchádzajúceho núdzového stavu vyhláseného z tých istých dôvodov neuplynulo 90 dní. V čase núdzového stavu, okrem núdzového stavu vyhláseného z dôvodu ohrozenia života a zdravia osôb v príčinnej súvislosti so vznikom pandémie, možno v nevyhnutnom rozsahu a na nevyhnutný čas podľa závažnosti ohrozenia obmedziť základné práva a slobody a uložiť povinnosti na postihnutom alebo na bezprostredne ohrozenom území, ktorým môže byť aj celé územie Slovenskej republiky, a to najviac v rozsahu článku 5 odseku 3 citovaného ústavného zákona.

15.5.3 Právomoci ústredných orgánov štátnej správy a ich organizačných zložiek

Ďalšie subjekty v hierarchickej štruktúre riadenia štátu na úseku obrany v SR sú Ministerstvo obrany Slovenskej republiky (ďalej len „MO SR“), Vojenské spravodajstvo, Parlamentná rada Slovenskej republiky (ďalej len „Parlamentná rada“), Bezpečnostná rada Slovenskej republiky (ďalej len „Bezpečnostná rada“), Bezpečnostná rada kraja, Bezpečnostná rada okresu, Centrum pre kybernetickú obranu Slovenskej republiky pri Ministerstve obrany SR (ďalej len „CKO“).

Podľa citovaného zákona za obranu a bezpečnosť štátu zodpovedá vláda, ktorá riadi činnosti orgánov verejnej správy a celý proces obranného plánovania, schvaľuje koncepcie, medzirezortné programy a iné strategické dokumenty, predkladá národnej rade legislatívne návrhy zákonov, prijíma opatrenia na predchádzanie rizikám a ohrozeniam, rozhoduje o zásadných opatreniach prípravy na obranu štátu, o určení objektov pre ich zaradenie do kategórie objektov osobitnej dôležitosti (ďalej len „OOD“) a ďalších dôležitých objektov (ďalej len „ĎDO“), ktoré jej predkladá na schválenie MO SR. Vláda ďalej schvaľuje zaradenie prvkov kritickej infraštruktúry (ďalej len „KII“) do zoznamu prvkov kritickej infraštruktúry, ktoré jej predkladá Ministerstvo vnútra Slovenskej republiky (ďalej len „MV SR“). Pri bezprostredných ohrozeniach štátu definovaných v citovanom ústavnom zákone vláda vyhlasuje núdzový stav na ohrozenom území a navrhuje prezidentovi vyhlásenie výnimočného stavu.

Za ďalšie činnosti na úseku obrany štátu zodpovedajú, v rozsahu ustanovenom osobitnými právnymi predpismi, **ústredné orgány štátnej správy** a ostatné ústredné orgány štátnej správy, **krajské a okresné úrady, obce a vyššie územné celky**. Súčasnú štruktúru riadenia uvedenú v hierarchickej postupnosti dopĺňajú poradné a koordinačné orgány, a to na úrovni parlamentu **Parlamentná rada**, na úrovni vlády **Bezpečnostná rada**, na úrovni krajov a okresov sú to **Bezpečnostná rada kraja a Bezpečnostná rada okresu**. Rozsah pôsobnosti, týchto poradných, koordinačných, a v závislosti od stavu situácie aj výkonných orgánov, je ustanovený v ústavnom zákone č. 227/2002 Z. z., ďalších všeobecne záväzných právnych predpisoch a príslušných štatútoch a rokovacích poriadkoch týchto orgánov. V čase prechodu do vojnového stavu a vojny sa na zabezpečenie riadenia obrany štátu vytvára **hlavné miesto riadenia obrany štátu** pre prezidenta, predsedu vlády/predsedu Bezpečnostnej rady a jej členov.

15.5.4 Pôsobnosť ústredných orgánov štátnej správy na úseku obrany štátu

Vymedzenie rozsahu pôsobnosti na úseku obrany štátu v zmysle definície podľa výkladového slovníka na strane 502 je určené viacerými všeobecne záväznými právnymi predpismi, medzinárodnými zmluvami a dohovormi.

Podľa ustanovenia **§ 18 ods. 1 zákona č. 575/2001 Z. z.** o organizácii činnosti vlády a organizácii ústrednej štátnej správy (Kompetenčný zákon) je MO SR v oblasti kybernetickej bezpečnosti ústredným orgánom štátnej správy pre riadenie a kontrolu obrany Slovenskej republiky, koordináciu činností a kontrolu orgánov štátnej správy, orgánov územnej samosprávy a iných právnických osôb pri príprave na obranu Slovenskej republiky, koordináciu obranného plánovania a vojenské spravodajstvo.

V zmysle ustanovenia **§ 35 ods. 3** citovaného zákona, ministerstvá a ostatné ústredné orgány štátnej správy v rozsahu vymedzenej pôsobnosti zodpovedajú aj za úlohy obrany, kybernetickú bezpečnosť a vytváranie podmienok na realizáciu požiadaviek zabezpečovania príprav na obranu, ochranu a kybernetickú bezpečnosť. Práva a povinnosti pre jednotlivé ústredné orgány v ich pôsobnosti sú ustanovené v osobitných predpisoch. Pre MO SR je rozsah pôsobnosti v tejto oblasti vymedzený osobitnými právnymi predpismi, najmä ustanovením **§ 2 ods. 2 zákona č. 319/2002 Z. z.** o obrane Slovenskej republiky, podľa ktorého sa obrana štátu pred kybernetickým napadnutím zabezpečuje aj v kybernetickom priestore zadefinovanom/vymedzenom osobitným právnym predpisom[5] prostredníctvom opatrení zameraných na

- riešenie závažných kybernetických bezpečnostných incidentov[6],
- obranu objektov OOD a ĎDO[7],
- obranu prvkov KI[8].

V zmysle § 7 písm. f) citovaného zákona to znamená, že MO SR na úseku obrany štátu koordinuje a kontroluje v rozsahu svojej pôsobnosti výkon štátnej správy pri príprave a zabezpečovaní obrany štátu uskutočňovaný ministerstvami, ostatnými ústrednými orgánmi štátnej správy, ďalšími orgánmi štátnej správy s celoštátnou pôsobnosťou a orgánmi miestnej štátnej správy. Ďalej MO SR koordinuje a kontroluje v rozsahu svojej pôsobnosti aj plnenie úloh obrany štátu samosprávnymi subjektmi, a to obcami a vyššími územnými celkami, riadi, koordinuje a kontroluje výkon štátnej správy uskutočňovaný obvodnými úradmi v sídlach krajov a vojenskými obvodmi.

15.5.5 Úlohy vojenského spravodajstva na úseku obrany štátu

Činnosti na úseku obrany štátu v kybernetickom priestore (ďalej len „kybernetická obrana“) MO SR vykonáva prostredníctvom Vojenského spravodajstva. Rozsah pôsobnosti Vojenského spravodajstva v oblasti kybernetickej bezpečnosti je upravený osobitným právnym predpisom, v ustanovení § 2 ods. 1 **zákona č. 198/1994 Z. z.**, podľa ktorého Vojenské spravodajstvo

[5] § 3 písm. b) zákona č. 69/2018 Z. z.
[6] § 27 ods. 10 zákona č. 69/2018 Z. z. (poznámka: závažné kybernetické incidenty III. stupňa)
[7] § 27 zákona č. 319/2002 Z. z
[8] § 2 písm. a) zákona č. 45/2011 Z. z.; § 2 ods. 2 zákona č. 319/2002 Z.z.

v rozsahu svojej pôsobnosti získava, sústreďuje a vyhodnocuje informácie, vrátane informácií odvodených od signálov v elektromagnetickom spektre, dôležité pre zabezpečenie obrany a obranyschopnosti Slovenskej republiky na území Slovenskej republiky a v zahraničí zamerané na činnosti ohrozujúce suverenitu, ústavné zriadenie, zvrchovanosť, územnú celistvosť a obranyschopnosť Slovenskej republiky, kybernetický terorizmus a aktivity a ohrozenia v kybernetickom priestore.

Vojenské spravodajstvo v oblasti kybernetickej bezpečnosti pri plnení svojich úloh vystupuje k národným a zahraničným orgánom obdobného zamerania ako národná autorita.

Kybernetickú obranu Vojenské spravodajstvo vykonáva prostredníctvom CKO, ktoré je jeho osobitnou organizačnou zložkou. Rozsah činností v kybernetickej obrane a bezpečnosti je upravený v § 4a ods. 1 citovaného zákona, kde CKO v rámci svojej kompetencie

a) získava, sústreďuje, analyzuje a vyhodnocuje informácie dôležité na zabezpečenie kybernetickej obrany, informuje dotknuté subjekty a navrhuje vhodné opatrenia,

b) je oprávnené požadovať od vlastníka alebo prevádzkovateľa OOD, ĎDO a prvkov KI súčinnosť a informácie v rozsahu potrebnom na účely zabezpečenia kybernetickej obrany,

c) na účely zabezpečenia plnenia úloh podľa uvedeného zákona má CKO priamy prístup v elektronickej podobe, v reálnom čase a v plnom rozsahu k jednotnému informačnému systému kybernetickej bezpečnosti[9],

d) a podľa § 14b, ak to nie je v rozpore s osobitným predpisom[10], a zabránenie aktivitám a ohrozeniam podľa § 2 ods. 1 je Vojenské spravodajstvo prostredníctvom CKO oprávnené získavať, sústreďovať a vyhodnocovať informácie odvodené zo signálov v elektromagnetickom spektre. Vojenské spravodajstvo pri plnení týchto úloh vystupuje ako národná autorita k domácim a zahraničným orgánom obdobného zamerania a pôsobnosti.

15.6 Kybernetická obrana a ochrana dôležitých objektov a prvkov KI

Za obranu štátu pred kybernetickým napadnutím v priestore štátu vymedzenom osobitnými právnymi predpismi zodpovedá MO SR. Svoju činnosť vykonáva prostredníctvom Vojenského spravodajstva a jeho osobitnej organizačnej zložky – CKO, prostredníctvom opatrení zameraných najmä na:

Riešenie závažných kybernetických incidentov
pričom závažnosť kybernetického incidentu sa posudzuje v zmysle **zákona č. 69/2018 Z. z.** zákona o kybernetickej bezpečnosti a o zmene a doplnení niektorých predpisov (ďalej len „ZoKB“) na základe identifikačných kritérií ustanovených **vyhláškou NBÚ č. 165/2018 Z. z.**, ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických

[9] § 8 zákona č.69/2018 Z. z.

[10] Zákon č.166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním) v znení neskorších predpisov.

bezpečnostných incidentov. Kybernetický bezpečnostný incident je považovaný za závažný incident, ak spĺňa aspoň jedno identifikačné kritérium pre jednu z troch kategórií uvedených v citovanej vyhláške. Pôsobnosť Vojenského spravodajstva pri riešení závažného kybernetického incidentu vymedzuje ustanovenie § 27 ods. 10 ZoKB, a to len so zameraním sa na závažné kybernetické bezpečnostné incidenty kategórie tretieho (III.) stupňa alebo iné skutočnosti, ktoré nasvedčujú, že závažný kybernetický bezpečnostný incident môže byť kybernetickým terorizmom, pričom na NBÚ sa v tejto oblasti voči Vojenskému spravodajstvu vzťahuje informačná povinnosť. Podľa citovanej vyhlášky, incidenty kategórie III. stupňa spadajúce do pôsobnosti Vojenského spravodajstva sú incidenty, pri ktorých počet používateľov elektronickej služby zasiahne minimálne 100 tisíc používateľov alebo obmedzí prevádzku základnej služby na viac ako 500 používateľských hodín alebo incident spôsobil úplnú nedostupnosť základnej služby alebo spôsobil hospodársku stratu viac ako 1 milión eur alebo spôsobil obete na životoch 500 mŕtvych alebo 5 000 zranených alebo narušil verejný poriadok vo významnej časti štátu, pričom významnou časťou štátu sa rozumie priestor vymedzený v čl. 4 ods. 1 a čl. 5 ods. 1 zákona č. 227/2002 Z. z. Prevádzkovateľ základnej služby a poskytovateľ digitálnej služby, ktorí hlásia tento závažný kybernetický bezpečnostný incident, sú na účely zabezpečenia kybernetickej obrany povinní poskytnúť Vojenskému spravodajstvu informácie v potrebnom rozsahu. O postupe riešenia takéhoto závažného kybernetického bezpečnostného incidentu úrad (NBÚ) informuje predsedu Bezpečnostnej rady.

Kybernetickú obranu objektov osobitnej dôležitosti a ďalších dôležitých objektov pričom do kategórie OOD a ĎDO sú zaradené strategické objekty obrannej infraštruktúry, ktorých poškodenie alebo zničenie obmedzí zabezpečenie obrany štátu a objekty obrannej infraštruktúry, ktorých poškodenie alebo zničenie obmedzí činnosť ozbrojených síl alebo chod hospodárstva Slovenskej republiky. Obrana týchto objektov je v súčasnej dobe legislatívne riešená ustanovením § 27 zákona č. 319/2002 Z. z. o obrane Slovenskej republiky v znení neskorších predpisov, podľa ktorého za obranu OOD a ĎDO zodpovedá MO SR. Návrhy správcov a prevádzkovateľov (vlastníkov) týchto objektov, ktoré spĺňajú kritériá na ich zaradenie do zoznamu alebo vyradenie zo zoznamu objektov, posudzuje MO SR a predkladá ich na schválenie vláde. Návrh na zaradenie objektov do zoznamu pre rok 2018 predložilo MO SR Vláde na určenie na základe kritérií vydaných všeobecne záväzným právnym predpisom, vyhláškou MO SR č. 353/2004 Z. z., ktorou sa ustanovili kritériá na zaradenie objektov obrannej infraštruktúry do kategórie OOD a do kategórie ĎDO. Aktualizáciu zoznamu objektov vykonáva MO SR každoročne do 31. augusta vždy pre nasledujúci kalendárny rok. Spôsob obrany a ochrany objektov zaradených do uvedených kategórií spresňuje metodické usmernenie vydané MO SR v roku 2013. Zoznam objektov je utajovanou skutočnosťou podľa zákona č. 215/2002 Z. z.

