Základy bezpečnostných opatrení

Príručka manažéra kybernetickej bezpečnosti

Ing. Ivan Makatura, CRISC, CDPSE

Vzor citácie: Makatura, I.: Základy bezpečnostných opatrení. Príručka manažéra kybernetickej bezpečnosti. Žilina: Poradca podnikateľa, s. r. o., 2024, 212 s.

Recenzenti: JUDr. Lucia Bezáková
prof. RNDr. Michal Greguš, PhD.
Mgr. Ivan Kopáčik
por. Mgr. Matej Šalmík
Mgr. Marek Zeman, PhD.

Základy bezpečnostných opatrení

Príručka manažéra kybernetickej bezpečnosti

prvé vydanie, Žilina: Poradca podnikateľa, s. r. o., február 2024, 212 s.
ISBN 978-80-8186-161-1

EUROKÓDEX
www.eurokodex.sk

Predslov

Vzhľadom na neustále sa rozvíjajúce hrozby v oblasti informačnej a kybernetickej bezpečnosti je ošetrenie rizík, spojených s kybernetickou bezpečnosťou, jednou z hlavných výziev pre zabezpečenie udržateľného a dôveryhodného digitálneho trhu.

Kde sa nachádzame v súčasnosti? Pri každodennej rutinnej práci či zábave s výpočtovými zariadeniami si dnes málokto uvedomuje, že merateľný výpočtový výkon bežne dostupného lacného smartfónu sa už vôbec nedá porovnať s výkonom niekdajšieho špičkového osobného počítača. Práca i súkromie sa čoraz viac presúvajú do kybernetického priestoru. Zvýšený objem dát a informácií spracúvaných v kybernetickom priestore spolu so zvyšujúcou sa komplexitou technologického prostredia a väčším množstvom automatizovaných pracovných procesov nutne generuje zvýšený počet kybernetických bezpečnostných hrozieb.

Ambíciou tejto publikácie je poskytnúť nezávislý pohľad na výkladové a aplikačné problémy, praktickú stránku požiadaviek na bezpečnostné opatrenia vrátane vysvetlenia všeobecného významu opatrení a procesných povinností, ktoré vyplývajú povinným osobám z legislatívy. Príručka je určená na vzdelávanie dospelých, teda čitateľom, ktorí už majú určitú prax v informatike a v manažmente. Preto jednotlivé témy nie sú rozpracované do úplného technického detailu. Primárnou snahou bolo prepojiť požiadavky právnych predpisov, najmä zákona o kybernetickej bezpečnosti, s praktickými otázkami kybernetickej bezpečnosti a poskytnúť náhľad do problematiky aplikácie bezpečnostných opatrení.

Dobrá prax, európska aj národná legislatíva v posledných rokoch výraznejšie presadzujú prístup ku kybernetickej bezpečnosti a ochrane údajov pomocou prístupu založeného na riadení rizika. Keďže aj návrh bezpečnostných opatrení a rozhodnutie o ich implementácii musia byť prispôsobené identifikovaným rizikám, oblasti riadenia rizík je v tejto publikácii venovaná rozsiahlejšia kapitola. Napriek tomu záujemcom o hlbšie pochopenie problematiky riadenia rizík odporúčame ďalšiu literatúru, ktorá sa touto témou zaoberá.

Inšpiráciou pre kompozíciu tohto textu bola séria článkov zverejnených postupne na portáli bezpecnostvpraxi.sk. Zverejnené články sa stali základom tejto knižnej publikácie.

Príručka nie je iba teóriou, ktorá nikdy nebola overená v praxi, ale naopak — pohľadom a poznámkami z reálnej praxe informačnej a kybernetickej bezpečnosti.

Poďakovanie za cenné pripomienky k publikácii patrí recenzentom. K finálnemu textu obzvlášť prispeli (v abecednom poradí): JUDr. Lucia Bezáková, prof. RNDr. Michal Greguš, PhD., Mgr. Ivan Kopáčik, por. Mgr. Matej Šalmík a Mgr. Marek Zeman, PhD.

autor

O autorovi

Ivan Makatura je bezpečnostný manažér a konzultant s mnohoročnou praxou riaditeľa odboru bezpečnosti v bankách a neskôr praxou vedúceho konzultanta v nadnárodnej konzultačnej spoločnosti — so zameraním na oblasť informačnej a kybernetickej bezpečnosti, ochranu osobných údajov a riadenie rizík.