Kybernetickú obranu prvkov kritickej infraštruktúry pričom prvkom kritickej infraštruktúry a prvkom európskej kritickej infraštruktúry sa podľa **zákona č. 45/2011 Z. z.** rozumie najmä inžinierska stavba, služba vo verejnom záujme a informačný systém v sektore kritickej infraštruktúry, ktorých narušenie alebo zničenie by malo podľa sektorových kritérií a prierezových kritérií závažné nepriaznivé dôsledky na uskutočňovanie hospodárskej a sociálnej funkcie štátu, a tým na kvalitu života obyvateľov z hľadiska ich života, zdravia, bezpečnosti, majetku, ako aj životného prostredia. V súčasnej dobe je obrana prvkov kritickej infraštruktúry legislatívne rie-

šená v súlade s ustanovením § 2 ods. 2 zákona č. 319/2002 Z. z. o obrane Slovenskej republiky v znení neskorších predpisov. Sektory kritickej infraštruktúry sú určené zákonom č. 45/2011 Z. z., pričom posudzovanie týchto prvkov a ich zaradenie do zoznamu prvkov kritickej infraštruktúry sa vykonáva na základe splnenia sektorových a prierezových kritérií a európskych sektorových a európskych prierezových kritérií. Predkladanie návrhov na zaradenie/vyradenie prvku do/z registra prvkov KI je záležitosťou MV SR, ktoré ich aj so svojim stanoviskom predkladá na určenie Vláde. Kritériá a zoznam prvkov KI sú obsiahnuté/určené v Návrhu sektorových a prierezových kritérií na určenie prvkov kritickej infraštruktúry a zoznamu prvkov kritickej infraštruktúry a ich zaradenie do sektorov kritickej infraštruktúry. Register/zoznam prvkov kritickej infraštruktúry je citlivou informáciu neverejného charakteru a utajovanou skutočnosťou podľa zákona č. 215/2004 Z. z.

15.6.1 Kybernetická ochrana

Za **ochranu** objektov dôležitých objektov považovanú za základný stupeň ochrany, určených vládou, zodpovedajú v rozsahu svojej pôsobnosti ministerstvá, ostatné ústredné orgány štátnej správy, ďalšie orgány štátnej správy s celoštátnou pôsobnosťou a subjekty hospodárskej mobilizácie určené osobitným právnym predpisom.[11]

Ochranu prvku kritickej infraštruktúry pred narušením, zničením alebo zneužitím, ktorá je považovaná za základný stupeň ochrany, zabezpečuje jeho prevádzkovateľ v zmysle ustanovenia § 9 zákona č. 45/2011 Z. z.

Zoznamy prvkov sú predkladané Vláde na určenie každoročne sa môžu v jednotlivých rokoch meniť v počtoch a rozsahom ich určenia.

15.7 Bezpečnostné opatrenia na úseku kybernetickej obrany štátu

Cieľom vytvorenia celoúnijného rámca a návrhu súboru bezpečnostných opatrení je zvýšiť kybernetickú bezpečnosť produktov a služieb v digitálnom svete, ako aj realizáciu koncepcie rýchlej a koordinovanej reakcie na závažné kybernetické incidenty, kybernetický terorizmus a krízy veľkého rozsahu. Sektory relevantné z hľadiska kybernetickej bezpečnosti (napr. energetika, obrana, doprava, financie, ...) a čiastkové oblasti sa v súčasnosti vzájomne nepodporujú dostatočne. Synergie medzi sektormi obrannej a civilnej (ochrannej) kybernetickej bezpečnosti sa v európskom priestore a na národných úrovniach takisto nevyužívajú v plnej miere[12]. Požiadavky na implementáciu bezpečnostných opatrení adekvátnej úrovne, ktoré vychádzajú z kategorizácie závažných kybernetických bezpečnostných incidentov a ich riešenia na národnej úrovni, sú vo všeobecnej rovine predmetom ZoKB a jeho vykonávacieho predpisu, vyhlášky Národného bezpečnostného úradu č. 165/2018 Z. z. ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov. Citovaný zákon však deklaruje, že v prípade

[11] § 4 zákona č. 179/2011 Z. z. o hospodárskej mobilizácii a o zmene a doplnení zákona č. 387/2002 Z. z. o riadení štátu v krízových situáciách mimo času vojny a vojnového stavu v znení neskorších predpisov.

[12] Technická správa Spoločného výskumného centra: Výsledky mapovania; Závery Rady o spoločnom oznámení Európskeho parlamentu a Rade: Odolnosť, odrádzanie a obrana: budovanie silnej kybernetickej bezpečnosti pre EÚ.

požiadaviek na zavedenie vyššej úrovne bezpečnostných opatrení ako sám predpisuje, sa majú **prednostne uplatňovať predpisy s požadovanou vyššou úrovňou bezpečnosti**. Tým zároveň ZoKB a jeho vykonávací právny predpis reflektujú na potrebné zvýšené požiadavky predpisované nadnárodnými právnymi aktmi EÚ a NATO a osobitnou legislatívou platnou na národnej úrovni v špecifických oblastiach národného hospodárstva, medzi ktoré sa radí práve obrana štátu.

Komplexnejšia právna úprava bezpečnostných požiadaviek a opatrení bola do značnej miery aj predmetom zákona č. 275/2006 Z. z. a jeho vykonávacieho predpisu, výnosu MF SR č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy, ktorý nahradil **zákon č. 95/2019 Z. z.** o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov, pričom na informačné systémy verejnej správy, ktoré sa týkajú zabezpečenia obrany Slovenskej republiky, bezpečnosti Slovenskej republiky a utajovaných skutočností sa tieto všeobecne záväzné právne predpisy nevzťahujú. Aktíva, ktorých správcami a prevádzkovateľmi sú rôzne právnické osoby a fyzické osoby, sú sumarizované v neverejných zoznamoch, ktoré posudzujú MO SR a MV SR, a ktoré po ich predložení vláde, ich táto schvaľuje na časové obdobie nasledujúceho kalendárneho roka. Predpokladá sa, že každoročným procesom identifikácie a schvaľovaním aktív je zabezpečená ich spoľahlivá aktualizácia platná v časovom rozmedzí 12 mesiacov. Zo zavedeného procesu zároveň vyplýva, že treba zvážiť aj ošetrenie prípadu vzniknutého nového aktíva bezprostredne po termíne určenia aktív na zaradenie do zoznamu vládou, resp. aj zánik aktíva po bezprostrednej aktualizácii zoznamu z dôvodu možného vzniku nesúladu zoznamov s reálnym stavom počas doby 12 mesiacov. Z hľadiska bezpečnostnej klasifikácie informácií a kategorizácie informačných systémov a sietí je podľa vyhlášky[13] rozdelenie informačných systémov a sietí riešené do troch kategórií I., II. a III. stupňa podľa klasifikačných kritérií. Uvedený vykonávací predpis neuvádza explicitne klasifikačnú schému s priradením konkrétnych bezpečnostných opatrení/súborov v ustanovených oblastiach, ale implicitne rozdeľuje informačné systémy a siete na dve kategórie, a to na tie na ktoré sa vzťahuje a na ostatné, čím vytvára priestor pre možné/žiaduce zabezpečenie kompatibility špecifického prostredia.

Z obsahu všeobecne záväzných právnych predpisov na národnej úrovni vyplýva, že súčasný právny rámec (t.j. štandardy, pravidlá a predpísané postupy pre informačnú/kybernetickú bezpečnosť a pod.) umožňuje dotknutým subjektom značnú voľnosť pri zavádzaní konkrétnejších bezpečnostných opatrení. Tieto opatrenia, pokiaľ nie sú už určené inými právnymi predpismi, si majú povinné osoby individuálne navrhnúť v rozsahu svojej pôsobnosti s možnosťou ich adaptácie na konkrétne prostredie a aktíva, avšak podľa možnosti pri dodržaní už predpísaného základného rámca. Prevádzkovatelia, ktorí už majú vykonanú klasifikáciu svojich informačných aktív podľa inej štandardizačnej metódy, sú povinní vykonať mapovanie na klasifikáciu v klasifikačnej schéme v súlade so štruktúrou klasifikácie podľa prílohy č. 2 k vyhláške[9], ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení. Výsledkom kategorizácie aktív má byť návrh bezpečnostných opatrení zoskupených do súborov konkrétnych bezpečnostných opatrení v jednotlivých oblastiach, ktoré majú dotknuté subjekty na základe posúdenia z analýzy rizík povinnosť navrhnúť a následne implementovať vo svojom prostredí.

[13] Vyhláška Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.

15.8 Zhrnutie

Cieľom tejto kapitoly bolo podať študentom stručný prehľad o legislatívnom rámci a z toho vyplývajúcich úloh a činností týkajúcich sa rozsahu pôsobnosti kompetentných orgánov a ďalších subjektov na úseku obrany štátu. Súčasťou je aj kladenie dôrazu na vytvorenie komunikačného prostredia a pravidiel komunikácie medzi dotknutými subjektmi a to najmä za účelom odhaľovania zraniteľnosti, účinného riešenia závažných kybernetických bezpečnostných incidentov, krízových stavov a bezpečnostného dohľadu nad obrannou infraštruktúrou štátu, ako aj s tým súvisiacej výskumnej a vzdelávacej činnosti, výmeny informácií a poradenstva.

Dôležitosť postupov pri obrane a ochrane aktív štátu, ktoré je potrebné vzhľadom na veľké zmeny a dynamiku prostredia neustále sledovať a priebežne aktualizovať, vychádza z rastúceho napätia vo svete a nárastu technologických, personálnych a finančných požiadaviek na vývoj a zavádzanie nových IKT technológií do kybernetickej bezpečnosti a dynamicky sa meniacich sa spôsobov kybernetického boja. Postupy a dohľad nad obrannou infraštruktúrou štátu tvorenou dôležitými aktívami štátu vychádza z potreby riešenia kybernetickej obrany obranných a kritických infraštruktúr, dynamického vývoja hrozieb na informačné a komunikačné technológie (IKT) a aktuálneho postavenia MO SR, jeho organizačných zložiek a ďalších subjektov. Dôvodmi sú celkovo sa zhoršujúca bezpečnostná situácia v Európe a vo svete, zvyšujúce sa nároky EÚ na obranu, rastúce požiadavky vyplývajúce z členstva v NATO na obranné plánovanie a budovanie vlastných obranných spôsobilostí v súlade s článkom 3 Washingtonskej zmluvy, požiadavky legislatívy EÚ a legislatívy na národnej úrovni, požiadavky zo strany národných a medzinárodných prevádzkovateľov kritických informačných infraštruktúr, nárast cielených kybernetických útokov na vládne inštitúcie štátu a rozmáhajúci sa kybernetický terorizmus. V zmysle medzinárodného práva jednotlivé štáty nesú primárnu zodpovednosť za dianie v ich suverénnom teritóriu nielen z pohľadu štátnych inštitúcií, ale aj jednotlivcov. V prípade, ak suverénny štát nezabraní neštátnemu aktérovi pokračovať v kybernetickom útoku voči druhému štátu, druhý – napadnutý štát má právo zasiahnuť voči tomuto neštátnemu aktérovi aj na pôde štátu, z ktorého je takýto útok vykonávaný. V zmysle platnej právnej úpravy v Slovenskej republike za obranu dôležitých aktív v kybernetickom priestore na úseku obrany štátu a elimináciu nežiaducich aktivít, vrátane zodpovednosti s obranou súvisiacej koordinačnej a kontrolnej činnosti a zavádzania bezpečnostných opatrení zodpovedá v zmysle platnej legislatívy, MO SR a jeho organizačné zložky.

Príloha: právne základy

Právny základ a súvisiace dokumenty

a) Zákon č. 45/2011 Z. z. o kritickej infraštruktúre

b) Zákon č. 387/2002 Z. z. o riadení štátu v krízových situáciách mimo času vojny a vojnového stavu

c) Zákon č. 110/2004 Z. z. o fungovaní Bezpečnostnej rady Slovenskej republiky v čase mieru

d) Zákon č. 179/2011 Z. z. o hospodárskej mobilizácii a o zmene a doplnení zákona číslo 387/2002 Z. z. o riadení štátu v krízových situáciách mimo času vojny a vojnového stavu v znení neskorších predpisov

e) Zákon č. 95/2019/ Z. z. o informačných technológiách vo verejnej správe a zmene a doplnení niektorých zákonov

f) Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov

g) Vyhláška NBÚ č. 165/2018 Z. z. ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov

h) Vyhláška MBÚ č. 362/2018 Z. z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení

i) Vyhláška Ministerstva dopravy, pôšt a telekomunikácií Slovenskej republiky č. 194/2003 Z. z., ktorou sa ustanovujú podrobnosti o organizácii telekomunikačných služieb na obdobie krízovej situácie

j) Štatút Bezpečnostnej rady Slovenskej republiky (uznesenie vlády SR č. 1177/2004, zmeny a doplnenia uznesenie č. 702/2015)

k) Koncepcia kritickej infraštruktúry v Slovenskej republike a spôsobu jej ochrany a obrany, (uznesenie vlády SR č. 120/2007)

l) Smernica Rady 2008/114/ES o identifikácii a označovaní európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu, (Ú. v. EÚ, L 345, 23.12.2008)

m) Národný program pre ochranu a obranu kritickej infraštruktúry v Slovenskej republike, (uznesenie vlády SR č. 185/2008)

n) Smernica Európskeho parlamentu a rady (EÚ) 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii, (Ú. v. L 194, 19.7.2016)

o) Návrh sektorových a prierezových kritérií na určenie prvkov kritickej infraštruktúry a zoznam prvkov kritickej infraštruktúry a ich zaradenia do sektorov kritickej infraštruktúry, (uznesenie vlády SR č. ... /2018)

p) Návrh aktualizácie zaradenia stavieb a budov do kategórie objektov osobitnej dôležitosti alebo do kategórie ďalších dôležitých objektov na obranu štátu, spôsobu ich ochrany a obrany, (uznesenie vlády SR č. 453/2017)

Ďalšie súvisiace právne predpisy

- Zákon č. 211/2016 Z. z. o slobodnom prístupe k informáciám
- Zákon č. 2015/2004 Z. z. o ochrane utajovaných skutočnosti a o zmene a doplnení niektorých zákonov
- Zákon č. 300/2005 Z. z. Trestný zákon
- Zákon č. 351/2011 Z. z. o elektronických komunikáciách
- Zákon č. 46/1993 Z. z. o slovenskej informačnej službe v znení zákona č. 151/2010 Z. z.
- Zákon č. 398/2015 Z. z. o európskom ochrannom príkaze v trestných veciach a o zmene a doplnení niektorých zákonov, zákon č. 91/2016 Z. z. o trestnoprávnej zodpovednosti právnických osôb a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
- Nariadenie EP a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (Ú. V. EÚ L257,28. 8. 2014),
- Zákon č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním) v znení neskorších predpisov,
- Zákon č. 556/1992 Zb. Zákon Národnej rady Slovenskej republiky o Národnej banke Slovenska,
- 73/1998 Z. z. o služobnom pomere príslušníkov Policajného zboru, Slovenskej informačnej službe, Zboru väzenskej a justičnej stráže Slovenskej republiky a Železničnej polície v znení neskorších predpisov.
- Zákon č. 281/2015 Z. z. o štátnej službe profesionálnych vojakov v znení neskorších predpisov.
- Zákon č. 55/2017 Z. z. štátnej službe a o zmene a doplnení niektorých predpisov,
- Zákon č. 583/2008 Z. z. o prevencii kriminality a inej protispoločenskej činnosti a o zmene a doplnení niektorých zákonov
- Zákon č. 307/2014 Z. z. o niektorých opatreniach súvisiacich s oznamovaním protispoločenskej činnosti a o zmene a doplnení niektorých zákonov
- Nariadenie EP a Rady (EÚ) č. 2016/679 z 27. apríla o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane osobných údajov) (Ú. V. EÚ L 119/89, 4. 5. 2016),
- STN ISO/IEC 27002 Informačné technológie. Bezpečnostné metódy. Pravidlá dobrej praxe riadenia informačnej bezpečnosti (ISO/IRC 27002:2013)
- Vykonávacie nariadenie Komisie (EÚ) 2018/151 z 30. januára 2018, ktorým sa ustanovujú pravidlá uplatňovania smernice Európskeho parlamentu a rady (EÚ) 2016/1148, pokiaľ ide o bližšiu špecifikáciu prvkov, ktoré musia poskytovatelia digitálnych služieb zohľadňovať pri riadení rizík v oblasti bezpečnosti sietí a informačných systémov, a posudzovanie parametrov na posudzovanie toho, či má incident závažný vplyv (Ú. V. EÚ L 26, 31. 1. 2018).

Kapitola 16

Stručný výkladový slovník

Daniel Olejár a kol.

16.1 Úvod

Táto kapitola obsahuje stručný výkladový slovník termínov kybernetickej a informačnej bezpečnosti. Základom je výkladový slovník informačnej bezpečnosti vytvorený pre MF SR v roku 2012, ktorý je priebežne rozširovaný o ďalšie pojmy z noriem, európskych dokumentov a slovenských zákonov a vykonávacích predpisov. Stručný výkladový slovník obsahuje približne 250 najdôležitejších pojmov kybernetickej a informačnej bezpečnosti a má slúžiť čitateľom tejto knihy na rýchlu orientáciu v preberanej problematike.

Heslá slovníka sú organizované nasledovne: slovenský termín, [jeho anglický ekvivalent], výklad pojmu. Na pojmy, ktoré používajú vo výklade a nachádzajú sa v slovníku je v texte hesla uvedený hypertextový odkaz. Viacslovné pojmy sú usporiadané podľa kľúčového slova. Pri skratkách vo všeobecnosti a pri anglických skratkách, ktoré nemajú slovenský ekvivalent zvlášť, uvádzame odkaz na heslo vykladajúce pojem označený skratkou. Pojmy, ktoré nemajú slovenský ekvivalent uvádzame pod pôvodným anglickým názvom. Keďže väčšina pojmov informačnej bezpečnosti vznikla v anglicky hovoriacom prostredí, pre uľahčenie vyhľadávania v slovníku je k slovníku je pripojený anglicko-slovenský register.

16.2 Výkladová časť

A

aktívum [asset] čokoľvek, čo má pre organizáciu hodnotu. Aktíva sú hmotné (zariadenia, infraštruktúra, personál) nehmotné (informácie, know-how, dobré meno). Môžu sa stať objektom hrozby (s. 497) alebo cieľom útoku (s. 508) a vyžadujú si ochranu.

analýza rizík [risk analysis] proces identifikácie rizík (s. 505) a stanovenia ich hodnôt (s. 505)

anonymita [anonymity] 1. bezpečnostná služba umožňujúca používateľovi systému využívať zdroje systému bez prezradenia používateľovej identity (s. 497) 2. bezpečnostná požiadavka (s. 492) na riešenie, systém alebo nejakú službu, aby pri interakcii používateľa so systémom (používaní riešenia, služby) nebola prezradená používateľova identita

antivírový softvér, antivírus [antivirus software] program, ktorý podľa toho ako je

nakonfigurovaný monitoruje počítač alebo počítačovú sieť, aby odhalil škodlivý kód a zabránil bezpečnostným incidentom spôsobeným škodlivým kódom a pomáhal ich riešiť

atribút [attribute] vlastnosť, charakteristická črta alebo prívlastok entity (s. 496), ktorý môže kvantitatívne alebo kvalitatívne rozlíšiť človek, technické zariadenie alebo program

audit [audit] formálne preskúmanie, preskúšanie alebo verifikácia (s. 509) skutočného stavu systému alebo jeho definovanej časti na zhodu alebo súlad so stanovenými očakávaniami

autentifikácia/autentizácia [authentication] potvrdenie deklarovanej identity (s. 497) nejakej entity (s. 496)

autentickosť [autenticity] vlastnosť, ktorá znamená, že deklarovaná identita entity je pravdivá

autorita, atribútová [attribute authority] dôveryhodná tretia strana, ktorá overuje atribúty entity a v prípade úspešného overenia (a prípadne splnenia ďalších podmienok) vydáva o tom potvrdenie v podobe atribútového certifikátu, ktorý viaže overené atribúty entity s jej identitou

autorita, certifikačná [certification authority] pozri certifikačná autorita (s. 493)

autorita časových pečiatok [timestamping authority] dôveryhodná tretia strana, ktorá poskytuje služby časových pečiatok (vydávanie, overovanie)

autorizácia [authorization] udelenie oprávnení nejakej entite (s. 496) na prístup k zdrojom systému/organizácie a/alebo na ich využívanie

B

bezpečnostná architektúra [security architecture] súbor princípov, ktoré popisujú

(a) bezpečnostné služby, ktoré od systému požadujú jeho používatelia
(b) komponenty systému, ktoré majú implementovať dané služby
(c) výkonostné úrovne/parametre jednotlivých komponentov potrebné na to, aby sa dokázali vyporiadať s predpokladanými hrozbami (s. 497).

bezpečnostná funkcia [security function] implementačne nezávislý spôsob realizácie bezpečnostnej požiadavky (s. 492)

bezpečnostná politika(inštitúcie) [security policy] 1.formálny dokument schválený vedením inštitúcie, ktorým sa podrobnejšie rozpracovávajú bezpečnostné ciele inštitúcie, upresňuje úroveň bezpečnostných požiadaviek (s. 492), stanovuje zodpovednosť za informačnú bezpečnosť v inštitúcii a rámcovo definujú spôsoby na dosiahnutie stanovených cieľov 2. dokument, ktorý podrobnejšie rozpracúva bezpečnostnú politiku organizácie pre nejakú oblasť (napr. riadenie prístupu), alebo systém.

bezpečnostná požiadavka [security requirement] špecifikácia ohraničení na usporiadanie aktíva (s. 491), spôsob jeho používania alebo na činnosť inštitúcie, ktorých cieľom je eliminácia alebo zníženie pravdepodobnosti rizika (s. 505) spojeného s používaním aktíva, alebo činnosťou inštitúcie,

bezpečnostná záruka [security assurance] miera naplnenia bezpečnostnej požiadavky (s. 492) odvodená od spôsobu (bezpečnostných opatrení (s. 492)), akým bola bezpečnostná požiadavka realizovaná

bezpečnostné opatrenie [security measure/control] technické, organizačné, právne alebo iné riešenie, ktoré úplne alebo čiastočne odstraňuje zraniteľnosť (s. 510) aktíva, a/alebo znižuje pravdepodobnosť naplnenia

hrozby (s. 497) a/alebo v prípade jej naplnenia znižuje jej dopad na aktívum a organizáciu, ktorá ho vlastní. Bezpečnostné opatrenie je realizáciou jednej alebo viacerých bezpečnostných funkcií.

bezpečnostné povedomie [awareness] poznanie potreby ochrany informácie a IKT ako aj povinnosti osobne sa na nej podieľať

bezpečnostné prostredie [security environment] súbor externých entít (s. 496), procedúr, pravidiel a podmienok, ktoré majú vplyv na bezpečný vývoj, prevádzku, činnosť a údržbu systému

bezpečnostné smernice [security directives] sú podrobnejším opisom jednotlivých bezpečnostných opatrení (s. 492) a spravidla pozostávajú z opisu technických, organizačných, právnych, personálnych a iných riešení.

bezpečnostný incident [security incident] pozri incident (s. 497)

bezpečnostný mechanizmus [security mechanism] konkrétna implementácia bezpečnostnej funkcie (s. 492)

bezpečnostný projekt [security project] komplexné posúdenie bezpečnostných potrieb/požiadaviek na systém a návrh spôsobu, ako im efektívne vyhovieť. Výstup bezpečnostného projektu pozostáva z bezpečnostného zámeru (s. 493), analýzy rizík (s. 491) a bezpečnostných smerníc. (s. 493)

bezpečnostný zámer [security target] formálny dokument schválený vedením inštitúcie, ktorým vedenie inštitúcie deklaruje základné ciele inštitúcie v oblasti informačnej bezpečnosti (s. 493)informačnej bezpečnosti

bezpečnosť, informačná [information security] 1. ideálny stav systému, kedy všetko funguje v súlade s očakávaniami (bezpečnostnou politikou) 2. multiodborová disciplína, ktorá sa zaoberá hrozbami (s. 497) voči systémom/aktívam (s. 491) a metódami, ako aktíva pred hrozbami chrániť, 3. činnosti zamerané na dosiahnutie ideálneho stavu systému.

bezpečnosť pomocou utajovania [security by obscurity] snaha udržať alebo zvýšiť bezpečenosť systému utajením návrhu alebo konštrukcie bezpečnostného mechanizmu. V kryptológii sa tento prístup považuje za prekonaný.

biometrická autentifikácia [biometric authentication] overenie deklarovanej identity (s. 497) osoby na základe jej biometrických údajov (s. 493)

biometrické charakteristiky [biometric characteristics] parametre odvodené od fyziologických vlastností človeka

biometrické údaje [biometric data] údaje (s. 508) získané zanamenávaním alebo meraním →biometrických charakteristík nejakej osoby

biometrický [biometric] týkajúci sa špecifických fyziologických alebo behaviorálnych charakteristík (atribútov) predstavujúcich identitu (s. 497) určitej osoby

C

CA [CA] pozri certifikačná autorita (s. 493)

certifikačná autorita [certification authority] dôveryhodná tretia osoba, ktorá najmä vydáva certifikáty verejných kľúčov (s. 494), poskytuje informácie o ich platnosti, ruší predčasne ich platnosť a poskytuje aj iné certifikačné služby.

certifikačná autorita, koreňová [root certification authority, R-CA] v hierarchicky usporiadanej PKI najvyššie postavená CA, ktorá spravuje (vydáva, ruší a poskytuje informácie o platnosti) certifikáty verejných kľúčov (s. 494) hierarchicky nižšie postavených CA

certifikačná cesta [certification path] je postupnosť certifikátov (verejných kľúčov)

(s. 494) $C_1, C_2, \ldots, C_n$ taká, že držiteľ certifikátu (s. 495) C_i je vydavateľom certifikátu (s. 509) C_{i+1}, pričom C_1 je cerifikát verejného kľúča známej (napr. koreňovej) CA (s. 493) a C_n je certifikát, ktorého platnosť je potrebné overiť

certifikačná služba [certification service] vydávanie certifikátov, zrušovanie platnosti certifikátov, poskytovanie zoznamu zrušených certifikátov (s. 510), potvrdzovanie existencie a platnosti certifikátov, vyhľadávanie a poskytovanie vydaných certifikátov, vydávanie časových pečiatok (s. 495), dlhobobá archivácia podpísaných elektronických dokumentov a i.

certifikát [certificate] 1. dokument, ktorý potvrdzuje pravdivosť, pravosť alebo kvalitu niečoho alebo vlastníctvo niečoho, 2. dokument vydaný nezávislou oprávnenou autoritou deklarujúci, že posudzovaný system (zariadenie alebo výrobok) spĺňa funkcionálne, kvalitatívne, bezpečnostné a iné požiadavky definované v certifikačných kritériách 3.digitálny certifikát

certifikát verejného kľúča [public key certificate] dokument, ktorým vydavateľ (CA) potvrdzuje identitu držiteľa daného certifikátu a spája ho s verejným kľúčom uvedeným v certifikáte, čím umožňuje použiť verejný kľúč z certifikátu na overenie toho, či digitálny/elektronický podpis vytvoril držiteľ certifikátu. Okrem verejného kľúča certifikát verejného kľúča obsahuje aj ďalšie údaje potrebné na overenie platnosti certifikátu a digitálneho/elektronického podpisu. Certifikát verejného kľúča je podpísaný digitálnym/elektronickým podpisom vydavateľa certifikátu. Pozri X-509 certifikát verejného kľúča (s. 510)

certifikát, atribútový [attribute certificate] digitálny certifikát (s. 494), ktorý spája množinu popisných údajových položiek odlišných od verejného kľúča (s. 499) buď priamo s menom nejakého subjektu, alebo s certifikátom verejného kľúča. (s. 494) Atribútový certifikát digitálne podpisuje a vydáva atribútová autorita.

certifikát, digitálny [digital certificate] certifikát verejného kľúča (s. 494) alebo atribútový certifikát (s. 494)

certifikát, koreňový [root certificate] certifikát verejného kľúča (s. 494) koreňovej certifikačnej authority (s. 493), ktorý si koreňová certifikačná autorita sama vydala na svoj verejný kľúč (s. 499)verejný kľúč a podpísala súkromným kľúčom (s. 499) tvoriacim pár k verejnému kľúču, uvedenému v danom certifikáte.

certifikát, zrušenie [revocation of certificate] úkon, ktorým na podnet držiteľa certifikátu (s. 495) alebo inej, zákonom oprávnenej osoby CA (s. 493) predčasne ukončí platnosť certifikátu, ktorý vydala a o ktorého zrušenie bola požiadaná

cieľ opatrení [control objective] výrok popisujúci, čo sa má dosiahnuť prostredníctvom zavedenia opatrenia

citlivá informácia [sensitive information] 1. informácia, ktorej odhalenie, zmena, zničenie alebo zneprístupnenie môže mať negatívny dopad na jej vlastníka alebo používateľa, 2. informácia, ktorá je za citlivú prehlásená zákonom alebo vnútornými predpismi organizácie.

citlivá ale neklasifikovaná informácia [sensitive but unclassified information] informácia, ktorá nie je označená ako klasifikovaná (v SR utajované skutočnosti), ale nakladanie s ktorou je upravené legislatívou alebo vnútornými predpismi organizácie.