V oblasti informačnej bezpečnosti a riadenia IT pracuje už viac ako štvrťstoročie. Je generálnym riaditeľom Kompetenčného a certifikačného centra kybernetickej bezpečnosti, členom Správnej rady Európskeho centra odvetvových, technologických a výskumných kompetencií v kybernetickej bezpečnosti, National Liaison Officer a člen poradnej skupiny Európskej agentúry pre kybernetickú bezpečnosť (ENISA). Zároveň pôsobí ako súdny znalec v odvetví Bezpečnosť a ochrana informačných systémov zapísaný v Zozname znalcov, tlmočníkov a prekladateľov Ministerstva spravodlivosti Slovenskej republiky a tiež ako certifikovaný audítor a certifikovaný manažér kybernetickej bezpečnosti. V úlohe člena Technickej komisie Úradu pre normalizáciu a metrológiu SR sa spolupodieľa na preklade noriem ISO pre oblasť informačnej bezpečnosti a na ich implementácii do sústavy slovenských technických noriem.

Vyštudoval odbor výpočtová technika a neskôr odbor aplikovaná informatika na Fakulte elektrotechniky a informatiky Technickej univerzity v Košiciach. Absolvoval postgraduálne štúdium na Znaleckom ústave elektrotechniky a informatiky Fakulty elektrotechniky a informatiky Slovenskej Technickej univerzity v Bratislave. V súčasnosti je študentom doktorandského štúdia na Fakulte managementu Univerzity Komenského v Bratislave. Je držiteľom mnohých profesijných certifikácií v oblasti informačnej bezpečnosti a riadenia rizika.

Až do odchodu z bankovej sféry viedol mnoho rokov pracovnú skupinu pre informačnú bezpečnosť Komisie pre bezpečnosť bánk a finančných operácií pri Slovenskej bankovej asociácii (SBA). Od roku 2013 sa podieľal na rozvojovom programe Európskej komisie Digitálna agenda. V implementácii Národnej koncepcie informatizácie verejnej správy SR sa zúčastňoval väčšiny aktivít súvisiacich s otázkami kybernetickej bezpečnosti. Spolupracoval na príprave väčšiny právnych predpisov týkajúcich sa kybernetickej bezpečnosti, tiež je spoluautorom Národnej stratégie kybernetickej bezpečnosti vrátane jej akčného plánu na roky 2021 — 2025.

Stál pri zrode IT Service Management fóra Slovensko (itSMF.SK), ktorého predsedom bol počas prvých troch volebných období. Je dlhoročným členom ISACA Slovensko (ISACA.SK), od roku 2019 aj členom Rady ISACA Slovensko. V roku 2018, spolu s niekoľkými ďalšími kolegami z odvetvia, založil Asociáciu kybernetickej bezpečnosti (AKB.SK) ako dobrovoľné a nezávislé občianske združenie, ktorého cieľom je reprezentovať slovenskú komunitu informačnej bezpečnosti. Na zakladajúcom valnom zhromaždení bol zvolený za jej predsedu.

Je známym prednášajúcim na slovenských i medzinárodných konferenciách, ako aj autorom niekoľkých publikácií a mnohých článkov s témou kybernetickej bezpečnosti a ochrany osobných údajov, príležitostne prednáša na vysokých školách. Práve zvyšovanie IT gramotnosti a neustále zvyšovanie kvality spolupráce bezpečnostných profesionálov považuje za svoj profesionálny cieľ.

• • • •

Obsah

1

Čo je to bezpečnosť?

Ľudia sú od informácií závislí. A nie je to len závislosť v zmysle pohľadov neustále uprených do mobilných telefónov. Závislosť od informácií sa týka mnohých spoločenských odvetví. Informácií je dnes viac než kedykoľvek v histórii. Informácie sú navyše spracúvané rýchlejšie a v obrovských objemoch, a to najmä elektronicky. Preto sa aj hrozby presúvajú do toho imaginárneho obláčika nazvaného „kybernetický priestor".