CRL pozri zoznam zrušených certifikátov (s. 510)

Č

časová pečiatka [timestamp] potvrdenie vydané dôveryhodnou treťou stranou, že dokument pre ktorý sa časová pečiatka vydáva, existoval pred časovým okamihom zachyteným v časovej pečiatke. Časová pečiatka má podobu hašovacej hodnotyhašovacej hodnoty daného dokumentu, zreťazeného s časovým údajom (doplneným autoritou časových pečiatok) podpísanej digitálnym (s. 503)/elektronickým (s. 503) podpisom autority časových pečiatok (s. 492).

D

deklasifikovať informáciu [declassify] rozhodnutie oprávnenej autority o zrušení pôvodnej klasifikácie informácie. Po tomto rozhodnutí sa informácia stáva neklasifikovanou, alebo môže byť klasifikovaná znova (prehodnotenie pôvodnej klasifikácie)

Deň Jedna [Day One] deň, kedy je zverejnená záplata na odhalenú zraniteľnosť (s. 510) systému alebo aplikácie

Deň Nula [Day Zero] deň, keď sa odhalí nová zraniteľnosť (s. 510) systému alebo aplikácie

dešifrovať [decipher] transformovať šifrový text (s. 508) na pôvodný otvorený text (s. 508). Na dešifrovanie sa používa dešifrovacia transformácia (s. 508) a v prípade použitia symetrických šifier (s. 507) tajný kľúč (s. 499), v prípade asymetrických šifier (s. 507) súkromný kľúč (s. 499) adresáta

digitálny odtlačok (textu) [digital fingerprint] kontrolný súčet textu (s. 499)

distribúcia kľúčov [key distribution] metódy zaistenia toho, aby oprávnené osoby (a len oni) poznali tajné kľúče (s. 499) symetrického kryptosystému alebo verejné kľúče (s. 499) partnerov pre komunikáciu pomocou asymetrického kryptosystému ešte pred začiatkom komunikácie.

distribuovaný útok typu denial of servis [distributed denial of servis attack, DDoS] útok (s. 508) typu denial of servis, vedený z viacerých počítačov na cieľový systém, so zámerom spôsobiť jeho preťaženie a zamedziť mu poskytovanie služieb

dosledovateľnosť [accountability] bezpečnostná požiadavka (s. 492) (na systém), aby bolo možné stanoviť, kto je zodpovedný za bezpečnostne relevantné aktivity v systéme

dostupnosť [availability] požiadavka, aby zdroje systému boli k dispozícii oprávnenej osobe 1. vždy keď o to požiada, 2. do času t od okamihu, keď o to požiada, 3. s pravdepodobnosťou meranou podielom doby, keď sú požadované zdroje k dispozícii ku celkovej dobe (napr. 24 x 7 znamená, že systém je dostupný nepretržite 24 hodín denne a 7 dní v týždni)

dôvera [trust] 1. pocit istoty (často nepodložený), že (a) systém nezlyhá (b) že systém robí len to, čo má robiť a nevykonáva žiadne nežiadúce činnosti 2. vo všeobecnosti, ak entita A dôveruje entite B, znamená, že entita A predpokladá, že sa entita B bude správať presne tak, ako entita A očakáva.

dôvernosť [confidentiality] 1. bezpečnostná požiadavka (s. 492), ktorej naplnenie znamená, že sa informáciu obsiahnutú v správe (dokumente) nedozvedia nepovolané osoby 2. druhý najnižší stupeň klasifikačnej schémy utajovaných skutočností

dôveryhodná (overená) výpočtová báza [trusted computing base] bezpečnostné jadro systému predstavované súborom bezpečnostných mechanizmov (s. 493) systému (hardvérových, softvérových a firmvérových) ktorých kombinácia je zodpovedná za presadzovanie bezpečnostnej politiky. (s. 492)

držiteľ certifikátu [certificate holder] v prípade digitálneho certifikátu (s. 494) podľa štandardu X-509 (s. 510) osoba, ktorej meno

alebo pseudonym je uvedené v položke Subject

dvojfaktorová autentifikácia [two-factor autentication] autentifikácia (s. 492) entity na základe dvoch nezávislých metód overenia jej proklamovanej identity (s. 497)

E

entita [entity] akýkoľvek objekt (človek, zviera, vec, myšlienka, abstraktný objekt), ktorý je jedinečný a zhodný len so sebou samým (t.j. niečím sa odlišuje od podobných objektov). Entita sa vyznačuje množinou →atribútov, ktoré tvoria jej →identitu.

efektivita [efficiency] vzťah medzi dosiahnutými výsledkami a vynaloženým úsilím (vynaloženými zdrojmi)

externý kontext [external context] vonkajšie prostredie, v ktorom sa organizácia snaží dosiahnuť svoje ciele

F

fyzická bezpečnosť [physical security] fyzické prostriedky na ochranu systému pred krádežou, zneužitím, náhodným poškodením, technickými poruchami a prírodnými vplyvmi.

G

generátor kľúčov [key generator] generátor náhodných čísel alebo generátor pseudonáhodných (s. 496) čísel ktoré sú buď priamo používané ako kryptografické kľúče (s. 498), alebo sa z nich vytvárajú kryptografické kľúče

generátor náhodných čísel [random numbers generator] technický alebo prírodný systém, ktorý na základe náhodných procesov prebiehajúcich v systéme alebo jeho okolí mení svoj stav, pričom stav systému je možné vyjadriť číslom a budúci stav systému nie je predpovedateľný na základe znalosti predchádzajúcich stavov

generátor pseudonáhodných čísel [pseudorandom numbers generator] systém deterministicky generujúci postupnosť čísel, ktorá nie je pomocou štatistických testov odlíšiteľná od náhodnej postupnosti a pre ktorú je ťažké vypočítať z predchádzajúcich hodnôt nasledujúce hodnoty. Počiatočná hodnota (stav) generátora pseudonáhodných čísel sa nazýva inicializačný vektor (s. 498)

generovanie kľúčov [key generation] 1. metódy a algoritmy na vytváranie kryptografických kľúčov (s. 498) 2. použitie metód a algoritmov na vytváranie kryptografických kľúčov

granularita [granularity] 1. relatívna miera jemnosti nastavenia mechanizmu na riadenie prístupu (s. 505) 2. veľkosť najmenšej jednotky informácie, ktorú možno individuálne chrániť v dôveryhodnom systéme 3. miera podrobnosti

H

hacker [hacker] človek hľadajúci zraniteľnosti systémov (s. 510) s cieľom využiť ich na prienik do systémov. Hacker sa neusiluje ani o zisk, ani o poškodenie systémov.

hašovacia funkcia [hash function] zobrazenie, ktoré textu ľubovoľnej konečnej dĺžky priradí reťazec pevnej dĺžky. Pozri kryptograficky silná hašovacia funkcia (s. 496)

hašovacia funkcia, kryptograficky silná [cryptographic hash function] hašovacia funkcia, pre ktorú je výpočtovo veľmi ťažko zvládnuteľné

(a) pre danú hašovaciu hodnotu nájsť/zostrojiť taký vstup (dokument, súbor), ktorého hašovacia hodnota nadobúda danú hodnotu,
(b) nájsť dva rôzne vstupy, ktorých hašovacie hodnoty sú zhodné.

hašovacia hodnota [hash value, hash] výsledok výpočtu hašovacej funkcie (s. 496)

heslo [password] tajný reťazec znakov známy len určitej entite (s. 496) (a overovateľovi identity (s. 497)), ktorý sa používa na autentifikáciu (s. 492) danej entity

I

identifikácia [identification] deklarácia identity (s. 497) nejakej entity (s. 496). (V praxi napr. prihlásenie sa do systému menom.)

identifikátor [identifier] 1. informačný alebo materiálny objekt na základe ktorého je možné jednoznačne určiť buď identitu (s. 497) entity, alebo samotnú entitu (s. 496) 2. umelá identita entity, ktorá sláži na jej jednoznačnú identifikáciu. Identita človeka je meno, priezvisko, dátum narodenia, adresa bydliska, identifikátor je napr. občiansky preukaz, pas, rodné číslo a pod.

identita [identity] množina atribútov (s. 492) nejakej entity, ktorá ju jednoznačne odlišuje od iných entít podobného druhu v nejakej oblasti aplikovateľnosti identity (s. 502).

incident [incident] incident [incident] udalosť alebo situácia, ktorá spôsobí alebo môže spôsobiť nežiadúce prerušenie činnosti, stratu, núdzový stav alebo krízu v nejakej organizácii alebo v systéme.

informácia [information] základný pojem s rozličnou interpretáciou v rôznych oblastiach. V informatike informácia predstavuje opis nejakej skutočnosti (reálnej alebo fiktívnej) zaznamenaný v podobe údajov (s. 508). Informácia predstavuje obsah údajov a údaje sú formou zápisu informácie.

hrozba [threat] čokoľvek, čo je potenciálne schopné priamo alebo nepriamo spôsobiť škodu na systéme, alebo informáciách ktoré sa v ňom spracovávajú

hierarchická PKI [hierarchic PKI] PKI (s. 503) s architektúrou hviezdy, alebo koreňového stromu, na vrchole ktorej stojí koreňová CA (s. 493), ktorá vydáva certifikáty verejných kľúčov (s. 494) hierarchicky podriadeným CA. Tieto vydávajú certifikáty verejných kľúčov koncovým používateľom, alebo predstavujú koreňové autority nižšej úrovne pre časti PKI.

informácia, klasifikácia [information classification] pozri klasifikácia údajov (s. 498)

informačná a komunikačná infraštruktúra[information and communication infrastructure] pozri infraštruktúra, informačná (s. 498)

informačné a komunikačné technológie, IKT [information and communication technology, ICT] technológie na prenos a spracovanie informácie, ktoré vznikli spojením počítačov, telekomunikačných sietí a masovokomunikačných prostriedkov, využívajúce digitálne kódovanie informácie a spoločné komunikačné kanály (s. 498) pre prenos údajov.

informačný systém [information system] technické zariadenie, aplikácia, služba alebo iný prvok, ktorý spracováva informáciu

infraštruktúra [infrastructure] z hľadiska organizácie je infraštruktúrou všetko to, čo sa priamo nepodieľa na plnení poslania organizácie, vrátane toho, čo organizácia nevlastní, ale čo však pre plnenie svojho poslania organizácia nevyhnutne potrebuje.

infraštruktúra, kritická [critical infrastructure] infraštruktúra, ktorej narušenie, zneprístupnenie alebo znefunkčnenie môže spôsobiť stratu schopnosti organizácie plniť

svoje poslanie, spôsobiť jej finančnú stratu, ktorú nedokáže kompenzovať alebo spôsobí ohrozenie zdravia a života ľudí.

infraštruktúra, informačná [information infrastructure] infraštruktúra, ktorá slúži na získavanie, prenos, spracovávanie a uchovávanie informácií.

infraštruktúra verejného kľúča [public key infrastructure, PKI] súbor hardvérových a softvérových prostriedkov, politík, procedúr a ľudí potrebných na zaistenie manažmentu certifikátov verejných kľúčov a poskytovanie iných certifikačných služieb (s. 494) certifikačných služieb.

inicializačný vektor [initialization vector, seed] počiatočná hodnota (stav) generátora pseudonáhodných čísel (s. 496), z ktorej je odvodená postupnosť pseudonáhodných čísel (s. 504)

integrita [integrity] 1. základná bezpečnostná požiadavka (s. 492) na údaje, ktorej naplnenie znamená, že údaje nie je možné zmeniť bez toho, aby to ich vlastník alebo adresát nemohol zistiť. 2. v širšom zmysle je integrita bezpečnostná požiadavka na vylúčenie neoprávnených zmien v systémoch; t.j. zmien hardvéru, programového vybavenia alebo údajov.

J

jediné odhlásenie [single sign-off] korektné ukončenie viacerých činností (prebiehajúcich aj na viacerých systémoch) pomocou jediného odhlásenia

jediné prihlásenie [single sign-on] metóda umožňujúca riadenie prístupu (s. 505) na viaceré rôzne systémy pomocou prihlásenia sa na jediný systém

jednorazové heslo [one time password] heslo (s. 497) na jedno použitie, ktoré sa nedá použiť opakovane

K

kanál, komunikačný [communication channel] 1. fyzické médium (kovový vodič, optické vlákno, priestor pre šírenie signálov a pod.) ktoré je schopné sprostredkovať šírenie signálov, prenášajúcich informáciu 2. logické spojenie medzi účastníkmi komunikácie, ktoré môže byť vytvorené *ad hoc* len pre konkrétnu komunikáciu a môže využívať rôzne druhy fyzických médií

kanál, skrytý [covert channel] metóda prenosu informácie (s. 497) pomocou vedľajšieho (skrytého) efektu nejakej udalosti alebo činnosti nejakého mechanizmu pôvodne určeného na iný účel.

klasifikácia údajov [data classification] (z hľadiska bezpečnosti) kategorizácia údajov, posúdenie potrieb ich ochrany údajov z hľadiska požiadaviek na zaistenie dostupnosti (s. 495), dôvernosti (s. 495), integrity (s. 498), autentickosti (s. 492) prípadne iných bezpečnostných požiadaviek (s. 492) na ochranu informácie, ktorú údaje obsahujú a ich následné zaradenie do klasifikačnej kategórie (triedy) zodpovedajúcej týmto potrebám.

klasifikačná schéma [classification scheme] zvyčajne systém hierarchicky usporiadaných tried, spolu s pravidlami, umožňujúcimi zaradiť údaje do práve jednej z tried a bezpečnostnými požiadavkami (s. 492) pre jednotlivé triedy

klasifikovaná informácia [classified information] 1. (všeob.) informácia zaradená do niektorej z klasifikačných tried 2. (SR) informácia patriaca medzi utajované skutočnosti

kľúč, kryptografický [cryptographic key] parameter kryptografických algoritmov, ktorého úlohou je zvýšiť počet transformácií,

ktoré tieto algoritmy realizujú na takú úroveň, aby protivník nemohol použiť útok úplným preberaním všetkých možností. (Sila kryptografického algoritmu však nezávisí len od kryptografického kľúča, ale aj od odolnosti transformácií, ktoré realizuje voči kryptoanalýze.)

kľúč na šifrovanie kľúčov [key encryption key] kľúč určený na šifrovanie (s. 507)/dešifrovanie kryptografických kľúčov (s. 498) na ochranu ich dôvernosti (s. 495) počas ich prenosu alebo uchovávania

kľúč, súkromný [private key] jeden z dvojice kryptografických kľúčov (s. 498) asymetrického šifrovacieho systému (tým druhým je verejný kľúč). Súkromný kľúč sa nezverejňuje a používa sa na 1. vytváranie digitálnych podpisov alebo 2. na dešifrovanie šifrových textov, šifrovaných pomocou verejného kľúča

kľúč, tajný [secret key] parameter symetrických šifier (kryptosystém symetrický), ktorý sa používa tak na šifrovanie (s. 507) otvorených (s. 508)otvorených, ako aj na dešifrovanie šifrových textov. (s. 508)

kľúč, verejný [public key] druhý z dvojice kryptografických kľúčov (s. 498) asymetrického šifrovacieho systému. Tento kľúč je verejne dostupný, či už prostredníctvom zoznamu, alebo certifikátu verejného kľúča (s. 494) a slúži na šifrovanie (s. 507) správ určených držiteľovi verejného kľúča a na overovanie digitálnych/ elektronických podpisov.

kód [code] 1. množina kódových slov, 2. program

kontinuita činnosti [business continuity] kroky, ktoré organizácia podniká na to, aby zabezpečeila nepretržitú dostupnosť svojich kľučových funkcií (služieb, zdrojov) pre ich oprávnených používateľov

kontrolný súčet/suma [checksum] číselná hodnota vypočítaná na základe textu/dokumentu/ súboru (najčastejšie pomocou hašovacej funkcie (s. 496)), ktorá slúži na ochranu integrity (s. 498) textu/dokumentu/ súboru

korekcia, opravná činnosť [corrective action] činnosť, ktorej cieľom je eliminovať príčinu zisteného nesúladu (súlad (s. 506)) alebo inej neželanej situácie

krádež identity [identity theft] predstieranie cudzej identity (s. 497) za účelom získania neoprávnených výhod. Predchádza mu získanie identifikačných údajov a prostriedkov na autentifikáciu (s. 492) osoby, za ktorú sa podvodník chce vydávať.

krízová situácia [crisis] 1. obdobie, počas ktorého je bezprostredne ohrozená alebo narušená bezpečnosť štátu a ústavné orgány môžu po splnení podmienok ustanovených v ústavnom zákone na jej riešenie vypovedať vojnu, vyhlásiť vojnový stav alebo výnimočný stav, alebo núdzový stav[1]; 2. obdobie mimo času vojny a vojnového stavu, počas ktorého je bezprostredne ohrozená alebo narušená bezpečnosť štátu a ústavné orgány môžu po splnení podmienok ustanovených v ústavnom zákone alebo osobitnom zákone na jej riešenie vyhlásiť výnimočný stav (s. 509), núdzový stav (s. 502) alebo mimoriadnu situáciu[2]

krízové riadenie súhrn riadiacich činností orgánov krízového riadenia (s. 499), ktoré sú zamerané na analýzu a vyhodnotenie bezpečnostných rizík a ohrození, plánovanie, prijímanie preventívnych opatrení, organizovanie, realizáciu a kontrolu činností vykonávaných pri príprave na krízové situácie a pri ich riešení[3]

krízový štáb výkonný orgán orgánu krízového riadenia (s. 499), ktorého úlohou je analyzovať riziká krízovej situácie, navrhovať opatrenia na jej riešenie a koordinovať činnosť zložiek v jeho pôsobnosti v období krízovej situ-

[1] Čl. 1 ods. 4 Ústavného zákona č. 227/2002 Z. z.
[2] § 2 písm. a) zákona č. 387/2002 Z. z.
[3] § 2 písm. b) zákona č. 387/2002 Z. z.
[4] § 2 písm. c) zákona č. 387/2002 Z. z.

ácie[4]

kryptoanalýza [cryptanalysis] 1. vedná disciplína zaoberajúca sa vývojom metód lúštenia (rozbíjania) šifier (s. 507). 2. (lúštenie rozbíjanie) šifry (s. 501)

kryptografia [cryptography] vedná disciplína zaoberajúca sa návrhom kryptosystémov (s. 500) (šifier)

kryptografická transformácia [cryptographic transformation] šifrovacia alebo dešifrovaciatransformácia

kryptografický kľúč [cryptographic key] pozri kľúč, kryptografický (s. 498)

kryptograficky silný kontrolný súčet [cryptographic checksum] kontrolný súčet (napr. číselne kódovaných znakov dokumentu), vytvorený pomocou kryptograficky silnej hašovacej funkcie

kryptografický protokol [cryptographic protocol] postupnosť predpísaných komunikačných a výpočtových krokov vykonávaných dvoma alebo viacerými subjektami pre dosiahnutie konkrétneho kryptografického cieľa, napr. autentifikácie (s. 492), distribúcie kľúča (s. 495) a pod.

kryptológia [cryptology] vedná disciplína zaoberajúca sa štúdiom kryptosystémov (s. 500) (šifier). Pozostáva z kryptografie (s. 500) a kryptoanalýzy

kryptosystém [cryptosystem] dvojica kryptografických transformácií (E, D), kde E je šifrovacia (s. 508) a D dešifrovacia (s. 508) transformácia

kryptosystém s verejným kľúčom [public key cryptosystem] asymetrická šifra/kryptosystém, pre ktorú má každý jej používateľ dvojicu kryptografických kľúčov: súkromný a verejný. Súkromný kľúč je utajený a verejný kľúč je zverejnený napr. pomocou certifikátu verejného kľúča (s. 494). Na šifrovanie (s. 507) správy odosielateľ používa verejný kľúč adresáta, adresát šifrovú správu dešifruje pomocou svojho súkromného kľúča.

kybernetická bezpečnosť [cybersecurity] všeobecne akceptovaná definícia neexistuje.

1. informačná bezpečnosť kybernetického priestoru (s. 500)
2. stav v ktorom sú siete a informačné systémy schopné odolávať na určitom stupni spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov[5]

kybernetický priestor [cyberspace] pôvodne metaforické označenie prostredia v ktorom prebieha prenos a spracovanie digitálnej zaznamenanej informácie. Všeobecne akceptovaná definícia neexistuje.

1. informačná a komunikačná infraštruktúru organizácie, štátu alebo globálna informačná a komunikačná infraštruktúra,
2. je globálny dynamický otvorený systém sietí a informačných systémov, ktorý tvoria aktivované prvky kybernetického priestoru, osoby vykonávajúce aktivity v tomto, systéme a vzťahy a interakcie medzi nimi[6]

kybernetický zločin [cybercrime] – protiprávna činnosť, ktorá

(a) je zameraná na informačné a komunikačné systémy, alebo
(b) ich využíva na nekalé ciele

L

[5] § 3 písm. g) zákon č. 69/25018 Z. z.
[6] § 3 písm. b) zákona č. 69/2018 Z. z.

lúštenie šifry [cipher cryptanalysis] kryptoanalýza šifry môže byť zameraná na odhalenie obsahu šifrového textu bez znalosti použitého kryptografického kľúča, alebo na určenie samotného kľúča. Závisí od toho, aké informácie má k dispoyícii kryptoanalytik a čo má možnosť robiť s kryptosystémom, na ktorý útočí. Pozri kryptoanalýza.

M

manažment certifikátov [certificate management] vydávanie, distribúcia, uchovávanie, overovanie platnosti, používanie a rušenie certifikátov (s. 494)

manažment informačno-bezpečnostných incidentov [information security incident management] procesy odhaľovania, nahlasovania, vyhodnocovania informačno-bezpečnostných incidentov (s. 497), reakcií na ne, ich riešenia a poučenia sa z nich

manažment kľúčov [key management] generovanie (s. 496), distribúcia, používanie, uchovávanie, aktualizácia a ničenie kryptografických kľúčov (s. 498)

miera [measure] atribút (veličina) a metóda na kvantitatívne určenie jej hodnoty

mimoriadna situácia Obdobie ohrozenia alebo obdobie pôsobenia následkov mimoriadnej udalosti na život, zdravie alebo majetok, ktorá je vyhlásená podľa **zákona č. 42/1994 Z. z.**; počas nej sa vykonávajú opatrenia na záchranu života, zdravia alebo majetku, na znižovanie rizík ohrozenia alebo činnosti nevyhnutné na zamedzenie šírenia a pôsobenia následkov mimoriadnej udalosti. Mimoriadnou udalosťou sa rozumie živelná pohroma, havária, katastrofa, ohrozenie verejného zdravia II. stupňa alebo teroristický útok, pričom

- živelná pohroma je mimoriadna udalosť, pri ktorej dôjde k nežiaducemu uvoľneniu kumulovaných energií alebo hmôt v dôsledku nepriaznivého pôsobenia prírodných síl, pri ktorej môžu pôsobiť nebezpečné látky alebo pôsobia ničivé faktory, ktoré majú negatívny vplyv na život, zdravie alebo na majetok,
- havária je mimoriadna udalosť, ktorá spôsobí odchýlku od ustáleného prevádzkového stavu, v dôsledku čoho dôjde k úniku nebezpečných látok alebo k pôsobeniu iných ničivých faktorov, ktoré majú vplyv na život, zdravie alebo na majetok,
- katastrofa je mimoriadna udalosť, pri ktorej dôjde k narastaniu ničivých faktorov a ich následnej kumulácii v dôsledku živelnej pohromy a havárie[7].

N

náhodné číslo [random number] možný výsledok činnosti generátora náhodných čísel (s. 496)

náhodný [random] proces, ktorého priebeh sa neriadi žiadnymi deterministickými zákonitosťami; tiež možný stav alebo výsledok takého procesu. Podstatnou črtou náhodného procesu je nepredvídateľnosť výsledku

narušenie bezpečnosti [security violation] akt alebo udalosť, ktorá nie je v súlade s bezpečnostnou politikou (s. 492) systému alebo organizácie

nepopretie [non repudiation] schopnosť dokázať, že nastala nejaká udalosť, alebo bola vykonaná nejaká činnosť a čo/kto bol/o jej pôvodcom/vykonávateľom

nepopretie pôvodu [non repudiation of origin] bezpečnostná požiadavka (s. 492) na dokument, ktorej naplnenie znamená, že tvorca (odosielateľ) dokumentu nebude môcť

[7] § 3 ods. 1 a 2 zák. č. 42/1994 Z. z. o civilnej ochrane obyvateľstva

poprieť, že dokument vytvoril (poslal)

nepopretie prijatia [non repudiation of receipt] bezpečnostná požiadavka (s. 492) na dokument/správu, (resp. na systém doručovania dokumentov) ktorej naplnenie znamená, že adresát nemôže poprieť, že dokument prijal

nesúlad [non-conformity] nesplnenie požiadavky

núdzový stav môže **vláda** vyhlásiť len za podmienky, že došlo alebo bezprostredne hrozí, že dôjde k ohrozeniu života a zdravia osôb, a to aj v príčinnej súvislosti so vznikom pandémie, životného prostredia alebo k ohrozeniu značných majetkových hodnôt v dôsledku živelnej pohromy, katastrofy, priemyselnej, dopravnej alebo inej prevádzkovej havárie; núdzový stav možno vyhlásiť len na postihnutom alebo na bezprostredne ohrozenom území. Núdzový stav možno vyhlásiť v nevyhnutnom rozsahu a na nevyhnutný čas, najdlhšie na 90 dní.[8]

O

oblasť aplikovateľnosti identity [identity applicability domain] množina entít (s. 496), ktoré majú identitu daného typu, v ktorej daná identita (s. 497) postačuje na jednoznačné odlíšenie jednotlivých entít. Oblasťou aplikovateľnosti identity môže byť napríklad množina dospelých slovenských občanov, identitou údaje uvedené v občianskom preukaze, hodnoty údajov z konkrétneho OP predstavujú identitu držiteľa daného OP.