Závislosť od spätnej väzby

Organizmy, systémy, podsystémy, ekosystémy majú jednu spoločnú vlastnosť — vymieňajú si informácie. Tie následne podľa svojich vlastných potrieb spracovávajú, využívajú alebo si ich zapamätajú. Ak si jednotlivé komponenty akéhokoľvek systému či organizmu vymieňajú informácie, vznikajú medzi nimi informačné väzby, vzťahy. Spätná väzba (angl. „feedback") je taký systémový vzťah, ktorým sa vykoná prenos časti výstupnej informácie na pôvodný informačný vstup alebo na nový informačný vstup.

Systémy sa vzájomne ovplyvňujú a ich reakcie závisia len od spôsobu odovzdávania a prijímania informácií. To platí rovnako pre človeka, pre počítače, pre zvieratá, rastliny, astronomické objekty, ale aj pre výrobné linky, dopravu, vojenské operácie či pre riadenie štátov. Závislosť od spätnej väzby je univerzálna a platí pre celý známy i neznámy vesmír. **Kybernetika je veda o komunikácii dynamických systémov.**

Kybernetika s bezpečnosťou však súvisí iba nepriamo.

Životné priestory

Pojem **„priestor"** si najčastejšie spájame s fyzickým priestorom, ktorý sme schopní vnímať svojimi zmyslami. Až následne si pojem priestor stotožňujeme s inými abstraktnými prostrediami, v ktorých žijeme fyzicky či virtuálne — napríklad osobný priestor, verejný priestor, záujmový priestor, ekonomický priestor atď. Pri snahe o kategorizáciu priestorov a väčšiu úroveň detailu by sme z informatiky zachádzali až do filozofických vied.

Jestvuje mnoho rôznych definícií kybernetického priestoru. Podľa jednej z mnohých (takmer podobných) definícií je kybernetický priestor: *„komplexné prostredie, ktoré je výsledkom interakcie ľudí, softvéru a služieb na internete prostredníctvom technologických zariadení a sietí, ktoré sú k nemu pripojené a ktoré neexistujú v žiadnej fyzickej podobe"*. [1]

Zrejme prvou všeobecnou definíciou sa stala tá, ktorú použil v roku 1984 vo svojom kyberpunkovom sci-fi románe Neuromancer [1] americký spisovateľ William Ford Gibbson. V nasledujúcich rokoch sa tento výraz identifikoval najmä s počítačovými hrami a postupne prepájanými počítačovými sieťami. Časť románu Neuromancer, ktorá je zvyčajne citovaná v uvedenom kontexte, je nasledujúca: *„Kybernetický priestor. Hromadná halucinácia, ktorú denne prežívajú miliardy oprávnených v každom z národov, v ktorých sa deti učia matematické pojmy… Grafické zobrazenie údajov získaných z každého počítača v ľudskom systéme. Nepredstaviteľná zložitosť. Riadky svetla rozprestierajúce sa v medzipriestore mysle, zhlukov a súhvezdí dát. Ako ustupujúce*

svetlá miest…" Túto definíciu neskôr kritizoval aj samotný autor, ktorý ju komentoval vo filmovom dokumente No Maps for These Territories v roku 2000 slovami: „Všetko, čo som vedel o výraze ‚kybernetický priestor', keď som ho vytvoril, bolo, že sa mi to zdalo byť efektívnym, módnym výrazom. To slovo sa mi zdalo byť evokujúce a zároveň bezvýznamné. Bolo to čosi sugestívne, čo však nemalo skutočný sémantický význam, dokonca ani pre mňa samotného."

Takýto opis je, samozrejme, len umeleckou predstavou spisovateľa, navždy mu však bude patriť historické „čestné" miesto medzi definíciami kybernetického priestoru. Keď však chceme zostať v exaktných vedách, potom je vhodnejšie použiť formálne technické definície.