obnova činnosti [business recovery] kroky, ktoré organizácia musí podniknúť na to, aby po bezpečnostnom incidente (s. 497), havárii alebo katastrofe čo najrýchlejšie obnovila informačnú a komunikačnú infraštruktúru (s. 497) podporujúcu jej kritické činnosti (disaster recovery)

obrana štátu [state defence] súhrn opatrení, ktorými Slovenská republika zachováva mier, bezpečnosť, zvrchovanosť, územnú celistvosť a nedotknuteľnosť hraníc a plní záväzky vyplývajúce z medzinárodných zmlúv o spoločnej obrane proti napadnutiu a z ďalších medzinárodných zmlúv vojenskej povahy. Obrana štátu sa zabezpečuje aj v kybernetickom priestore (s. 500) prostredníctvom opatrení zameraných na riešenie závažných kybernetických incidentov. Obranu štátu tvorí aj súhrn opatrení Slovenskej republiky na boj s terorizmom, ktoré v tejto oblasti vykonávajú **spravodajské služby**, súdy, prokuratúra, ozbrojené zbory a ozbrojené sily Slovenskej republiky.[9]

obranná infraštruktúra [defence infrastructure] pozemky, stavby, budovy a zariadenia, telekomunikačné, energetické a dopravné systémy, informačné siete (ďalej len „objekty obrannej infraštruktúry“) a zásoby štátnych hmotných rezerv, ktoré slúžia v čase vojny alebo vojnového stavu na zabezpečenie obrany štátu[10]

odopretie služby [denial of servis, DoS] výsledok akcie, alebo niekoľkých akcií, ktorý znemožňuje systému a/alebo aplikácii (najčastejšie z dôvodu preťaženia) správne fungovať a poskytovať požadované služby

odpočúvanie [eavesdropping] monitorovanie komunikácie prebehajúcej po prenosovom kanáli s cieľom získať kópiu prenášaných údajov

opatrenie [measure] pozri bezpečnostné opatrenie (s. 492)

osobné informácie [personal information] informácie vzťahujúce sa na fyzickú osobu, ktorých kompromitácia by mohla danú

[8] Čl. 5 ods. 1 a 2 Úst. zákona č. 227/2002 Z. z.
[9] § 2 ods. 1, 2 a 3 zákona č. 319/2002 Z. z.
[10] § 26 zákona č. 319/2002 Z. z.

fyzickú osobu nejako poškodiť

osobné údaje [personal data] 1. údaje obsahujúce osobné informácie 2. údaje týkajúce sa fyzických, fyziologických, psychických, mentálnych, ekonomických, kultúrnych a podobných atribútov určenej alebo určiteľnej osoby, t.j. čiastočná alebo úplná identita danej fyzickej osoby

overiť [verify] otestovať alebo dokázať pravdivosť nejakého faktu alebo pravdivosť či presnosť nejakej hodnoty

overovanie [verification] 1.proces skúmania informácie, aby sa určila pravdivosť nejakého tvrdenia alebo správnosť/presnosť nejakej hodnoty 2. proces porovnávania dvoch úrovní špecifikácie nejakého systému s cieľom zistiť, či sú v súlade.

P

paradox, narodeninový [birthday paradox] paradox vyplývajúci z odpovede na dve otázky: koľko ľudí musí byť v miestnosti, aby tam s pravdepodobnosťou väčšou alebo rovnou 0.5 boli dvaja, ktorí

1. sa narodili v danom dni roka
2. majú narodeniny v ten istý deň.

Paradox je v tom, že v prvom prípade to musí byť aspoň 183 ľudí, kým v druhom len 26 ľudí. Tento paradox sa využíva v kryptoanalýze.

personálna bezpečnosť [personnel security] opatrenia na zaistenie toho, aby sa minimalizovala pravdepodobnosť úmyselných útokov a neúmyselných chýb interných pracovníkov na systém, resp. pri práci so systémom. Opatrenia zahŕňajú výber, preverovanie, prípravu, monitorovanie, personálu; procedúry pri zmene pracovného zaradenia a ukončení zamestnania v organizácii.

PKI pozri infraštruktúra verejného kľúča (s. 498)

plaintext [plaintext] – vstupné údaje pre nejakú kryptografickú transformáciu. Ak údaje neboli predtým kryptograficky spracovávané, plaintext je zároveň otvoreným textom (s. 508) (cleartext). V praxi sa často pojem plaintext stotožňuje s pojmom otvorený text.

plán kontinuity činnosti [business continuity plan, BCP] výstup plánovania kontinuity činnosti. Plán na zabezpečenie súvislej činnosti organizácie zahŕňajúci aj neinformatické aspekty, ako je zaistenie kľúčových ľudí, obnovu informačných zdrojov, zariadení, krízovú komunikáciu, ochranu dobrého mena. Plán kontinuity činnosti obsahuje aj preventívne, detekčné a korekčné opatrenia.

plán obnovy [disaster recovery plan, DRP] postupnosť krokov na čo najrýchlejšie odstránenie následkov havárie/katastrofy a obnovu kritickej informačnej infraštruktúry (s. 498) organizácie

plánovanie, havarijné [disaster recovery planning] plánovanie činnosti pre prípad havárií (preventívne opatrenia, detekcia havárií, opatrenia na zmiernenie následkov havárie, opatrenia na odstránenie následkov havárie plán obnovy (s. 503))

plánovanie kontinuity činnosti [business continuity planning] vytváranie, implementácia, testovanie a revízie plánov kontinuity činnosti

podpis, digitálny [digital signature] bezpečnostná funkcia (s. 492) garantujúca integritu (s. 498) dokumentu, pre ktorý bola vytvorená a identitu (s. 497) entity, ktorá digitálny podpis vytvorila. V praxi má podobu hašovacej hodnoty (s. 497) podpisovaného dokumentu zašifrovanej pomocou súkromného kľúča (s. 499) podpisovateľa.

podpis, elektronický [electronic signature] údaje (s. 508) v elektronickej forme, ktoré sú pripojené k iným elektronickým údajom alebo sú logicky spojené s inými elektro-

nickými údajmi; ktoré slúžia na dôkaz autentickosti (s. 492). V tomto chápaní je elektronický podpis slabší ako digitálny podpis, pretože definícia elektronického podpisu nehovorí nič o úrovni záruk.

podpis, elektronický pokročilý [advanced electronic signature] je →digitálny/elektronický podpis vytvorený pomocou bezpečného zariadenia na vytváranie elektronických podpisov, ktorý má podpisovateľ pod kontrolou. V slovenskej legislatíve mu zodpovedá zaručený elektronický podpis.

podpis, vlastnoručný [handwritten signature] vlastnoručne napísané meno, alebo značka jednoznačne určujúca osobu, ktorý podpis vytvorila (podpisovateľ) a jej súhlas s obsahom dokumentu, ktorý vytvorením podpisu potvrdila

postupnosť pseudonáhodných čísel postupnosť čísel vygenerovaných generátorom pseudonáhodných čísel

potvrdenie platnosti [validation] 1. potvrdenie správnosti alebo korektnosti nejakej konštrukcie, 2. oficiálne potvrdenie zhody posudzovanej veci s nejakým štandardom

povinné riadenie prístupu [mandatory access control] typ riadenia prístupu, v ktorom operačný systém obmedzuje schopnosť subjektu, alebo procesu vykonávať nejaké činnosti, alebo pristupovať k zdrojom systému

preventívna činnosť [preventive action] činnosť zameraná na eliminovanie potenciálneho nesúladu (s. 502) alebo inej potenciálnej nežiadúcej situácie

prienik [penetration] úspešný, opakovateľný neoprávnený prístup k chránenému zdroju v systéme

priestor, digitálny [digital space] globálnym digitálnym priestorom je súhrn

(a) všetkých informačných a komunikačných technológií (s. 497), ich programového vybavenia a dokumentácie opisujúcej ich štruktúru, konfiguráciu a činnosť;
(b) informácií (s. 497), ktoré sa prostredníctvom nich prenášajú, spracovávajú alebo uchovávajú,
(c) procesov, ktoré v nich prebiehajú
(d) podpornej infraštruktúry zabezpečujúcej ich činnosť,
(e) ľudí zabezpečujúcich ich činnosť
(f) vzťahov medzi entitami digitálneho priestoru a pravidiel upravujúcich tieto vzťahy.

priestor, kybernetický [cyberspace] pozri kybernetický priestor (s. 500)

princíp najmenšieho privilégia [least privilege principle] podstata princípu spočíva v tom, že každá entita (s. 496) (človek, program, proces) v systéme má prístup len k tým zdrojom ktoré potrebuje na plnenie svojho poslania

princíp potreby poznať [need-to-know principle] iná verzia princípu najmenšieho privilégia: človek má prístup len k tým informáciám, ktoré potrebuje poznať na plnenie svojich pracovných povinností

prístup [access] 1. možnosť a schopnosť entity (s. 496) využívať zdroje systému 2. interakcia entity a systému

prístupové práva [access rights] oprávnenia na prístup (s. 504) k zdrojom systému a na vykonávanie vybraných operácií s nimi (napr. čítanie a zápis údajov, spúšťanie programov)

procedúra [procedure] špecifický spôsob, ako vykonať nejakú činnosť alebo proces

proces [process] postupnosť navzájom súvisiacich činností, ktorá transformuje vstupy na výstupy

pseudonymita [pseudonymity] bezpečnostná služba umožňujúca uchovať v tajnosti identit (s. 497)u osoby pred neoprávnenými osobami tým, že sa namiesto jej mena používa pseudonym. Oprávnená osoba pozná meno osoby nahradené pseudonymom.

R

registračná autorita [registration authority, RA] samostatná organizácia, alebo organizačná zložka certifikačnej autority, ktorá pre certifikačnú autoritu zabezpečuje niektoré služby (kontakt s klientmi, prijímanie žiadostí o vydanie/zrušenie certifikátu)

riadenie prístupu [access control] opatrenia na zaistenie toho, aby prístup (s. 504) ku zdrojom (aktívam (s. 491)) mali len oprávnené entity a len v súlade s ich prístupovými právami (s. 504)

riziko [risk] veličina závisiaca od závažnosti hrozby (s. 497) a pravdepodobnosti, že sa hrozba naplní.

riziko, analýza [risk analysis] pozri analýza rizík (s. 491)

riziko, akceptovateľné [acceptable risk] úroveň zvyškového rizika (s. 505), ktorú je organizácia schopná/ochotná tolerovať

riziko, hodnota [risk value] vyjadrenie miery rizika. Matematicky sa vyjadruje ako stredná hodnota dopadu hrozby na aktívum (s. 491)

riziko, identifikácia [risk identification] proces vyhľadávania, rozpoznávania a popísania rizík (s. 505)

riziko, kritériá [risk criteria] referenčné hodnoty, oproti ktorým sa vyhodnocuje významnosť rizika (s. 505)

riziko, ošetrenie [risk treatment] proces modifikácie rizika

riziko, stanovenie [risk assesment] celkový proces identifikácie rizika (s. 505), analýzy rizík (s. 491) a vyhodnotenia rizika (s. 505)

riziko, vyhodnotenie [risk evaluation] proces porovnávania výsledkov analýzy rizík (s. 491) s kritériami rizika (s. 505), ktorého cieľom je rozhodnutie, či je riziko a/alebo jeho hodnota akceptovateľná alebo tolerovateľná

riziko, zvyškové [residual risk] riziko (s. 505), ktoré ostalo po prijatí opatrení (s. 502)

robotická sieť [botnet] množina počítačov infiltrovaných škodlivým softvérom (s. 507), umožňujúcim ich ovládanie zo vzdialeného riadiaceho centra. Takéto siete sa využívajú na šírenie spamu (s. 506) a na útoky (s. 508) na vybrané ciele na Internete.

rootkit [rootkit] súbor nástrojov, pomocou ktorých môže útočník získať oprávnenia na úrovni správcu systému

rozhodovacie kritériá [decision criteria] prahové hodnoty, ciele alebo vzory, ktoré sa používajú na rozhodnutie o (potrebe) činnosti, ďalšieho skúmania alebo na popísanie úrovne dôvery v dosiahnutý výsledok

rozsah auditu [audit scope] špecifikácia toho, čo sa pri audite bude posudzovať a voči čomu

S

sieťová bezpečnosť [network security] ochrana sietí a sieťových služieb pred neoprávnenou modifikáciou, zničením alebo únikom údajov, zneprístupnením služieb a tiež zaistenie záruk, že sieť správne funguje a nevznikajú žiadne škodlivé vedľajšie efekty

silná autentifikácia [strong autentication] autentifikácia (s. 492) založená na dvoch alebo viacerých nezávislých metódach na overenie identity (s. 497) entity

slovníkový útok [dictionary attack] útok na systém, v ktorom sa na riadenie prístupu (s. 505) (autentizáciu (s. 492)autentizáciu používateľov) používajú heslá (s. 497), ktorého podstatou je preberanie slovníka potenciálnych hesiel

sniffer [**sniffer**] program umožňujúci monitorovanie komunikácie prebiehajúcej prostredníctvom siete

sociálne inžinierstvo [**social engineering**] netechnické metódy prieniku (s. 504) do systémov založené na interakcii s inými ľuďmi, ktorých sa útočník snaží nejakým spôsobom oklamať a primäť k tomu, aby porušili normálne používané bezpečnostné postupy.

softvérové pirátstvo [**software piracy**] neoprávnené kopírovanie, distribúcia a používanie počítačových programov, ktoré spadajú pod zákon na ochranu autorských práv

soľ [**salt**] náhodná hodnota, ktorá sa používa na zvýšenie odolnosti hesiel oproti slovníkovým útokom (s. 505), na generovanie kryptografických kľúčov a pod.

spam [**spam**] nevyžiadaná elektronická pošta

spoľahlivosť [**reliability**] schopnosť/vlastnosť entity správať sa konzistentne zamýšľaným spôsobom a dosahovať požadované výsledky

spoof [**spoof**] pokus neoprávnenej osoby získať prístup (s. 504) do systému vydávaním sa za inú (oprávnenú) osobu

spracovanie informácie [**information processing**] zber, prenos, uchovávanie (vlastné spracovávanie: triedenie, spájanie výber), používanie, archivácia a ničenie informácie

správa rizík [**risk management**] identifikácia rizík, odhad rizík, vyhodnotenie rizík, prijatie opatrení a monitorovanie zostatkových rizík, prehodnocovanie rizík

stanovenie rizika [**risk assesment**] pozri riziko, stanovenie (s. 505)

súkromnosť [**privacy**] bezpečnostná požiadavka na údaje (s. 508), ktorej naplnenie znamená, že osoba, ktorej sa údaje týkajú, má možnosť rozhodnúť, komu, aké a za akých podmienok sa údaje, ktoré sa jej týkajú poskytnú a skontrolovať, či sa jej rozhodnutia dodržujú

súlad [**conformity**] splnenie nejakej požiadavky

systém [**system**] informačný a komunikačný systém slúžiaci na spracovanie informácie

systém obrany štátu [**system of state defence**] súhrn prvkov a opatrení štátu, ktorých prostredníctvom ministerstvá, ostatné ústredné orgány štátnej správy, súdy, prokuratúra, orgány miestnej štátnej správy, obce, vyššie územné celky, iné právnické osoby, fyzické osoby oprávnené na podnikanie a fyzické osoby vytvárajú predpoklady na zabezpečenie obrany štátu a na plnenie záväzkov vyplývajúcich z medzinárodných zmlúv o spoločnej obrane proti napadnutiu a z ďalších medzinárodných zmlúv, ktorými je Slovenská republika viazaná.[11]

systém riadenia informačnej bezpečnosti [**information security management system, ISMS**] systematický prístup k riešeniu informačnej bezpečnosti v organizácii založený na súbore formálne zdokumentovaných a vzájomne koordinovaných bezpečnostných politík stanovujúcich ciele a úroveň informačnej bezpečnosti v organizácii, zodpovednosť za IB, organizačné zabezpečenie, upravujúcich požiadavky na personálnu bezpečnosť, vzťahy s externými partnermi, fyzickú bezpečnosť, prevádzkovú a komunikačnú bezpečnosť, ochranu prístupu a súlad s legislatívou.

Š

[11] § 2 ods. 6 zákona č. 319/2002 Z. z.

šifra [cipher] synonymum pojmu kryptosystém (s. 500)

šifra, absolútne bezpečná [unconditionally secure cipher] šifra, ktorá sa dokázateľne nedá rozbiť ani s vynaložením ľubovoľne veľkých prostriedkov. Príkladom taketo šifry je Vernamova šifra (s. 507)

šifra, asymetrická [asymmetric cipher] 1. šifra, v ktorej sa na šifrovanie používa iný kľúč ako na dešifrovanie, 2.kryptosystém s verejným kľúčom (s. 500)

šifra, bloková [block cipher] podstata tejto šifry je v tom, že sa otvorený text rozdelí na časti rovnakej dĺžky (bloky), ktoré sa následne šifrujú pomocou toho istého tajného kľúča. Výsledkom šifrovania je postupnosť blokov šifrového textu, ktoré sa dešifrujú pomocou dešifrovacej transformácie a tajného kľúča.

šifra, klasická [classic cipher] synonymum pre symetrickú šifru (s. 507)

šifra, permutačná [permutation cipher] Symetrická (bloková) šifra, podstata šifrovania je v tom, že sa poprehadzuje poradie znakov otvoreného textu (s. 508). Tajným kľúčom (s. 499) je permutácia, určujúca nové poradie znakov.

šifra, prúdová [stream cipher] podstata prúdovej šifry je v tom, že sa z tajného kľúča (s. 499) (inicializačný vektor (s. 498) alebo seed) generuje postupnosť kľúčov. Otvorený text je rozdelený na krátke bloky (často jednotlivé znaky alebo bity) a v i-tom kroku sa i-ta časť otvoreného textu šifruje pomocou i-teho kľúča:

$$E(m_i, k_i) = c_i.$$

Pri dešifrovaní sa používa ten istý generátor kľúčov (s. 496) s rovnakým tajným kľúčom a v i-tom kroku sa dešifruje

$$D(c_i, k_i) = m_i.$$

šifra, substitučná [substitution cipher] substitučná →šifra nahrádza znaky otvoreného textu (s. 508) znakmi šifrového textu (s. 508). Šifra môže byť monoalfabetická, keď sa znak otvoreného textu nahrádza zakaždým tým istým znakom šifrového textu, alebo polyalfabetická, keď sa znak otvoreného textu nahrádza jedným z viacerých (potenciálne aj všetkých) znakov šifrového textu. Výber šifrového znaku pre daný znak otvoreného textu je daný šifrovacím kľúčom.

šifra, symetrická [symmetric cipher] šifra, v ktorej sa na šifrovanie a dešifrovanie používa ten istý tajný kľúč (s. 499)

šifra, Vernamova [Vernam cipher] absolútne bezpečná šifra. Text (binárny reťazec) sa šifruje pomocou kryptografického kľúča rovnakej dĺžky tak, že sa i-ty bit kľúča sčíta modulo 2 s i-tym bitom otvoreného textu (dešifrovanie šifrového textu sa robí rovnako). Kryptografický kľúč sa na šifrovanie môže použiť len raz a musí byť náhodný.

šifrovacia transformácia [encryption/enciphering transformation] pozri transformácia, šifrovacia (s. 508)

šifrovanie [encryption, enciphering] transformácia otvoreného textu (s. 508) na šifrový (s. 508) pomocou šifrovacej transformácie (s. 508) a šifrovacieho kľúča

šifrovanie od odosielateľa po príjemcu [end-to-end encryption] ochrana dôvernosti prenášaných správ založená na tom, že odosielateľ správu zašifruje, pošle ju v šifrovanej podobe príjemcovi, ktorý ju dešifruje.

šifrový text [ciphertext] pozri text, šifrový (s. 508)

škodlivý softvér [malicious software, malware] červy, vírusy, trójske kone a iné programy vytvorené s cieľom získať pre svojho používateľa neoprávnené privilégiá na cudzom počítači, alebo jeho majiteľa poškodiť.

T

text, otvorený [cleartext] text, ktorý nebol modifikovaný žiadnou kryptografickou transformáciou

text, šifrový [ciphertext] výsledok zašifrovania otvoreného textu pomocou šifrovacej transformácie (s. 508) E (a šifrovacieho kľúča).

transformácia, dešifrovacia [deciphering transformation] injektívne zobrazenie D, ktoré šifrovému textu (s. 508) c priradí otvorený text (s. 508) m. Dešifrovacia transformácia má okrem šifrového textu aj druhý parameter, k, dešifrovací kľúč. K dešifrovacej transformácii D prislúcha opačná šifrovacia transformácia (s. 508) E. Obe transformácie sú spojené vzťahom

$$\forall m \in M, \forall k \in K : D((E(m,k),k) = m,$$

kde M je množina správ (messages) a K množina kryptografických kľúčov.

transformácia, šifrovacia [enciphering transformation] je spravidla injektívne zobrazenie E (encryption, enciphering), ktoré správe m (→otvorenému textu) priradí šifrový text (s. 508) c (ciphertext). Šifrovacia transformácia má spravidla dva argumenty šifrovací kľúč k a správu m:

$$E(m,k) = c.$$

K šifrovacej transformácii prislúcha opačná, dešifrovacia transformácia (s. 508) D. Obe transformácie sú spojené vzťahom

$$\forall m \in M, \forall k \in K : D((E(m,k),k) = m,$$

kde M je množina správ (messages) a K množina kryptografických kľúčov.

U

účinnosť [effectivness] rozsah v ktorom boli vykonané plánované činnosti a dosiahnuté plánované výsledky

údaje [data] údaje [data] forma záznamu informácie (s. 497)informácie v informačných a komunikačných systémoch

udalosť [event] výskyt alebo zmena špecifickej množiny okolností

udalosť relevantná pre informačnú bezpečnosť [information security event] identifikovaný výskyt stavu systému, služby alebo siete, ktorý indikuje možné porušenie bezpečnostnej politiky, alebo zlyhanie bezpečnostného opatrenia; alebo dovtedy neznáma situácia, ktoré môže mať význam z hľadiska informačnej bezpečnosti

únik údajov [data leakage] náhodný tok citlivých údajov k neoprávnenej entite

úroveň rizika [level of risk] hodnota rizika; v kvantitatívnom vyjadrení stredná hodnota dopadu príslušnej hrozby na dané aktívum; pri kvalitatívnom vyjadrení hodnota zohľadňujúca dopad hrozby na aktívum a pravdepodobnosť jej naplnenia

útočník [attacker] osoba, ktorá vykonáva útok (s. 508) na systém, alebo nejaké aktívum systému/organizácie

útočný potenciál [attack potential] znalosti, motivácia a príležitosť útočníka uskutočniť úspešný útok (s. 508)

útok [attack] cieľavedomý pokus o využitie nejakej zraniteľnosti (s. 510) systému/aktíva za účelom získania neoprávnených oprávnení, alebo poškodenia/zničenia daného aktíva, alebo niektorého z iných aktív systému/organizácie.

útok hrubou silou [brute force attack] kryptoanalytický útok založený na preberaní všetkých možností (napríklad možných dešifrovacích kľúčov, →otvorených textov)

útok úplným prehľadávaním [exhaustive attack] útok hrubou silou (s. 508)

útok typu denial of servis [denial of servis (DoS) attack] útok na systém/aplikáciu s cieľom dosiahnuť odmietnutie služby (s. 502)

V

verifikácia [verification] overenie pravdivosti tvrdenia alebo skutočnosti

vniknutie [intrusion] hrozba (s. 497), pri naplnení ktorej neoprávnená osoba získava prístup k citlivým údajom (s. 494) tým, že obíde (úmyselne alebo neúmyselne) bezpečnostné opatrenia (s. 492) systému.

vojna [war] Vojnu vypovie prezident na základe rozhodnutia Národnej rady Slovenskej republiky (ďalej len „národná rada“) len za podmienky, že Slovenská republika je napadnutá cudzou mocou, ktorá jej vypovedala vojnu alebo ktorá bez vypovedania vojny narušila jej bezpečnosť, alebo za podmienky, že vypovedaním vojny Slovenská republika plní záväzky vyplývajúce z členstva v organizácii vzájomnej kolektívnej bezpečnosti alebo z medzinárodnej zmluvy o spoločnej obrane proti napadnutiu. Vypovedanie vojny sa vzťahuje na celé územie Slovenskej republiky.[12]

vojnový stav [state of war] môže na návrh vlády vyhlásiť prezident len za podmienky, že Slovenskej republike bezprostredne hrozí vypovedanie vojny alebo bezprostredne hrozí napadnutie cudzou mocou bez vypovedania vojny. Vyhlásenie vojnového stavu sa vzťahuje na celé územie Slovenskej republiky.[13]

voliteľné riadenie prístupu [discretionary access control] riadenie prístupu (s. 505) založené na tom, že (a) oprávnenia na činnosť v systéme sú viazané na entity, ktoré musia preukázať svoju identitu (b) entity sú vlastníkmi systémových zdrojov (napr. údajov) a môžu iným entitám prideliť alebo odňať prístupové práva (s. 504) k týmto zdrojom.

vyčíslenie rizík [risk assesment] analytická činnosť zameraná na systém alebo organizáciu, ktorej výsledkom je identifikácia rizík a odhad ich hodnôt

vydavateľ certifikátu [certificate issuer] v prípade digitálneho certifikátu (s. 494) certifikačná autorita (s. 493), ináč inštitúcia oprávnená certifikovať výrobky, služby, ľudí, organizácie a vydávať o kladnom výsledku certifikácie osvedčenie v podobe certifikátu.

výmena kľúčov [key exchange] protokoly na výmenu, dohodnutie alebo vytvorenie tajného kľúča (s. 499) pre bezpečnú komunikáciu dvoch alebo viacerých strán

výnimočný stav môže na **návrh vlády** vyhlásiť **prezident** len za podmienky, že došlo alebo bezprostredne hrozí, že dôjde k teroristickému útoku, k rozsiahlym pouličným nepokojom spojeným s útokmi na orgány verejnej moci, drancovaním obchodov a skladov alebo s inými hromadnými útokmi na majetok alebo dôjde k inému hromadnému násilnému protiprávnemu konaniu, ktoré svojím rozsahom alebo následkami podstatne ohrozuje alebo narušuje verejný poriadok a bezpečnosť štátu, ak ho nemožno odvrátiť činnosťou orgánov verejnej moci a ak je znemožnené účinné použitie zákonných prostriedkov; výnimočný stav možno vyhlásiť len na postihnutom alebo na bezprostredne ohrozenom území. Výnimočný stav možno vyhlásiť v nevyhnutnom rozsahu a na nevyhnutný čas, najdlhšie na 60 dní. Ak vzniknú nové okolnosti bezprostredne súvisiace s dôvodmi, pre ktoré bol výnimočný stav vyhlásený, možno výnimočný stav predĺžiť v nevyhnutnom rozsahu a na nevyhnutný čas, najviac o ďalších 30 dní.[14]

využitie [exploit] explicitne definovaný spôsob, ako narušiť bezpečnosť systému využitím nejakej jeho zraniteľnosti (s. 510)

[12] Čl. 2 ods. 1 a 2 Úst. zákona č. 227/2002 Z. z.
[13] Čl. 3 ods. 1 a 2 Úst. zákona č. 227/2002 Z. z.
[14] Čl. 4 ods. 1 a 2 Úst. zákona č. 227/2002 Z. z.

X

X-509 [**X-509**] Odporúčanie ITU-T X509, ktoré definuje rámec na poskytovanie a podporu autentifikácie pôvodu údajov a autentifikácie seberovných (peer) entít. X-509 obsahuje formáty X-509 certifikátu verejného kľúča, X-509 atribútového certifikátu a X-509 zoznamu zrušených certifikátov.