Podľa zákona [6] je kybernetickým priestorom *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.* Tu je potrebné povedať, že časť odbornej verejnosti túto definíciu kritizuje. Argumentuje tým, že časťou kybernetického priestoru nemajú byť ľudia, údajne z toho dôvodu, že kybernetický priestor sa tým nevhodne rozšíril o vzťahy a vzájomné interakcie ľudí, ktorí komunikujú s technickými komponentmi kybernetického priestoru. To je však príliš úzky, technokratický pohľad. Pokiaľ sa pozrieme na definície ISO alebo mnohé iné národné definície, nezostane než konštatovať, že definícia kybernetického priestoru použitá v zákone nie je menšinová a obstojí v porovnaní aj s inou než národnou legislatívou. Pokiaľ v roku 2016 uznali členské štáty Severoatlantickej aliancie kybernetický priestor za ďalšiu operačnú doménu[1)] **popri zemi, vzduchu, vode a vesmíre, kybernetický priestor sa stal piatou dimenziou, v ktorej aliancia predpokladá prípadný stret s nepriateľom.** Aj to je dostatočným dôvodom na predpoklad, že za súčasť kybernetického priestoru treba považovať aj interakcie ľudí s kybernetickým priestorom.

Definície kybernetického priestoru nájdeme v mnohých odborných slovníkoch aj v právnych predpisoch. Zo všetkých definícií vyplýva, že **predpona „kyber"** nadobúda zmysel vtedy a práve vtedy, ak je predmetom diskusie **v oblasti elektronického spracovania dát.** Dôležité je poznamenať, že elektronické spracúvanie si nesmieme zamieňať s digitálnym spracúvaním. To by znamenalo, že sa obmedzujeme len na spracovanie založené na znázorňovaní dát číslicami.

Zjednodušene sa dá tvrdiť, že v dnešnej informačnej dobe sa prídavné meno **„kybernetický"** chápe ako synonymum výrazu **„týkajúci sa kybernetického priestoru",** teda v prenesenom zmysle **„elektronicky spracúvaný".**

Bezpečnosť ako merateľný stav

Vráťme sa k nadpisu. Čo znamená „bezpečnosť"? Podľa slovníka [7] je bezpečnosť stav bez reálneho nebezpečenstva alebo hrozby. **Bezpečnosť nie je subjektívny pocit bezpečia, ale objektívny a merateľný stav bez nebezpečenstva.**

Pojem bezpečnosť pôvodne pochádza z latinského „securitas", čo znamenalo bezstarostnosť, bezpečnosť, istotu, pokoj, ochranu a zabezpečenie. V každom význame je to stav, v ktorom je chránený život, zdravie, prostredie či majetok.

Zaujímavé je chápanie bezpečnosti v rámci spoločenských vied. Tu je bezpečnosť vnímaná ako súhrn spoločenských vzťahov, ktoré upravuje právo a ktoré chránia záujmy fyzických a právnických osôb, záujmy spoločnosti a ústavné zriadenie. Je to najvyššia miera nebezpečenstva, ktorú spoločnosť v určitej oblasti života pripúšťa.

1) https://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=en

Na výslednú bezpečnosť sa dá pozerať dvoma spôsobmi: **objektívne** — ako na skutočnú absenciu hrozieb alebo **subjektívne** — ako na dôsledok absencie vnímania ohrozenia.

Bezpečnosť informácií je možné stanoviť a merať prostredníctvom jej troch základných kvalitatívnych atribútov:

- dôvernosť,
- dostupnosť,
- integrita.

Ich definície sú nasledovné.

Dôvernosť

Dôvernosť je určiteľná hodnota, do akej je prístup k informácii obmedzený pre vopred definovanú entitu, ktorá je efektívne oprávnená na prístup k tejto informácii. Hodnoty dôvernosti sa určujú pomocou tzv. klasifikačnej schémy, ktorá by mala obsahovať konvenciu klasifikácie, spôsob a kritériá na preskúmanie klasifikácie informácií. Klasifikácia poskytuje vlastníkom informácie indikáciu o zodpovedajúcej potrebe ochrany informácie. Požiadavka sa zvyčajne rieši vytvorením niekoľkých rôznych klasifikačných stupňov informácií, ktoré majú podobné potreby na ochranu. Bezpečnostné opatrenia sú potom aplikované tak, aby sa vzťahovali na celú skupinu informácií označených príslušným klasifikačným stupňom.

Podľa definície § 3 písm. e) zákona je dôvernosťou *záruka, že údaj alebo informácia nie je prezradená neoprávneným subjektom alebo procesom*. Norma STN EN ISO/IEC 27000:2023 [3] definuje dôvernosť ako *„vlastnosť, že informácia nie je sprístupnená alebo prezradená neoprávneným osobám, entitám alebo procesom“*. Definícia dôvernosti podľa § 3 písm. e) zákona je podľa nášho názoru sémanticky v súlade s definíciou uvedenou v ISO.

Dostupnosť

Dostupnosť je atribút spoľahlivosti informácie a zároveň aj bezpečnostná požiadavka, ktorá je paradoxne typicky ako jediná zahrnutá do zmlúv o úrovni poskytovaných služieb (SLA). Dôvodom je zrejme fakt, že dostupnosť je možné pomerne presne merať a na základe nej stanovovať spoľahlivosť informácie, presnejšie spoľahlivosť spracovateľskej operácie. Podľa STN EN ISO/IEC 27000:2023 [3] je dostupnosť *„vlastnosť (procesu, systému alebo informácie) byť dosiahnuteľný a použiteľný na požiadanie oprávnenej entity“*. Dostupnosť sa zvyčajne sleduje v mesačnom intervale a v agregovanej hodnote v rámci jedného roka. Na výpočet dostupnosti služby v sledovanom období sa používa funkcia:

$$[(T_s - T_n) / T_s] * 100;$$

kde T_s je obdobie, počas ktorého má byť služba v zmysle SLA v danom mesiaci poskytovaná a T_n je obdobie, počas ktorého bolo riadne poskytovanie služby obmedzené. Doby a obdobia sa počítajú na celé aj začaté časové hodnoty (napr. minúty alebo hodiny — podľa požiadavky na presnosť sledovania dostupnosti). Dostupnosť sa potom vyjadruje v percentách zaokrúhlených na dve desatinné miesta.

Definícia dostupnosti podľa § 3 písm. f) zákona, podľa ktorého dostupnosťou je záruka, že údaj alebo informácia je pre používateľa, informačný systém, sieť alebo zariadenie prístupné vo chvíli, keď je údaj a informácia potrebná a požadovaná, je podľa nášho názoru sémanticky v súlade s definíciou uvedenou v ISO. Pojem dostupnosť sa v Smernici NIS nenachádza, napriek tomu nepovažujeme uvedenie tohto pojmu v zákone za nadbytočné, skôr by sa absencia výkladu významu tohto bezpečnostného atribútu mohla vyčítať autorom Smernice NIS.

Integrita

Integrita je určiteľná hodnota, do akej sú informácie aktuálne a bezchybné. Vlastnosťami integrity sú úplnosť, celistvosť a správnosť informácií. A to je aj definíciou podľa STN EN ISO/IEC 27000:2023 [3]: *„vlastnosť presnosti a úplnosti“*.

Integrita je v praxi meraná napríklad na počet chybných záznamov z celej množiny záznamov, prípadne v stanovenom časovom intervale. Definícia v zákone správne rozširuje význam tohto pojmu aj na možné narušenie celistvosti, poškodenie systému alebo zmenu konfigurácie. Podľa § 3 písm. g) zákona je integritou záruka, že bezchybnosť, úplnosť alebo správnosť informácie neboli narušené. Opäť podľa nášho názoru je táto definícia sémanticky v súlade s definíciou uvedenou v ISO.

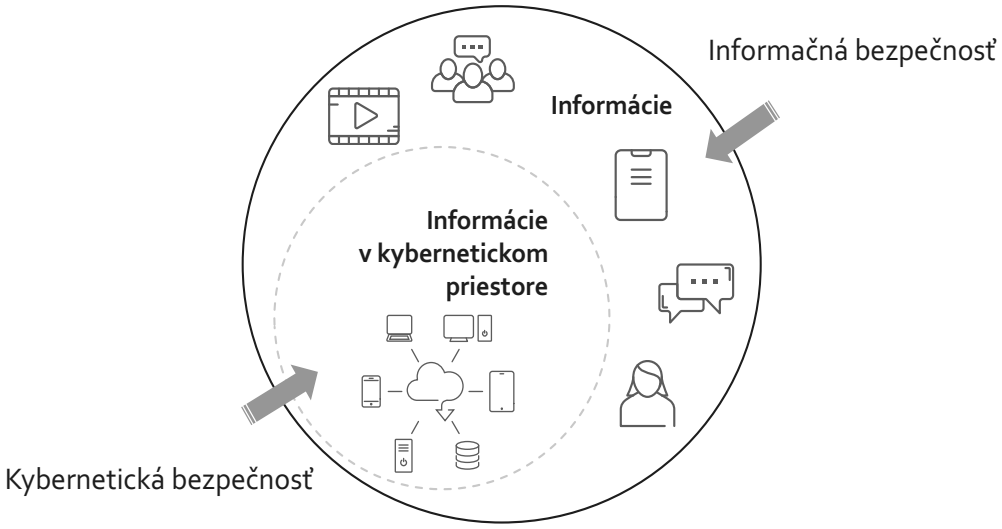
Informačná alebo kybernetická bezpečnosť?