X-509 certifikát verejného kľúča [**X-509 public key certificate**] certifikát verejného kľúča (s. 494) vo formáte špecifikovanom odporúčaním ITU-T X509 (s. 510)

X-509 atribútový certifikát [**X-509 attribute certificate**] atribútový certifikát (s. 494) vo formáte špecifikovanom odporúčaním ITU-T X509 (s. 510)

X-509 zoznam zrušených certifikátov [**X-509 certificate revocation list**] zoznam zrušených certifikáto (s. 510) vo formáte špecifikovanom odporúčaním ITU-T X509 (s. 510)

Z

zadné vrátka, skryté dvere [**trap door**] skrytý softvérový alebo hardvérový mechanizmus, ktorý po aktivácii umožní obchádzať bezpečnostné mechanizmy systému

zapisovač klávesnice [**key logger**] škodlivý program nepozorovane zaznamenávajúci stláčanie kláves na klávesnici, ktorý následne poskytuje túto informáciu inej osobe, ako je prihlásený používateľ

základné bezpečnostné štandardy [**baseline standards**] štandardy špecifikujúce minimálny (základný) súbor bezpečnostných opatrení (s. 492), ktoré sú za normálnych okolností vhodné pre väčšinu organizácií s podobným technickým a programovým vybavením a provnateľnými bezpečnostnými potrebami

záznam auditu [**audit log**] časovo usporiadaný zoznam zápisov o bezpečnostne relevantných udalostiach v systéme. Zápis o bezpečnostne relevantnej udalosti obsahuje minimálne čas, popis udalosti a identifikátor (s. 497) entity, ktorá udalosť spôsobila

zneužitie identity [**identity fraud**] podvod spojený s nelegálnym použitím identity, najčastejšie s predstieraním cudzej identity

zoznam zrušených certifikátov [**certificate revocation list, CRL**] zoznam certifikátov, ktorým bola z nejakých dôvodov predčasne zrušená platnosť. Vydáva ho certifikačná autorita, ktorá dané certifikáty vydala a musí byť v krátkych časových intervaloch (deň) aktualizovaný a verejne prístupný.

zraniteľnosť [**vulnerability**] vlastnosť, spôsob použitia alebo okolnosť umožňujúce naplnenie nejakej špecifickej hrozby. (s. 497) Napr. pripojenie nechráneného počítača k Internetu umožňuje hackerský útok, neaktuálna databáza vírusov je zraniteľnosťou umožňujúcou napadnutie počítača zlomyseľným softvérom.

16.3 Anglicko-slovenský register

acceptable risk akceptovateľné riziko
access prístup (s. 504)
access control riadenie prístupu (s. 505)
access rights prístupové práva (s. 504)
accreditation akreditácia
accountability dosledovateľnosť (s. 495)
advanced electronic signature pokročilý/zdokonalený elektronický podpis
air gap fyzické oddelenie
anonymity anonymita (s. 491)
antivirus software antivírový softvér, antivírus

asset aktívum (s. 491)
attribute atibút
attribute certificate atribútový certifikát
attack útok (s. 508)
attack potential útočný potenciál (s. 508)
attacker útočník (s. 508)
attack, brute force útok úplným preberaním
audit audit (s. 492)
audit log záznam auditu (s. 510)
audit scope rozsah auditu (s. 505)
authentication autentifikácia/autentizácia
autenticity autentickosť (s. 492)
authorization autorizácia, udelenie oprávnenia
aviability dostupnosť (s. 495)
archive archív, archivovať
assymetric cryptosystem asymetrický kryptosystém
assymetric cipher asymetrická šifra
awareness (bezpečnostné) povedomie
backup zálohovať
base measure základná miera
biometric biometrický (s. 493)
biometric authentication biometrická autentifikácia (s. 493)
biometric characteristics biometrické charakteristiky (s. 493)
biometric data biometrické údaje (s. 493)
birthday paradox narodeninový paradox
block cipher bloková šifra
botnet robotická sieť, botnet
brute force hrubá sila
brute force attack útok hrubou silou (s. 508)
business continuity kontinuita činnosti (s. 499)
business continuity plan, bcp plán kontinuity činnosti (s. 503)
business continuity planning plánovanie kontinuity činnosti
business recovery obnova činnosti (s. 502)
CA certifikačná autorita (s. 493)
certificate certifikát, certifikovať
certificate holder držiteľ certifikátu (s. 495)
certificate issuer vydavateľ certifikátu (s. 509)
certificate management manažment certifikátov (s. 501)
certificate revocation zrušenie platnosti certifikátu
certification authority certifikačná autorita (s. 493)
certification path certifikačná cesta (s. 493)
certificate revocation list, CRL zoznam zrušených certifikátov (s. 510)
certification service certifikačná služba (s. 494)
cipher šifra (s. 507)
cipher block chaining, cbc zreťazovanie šifrových blokov, (mód šifrovania blokových šifier)
ciphertext šifrový text (s. 507)
checksum kontrolný súčet (s. 499)
classic cipher klasická šifra
classification scheme klasifikačná schéma (s. 498)
cleartext otvorený text
code kód (s. 499)
communication channel komunikačný kanál
confidentiality dôvernosť (s. 495)
conformity konformnosť, súlad
control prostriedok, opatrenie, riadenie
control objective cieľ opatrenia
corrective action korekcia, opravná činnosť
covert channel skrytý kanál
critical infrastructure kritická infraštruktúra
CRL zoznam zrušených certifikátov (s. 510)
cryptanalysis kryptoanalýza
cryptographic chcecksum kryptograficky silný kontrolný súčet (s. 500)
cryptographic protocol kryptografický protokol (s. 500)
cryptographic transformation kryptografická transformácia (s. 500)
cryptography kryptografia (s. 500)
cryptology kryptológia
cryptosystem kryptosystém, šifra
cybercrime kybernetický zločin (s. 500)
cyberspace kybernetický priestor (s. 500)
data údaje (s. 508)
data classification klasifikácia údajov (s. 498)
data leakage únik údajov (s. 508)

day one deň jedna
day zero deň nula
deciphering dešifrovanie
declassify deklasifikovať (informáciu)
decision criteria rozhodovacie kritériá (s. 505)
decryption dešifrovanie
decryption transformation dešifrovacia transformácia
denial of service odopretie služby (s. 502)
denial of service attack, DoS attack útok typu denial of service
derived measure odvodená miera
dictionary attack slovníkový útok (s. 505)
digital certificate digitálny certifikát
digital fingerprint digitálny odtlačok (dokumentu)
digital signature digitálny podpis
digital space digitálny priestor
disaster recovery plan, BRP plán obnovy (s. 503)
disaster recovery planning havarijné plánovanie
discretionary access control voliteľné riadenie prístupu (s. 509)
distributed denial of service attack, DDoS distribuovaný útok typu denial of service (s. 495)
DoS odopretie služby (s. 502)
eavsdropping odpočúvanie (s. 502)
ECB elektronická kódová kniha
effectivness účinnosť (s. 508)
efficiency efektivita (s. 496)
electronic code book elektronická kódová kniha, šifrovací mod blokových šifier
electronic signature elektronický podpis
enciphering šifrovanie (s. 507)
enciphering transformation šifrovacia transformácia (s. 507)
encryption šifrovanie (s. 507)
encryption transformation šifrovacia transformácia (s. 507)
end-to-end encryption šifrovanie od odosielateľa po príjemcu (s. 507)
entity entita (s. 496)
event udalosť (s. 508)
exhaustiv attack útok úplným prehľadávaním (s. 508)
exploit využitie (s. 509)
external context externý kontext (s. 496)
granularity granularita, jemnosť
hacker hacker (s. 496)
handwritten signature vlastnoručný podpis
hash hašovacia hodnota (s. 497)
hash function hašovacia funkcia (s. 496)
identification identifikácia (s. 497)
identifier identifikátor (s. 497)
identity identita (s. 497)
identity fraud zneužitie identity (s. 510)
identity theft krádež identity (s. 499)
incident incident (s. 497)
information informácia (s. 497)
information and communication technology, ICT informačné a komunikačné technológie, IKT
information classification klasifikácia informácie
information infrastructure informačná infraštruktúra
information processing spracovanie informácie (s. 506)
information security informačná bezpečnosť
information security event udalosť relevantná pre informačnú bezpečnosť (s. 508)
information security incident management manažment informačno-bezpečnostných incidentov (s. 501)
information security management system, ISMS systém manažmentu informačnej bezpečnosti, SMIB
information system informačný systém (s. 497)
initialization vector inicializačný vektor, počiatočná hodnota PRNG
infrastructure infraštruktúra (s. 497)
incident incident (s. 497)
integrity integrita (s. 498)
intrusion vniknutie (s. 509)
key kľúč
key encryption key kľúč na šifrovanie kľúčov (s. 499)
key exchange výmena kľúčov (s. 509)
key generation generovanie kľúčov (s. 496)

key logger zapisovač klávesnice (s. 510)
key management manažment kľúčov (s. 501)
key, cryptographic kryptografický kľúč (s. 500)
key, public verejný kľúč
key, private súkromný kľúč
key, secret tajný kľúč
least privilege principle princíp najmenšieho privilégia (s. 504)
level of risk úroveň rizika (s. 508)
malicious software zlomyseľný softvér
malware zlomyseľný softvér
mandatory access control povinné riadenie prístupu (s. 504)
measure 1. miera, 2. opatrenie
need-to-know principle princíp potreby poznať
network security sieťová bezpečnosť (s. 505)
non-conformity nesúlad (s. 502)
non-repudiation nepopretie (s. 501)
non repudiation of origin nepopretie pôvodu (s. 501)
non repudiation of receipt nepopretie prijatia (s. 502)
one time password jednorazové heslo (s. 498)
password heslo (s. 497)
personal data osobné údaje (s. 503)
personal information osobné informácie (s. 502)
personnel security personálna bezpečnosť (s. 503)
physical security fyzická bezpečnosť (s. 496)
plaintext plaintext (s. 503)
penetration prienik (s. 504)
permutation cipher permutačná šifra
preventive action preventívna činnosť (s. 504)
privat key súkromný kľúč
privacy súkromnosť, súkromie
pseudonymity pseudonymita (s. 504)
procedure procedúra
process proces (s. 504)
pseudorandom number gererator, PRNG generátor pseudonáhodných čísel (s. 496)
public key infrastructure, PKI infraštruktúra verejného kľúča (s. 498)
public key verejný kľúč
public key certificate certifikát verejného kľúča (s. 494)
public key cryptography asymetrická kryptografia, kryptografia verejného kľúča
public key cryptosystem kryptosystém s verejným kľúčom (s. 500)
random náhodný (s. 501)
random number náhodné číslo (s. 501)
random number generator generátor náhodných čísel (s. 496)
registration authority registračná autorita (s. 505)
reliability spoľahlivosť (s. 506)
residual risk zvyškové riziko
risk riziko (s. 505)
risk, acceptable akceptovateľné riziko
risk acceptance akceptovanie rizika
risk analysis analýza rizík (s. 491)
risk assesment stanovenie rizík
risk criteria kritériá rizika
risk evaluation vyhodnocovanie rizika
risk identification identifikácia rizika
risk management správa rizík (s. 506)
risk treatment ošetrenie rizika
risk, residual zvyškové riziko
root CA koreňová ca
root certificate koreňový certifikát
rootkit rootkit (s. 505)
salt soľ (s. 506)
secret key tajný kľúč
security bezpečnosť
security assurance bezpečnostná záruka (s. 492)
security architecture bezpečnostná architektúra (s. 492)
security awareness bezpečnostné povedomie (s. 493)
security baselines základné bezpečnostné štandardy (s. 510)
security by obscurity bezpečnosť pomocou utajovania (s. 493)
security directives bezpečnostné smernice (s. 493)
security environment bezpečnostné prostredie (s. 493)

security function bezpečnostná funkcia (s. 492)
security goal bezpečnostný cieľ
security incident bezpečnostný incident (s. 493)
security measure/control bezpečnostné opatrenie (s. 492)
security policy bezpečnostná politika (s. 492)
security project bezpečnostný projekt (s. 493)
security requirement bezpečnostná požiadavka (s. 492)
security target bezpečnostný zámer (s. 493)
security violation narušenie bezpečnosti (s. 501)
seed počiatočná hodnota generátora pseudonáhodných čísel
sensitive information citlivá informácia (s. 494)
sensitive but unclassified citlivá ale neklasifikovaná (informácia)
single sign off jediné odhlásenie (s. 498)
single sign on jediné prihlásenie (s. 498)
signatory podpisovateľ
signature podpis
sniffer sniffer (s. 505)
social engineering sociálne inžinierstvo (s. 506)
software piracy softvérové pirátstvo (s. 506)
spam spam (s. 506)
spoof spoof (s. 506)
stream cipher prúdová šifra
strong authentication silná autentifikácia (s. 505)
substitution cipher substitučná šifra
symmetric cipher symetrická šifra
system systém (s. 506)
timestamp časová pečiatka (s. 495)
threat hrozba (s. 497)
trap door zadné vrátka (s. 510)
trusted computing base dôveryhodná výpočtová báza (s. 495)
trust dôvera (s. 495)
two-factor authentication dvojfaktorová autentifikácia (s. 496)
unconditionally secure cipher absolútne bezpečná šifra
validation potvrdenie platnosti (s. 504)
verification overovanie (s. 503)
verify overiť (s. 503)
Vernam cipher šifra, Vernamova (s. 507)
vulnerability zraniteľnosť (s. 510)

Literatúra

[1] W. contributors. *Wikipedia – The Free Encyclopedia*. 2020. URL: https://en.wikipedia.org/wiki (cit. 18. 12. 2020).

[2] *ISO/IEC 27000 Information technology – Security techniques – Information security management systems – Overview and vocabulary*. ISO.

[3] S. Lloyd. *Understanding Certification Path Construction*. Sept. 2002. URL: http://www.oasis-pki.org/pdfs/Understanding_Path_construction-DS2.pdf (cit. 18. 12. 2020).

[4] D. Olejár a kol. *Výkladový slovník termínov z informačnej bezpečnosti*. Bratislava: MF SR, 2009.

[5] B. Schneier. *Applied cryptography: protocols, algorithms, and source code in C*. 2nd ed. Wiley, 1996. ISBN: 9780471128458.