Oba výrazy sú správne. Dôležité je pochopiť, ako spolu súvisia.

Informačná bezpečnosť znamená bezpečnosť informácií. To je situácia, v ktorej sú informácie považované za bezpečné. Je to časť informačného manažmentu bez ohľadu na fyzikálny stav dát, bez ohľadu na ich formát, bez ohľadu na spôsob ich interpretácie a bez ohľadu na médium, prostredníctvom ktorého sú uchovávané a prenášané. Podľa definície: **informačná bezpečnosť** je zachovanie dôvernosti, integrity a dostupnosti **informácií.** [ISO/IEC 27032, čl. 2.33]. [1]

Na druhej strane, **kybernetická bezpečnosť** je zachovanie dôvernosti, integrity a dostupnosti **informácií v kybernetickom priestore** [ISO/IEC 27032, čl. 4.20] [1].

Ilustrácia č. 1: Vzťah informačnej a kybernetickej bezpečnosti

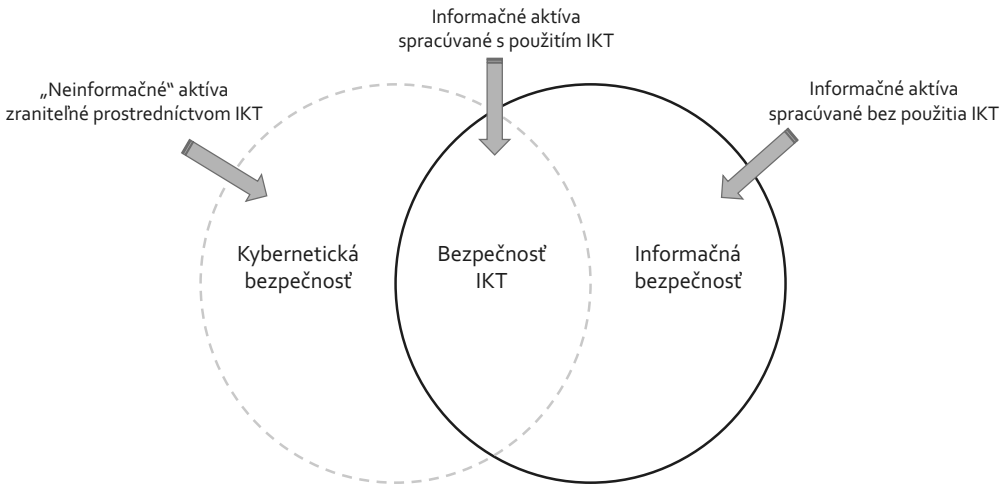


Oba druhy bezpečnosti majú rovnaký cieľ — ochranu informácií. Až na to, že **bezpečnosť „kybernetická“ sa týka len informácií v kontexte kybernetického priestoru.**

Ak by sme sa mali vyjadriť exaktne, tak „**kybernetická bezpečnosť“ je podmnožinou množiny „informačná bezpečnosť“ preto, že všetky jej prvky sú zároveň prvkami množiny „informačná bezpečnosť“,** zatiaľ čo inverzne toto tvrdenie neplatí.

Niektorí autori [4] opisujú kybernetickú bezpečnosť nie ako podmnožinu informačnej bezpečnosti, ale ako prienik dvoch iných množín — informačných aktív a „neinformačných“ aktív v zmysle nasledujúceho grafu.

Ilustrácia č. 2: Kybernetická bezpečnosť v kontexte „neinformačných“ aktív



Zaujímavý názor, ale len vtedy, ak ho použijeme ako doplnkovú ilustráciu. Toto zobrazenie totiž obchádza dva fakty: takmer všetky definície popisujú kybernetický priestor abstraktne, bez potreby jeho fyzického vymedzenia a tiež, že kybernetická bezpečnosť sa ako odbor zapodieva zachovaním dôvernosti, integrity a dostupnosti INFORMÁCIÍ. „Neinformačné aktíva“, samozrejme, už podľa svojho pomenovania, nie sú informáciami. Informačné aktíva, ktoré sú zároveň označované za neinformačné, je zjavný oxymoron.

Kyberbezpečnosť sa týka opatrení, ktoré by zainteresované strany mali podniknúť na zaručenie bezpečnosti informácií v kyberpriestore. Kyberbezpečnosť sa opiera o rôzne subdomény — aplikačnú bezpečnosť, sieťovú bezpečnosť, internetovú bezpečnosť, bezpečnosť priemyselných riadiacich systémov, bezpečnosť kritickej infraštruktúry — ako o svoje základné stavebné kamene. Kybernetická bezpečnosť sa, samozrejme, týka aj tých najcitlivejších oblastí vrátane národnej obrany, vyšetrovania počítačovej kriminality, ochrany života a zdravia občanov.

Nemýľme si objekt so subjektom

Ak chceme nájsť hranicu medzi tým, čo je a čo už nie je kybernetická bezpečnosť, musíme rozlišovať, či sa na definíciu kybernetickej bezpečnosti pozeráme z pohľadu subjektu, teda pozorovateľa, ktorého sa elektronicky spracúvané informácie týkajú, alebo z pohľadu objektu, teda predmetu pozorovania. Dáta v tomto vzťahu predstavujú OBJEKT, zatiaľ čo ľudia, ktorí vnímajú dopad hrozieb, sú SUBJEKT pozorovania. Aj v právnej teórii je objekt predmetom či cieľom, ktorý má byť právnym vzťahom v súvislosti s predmetom dosiahnutý, upravený. Za objekt sa považujú statky, aktíva, prípadne stav týchto prvkov. V tomto prípade tzv. informačné aktíva a ich prípadný stav či charakteristika (bezpečnosť alebo jej absencia).

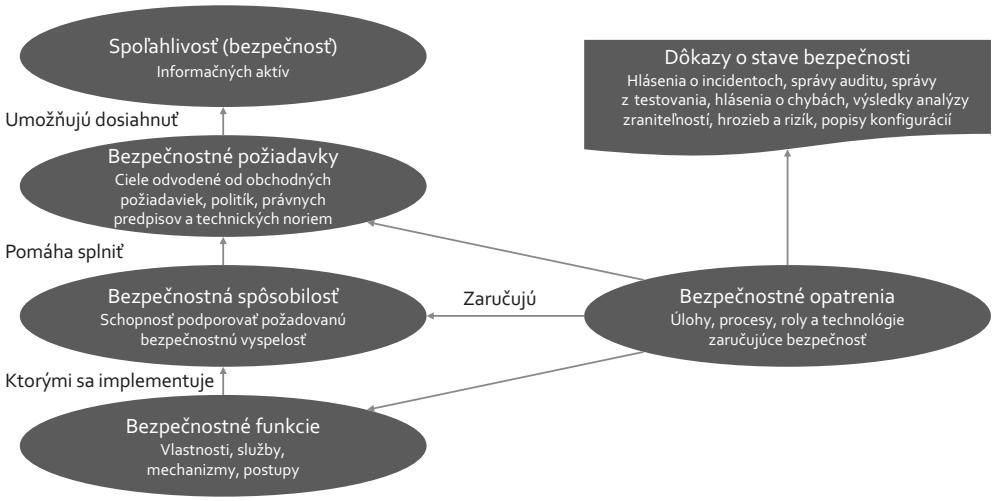
Rozdielne ponímanie odborovej kategorizácie bezpečnosti spočíva v chybnom presadzovaní pohľadu najmä z pozície subjektu a v určitom vedomom potláčaní podstaty či

existencie objektu. **Objektom ochrany je faktické zaručenie bezpečnosti informácií, nie pocit bezpečia vlastníkov informácií.**

Abstraktný model bezpečnosti

V opise artefaktov, ktorými chceme pomenovať jednotlivé fázy, činnosti a stavy v bezpečnosti, je možné inšpirovať sa z normy NIST SP 800-53 Security and Privacy Controls [5], ktorá v jednej zo svojich verzií navrhla schému vzťahov medzi jednotlivými komponentmi a pojmami v bezpečnosti spojenými do tzv. modelu dôveryhodnosti.

Ilustrácia č. 3: Vzťah medzi kľúčovými komponentmi v modeli bezpečnosti



Vzťahy medzi kľúčovými komponentmi v modeli bezpečnosti sa dajú v inverznom poradí slovne popísať nasledujúcim spôsobom:

- v prvom kroku k bezpečnosti (t. j. spoľahlivosti) informačných aktív by mali vlastníci týchto aktív transparentne definovať **bezpečnostné požiadavky,**
- bezpečnostné požiadavky by mali byť odvodené od cieľov organizácie a odvodené od prevádzkových požiadaviek, od požiadaviek právnych predpisov a na základe technických noriem. **Bezpečnostné požiadavky sa typicky definujú v bezpečnostnej stratégii.** Bezpečnostnou stratégiou sa zároveň deklaruje záväzok vedenia organizácie k podpore informačnej a kybernetickej bezpečnosti v organizácii,
- aby sa dosiahla požadovaná vyspelosť ochrany informačných aktív a aby mohli byť splnené ciele stanovené v bezpečnostných požiadavkách, organizácia musí **zaručiť určité spôsobilosti** v oblasti informačnej a kybernetickej bezpečnosti,
- spôsobilosti je možné dosiahnuť len reálnym konaním a zmenami vo fyzickom svete. Pre dosiahnutie spôsobilostí je potrebné aplikovať určité **bezpečnostné funkcie,** t. j. nastaviť vlastnosti prostredia, spustiť poskytovanie určitých služieb, implementovať bezpečnostné mechanizmy, stanoviť postupy týkajúce sa ochrany informačných aktív,
- bezpečnostnými opatreniami sa nazývajú práve tieto úlohy, procesy, roly a technológie, ktoré zaručujú plnenie potrebných bezpečnostných funkcií, a teda sprostredkovane bezpeč-

nostných spôsobilostí a bezpečnostných požiadaviek stanovených stratégiou informačnej a kybernetickej bezpečnosti.

Hlásenia o incidentoch, správy auditu, správy z testovania, hlásenia o chybách, výsledky analýzy zraniteľností, hrozieb a rizík, popisy konfigurácií, riadenie súladu a vnútorná kontrola sú často chybne zamieňané s pojmom opatrenie. Avšak tieto typy aktivít, procesov a výstupov nie sú podľa technických noriem bezpečnostným opatrením, ale **dôkazmi o stave bezpečnosti a procesmi pre overovanie efektivity bezpečnostných opatrení** (pozri napríklad spomínanú NIST SP 800-53 Security and Privacy Controls [5]).

Kyberbezpečnosť ako moderný výraz

Pokiaľ ide o politikov a manažérov, u nich mnohokrát nadužívanie výrazu „kyber“ spočíva najmä v marketingu. Skrátka, výraz „kybernetický“, ako aj predpony „kyber“ či „cyber“ znejú príťažlivo a prednášajúceho to v očiach poslucháčov robí odborne zdatnejším.

Áno, sme závislí od informačných a komunikačných technológií. Korelácia však nie je kauzalita a bolo by nekorektné tvrdiť, že predponu „kybernetický“ alebo „cyber“ použijeme pri každej ľudskej činnosti, pre ktorú je dôležité počítačové spracovanie dát.

Prečo je teda časť bezpečnosti „kybernetická“? Pretože sa týka ochrany údajov a informácií v kybernetickom priestore.

• • • •

2

Úvod k problematike bezpečnostných opatrení

Bezpečnostnými opatreniami sú úlohy, procesy, roly a technológie uplatnené v organizačnej, personálnej a technickej oblasti. Bezpečnostné opatrenia poskytujú záruky na získanie bezpečnostných spôsobilostí, najmä prostredníctvom bezpečnostných funkcií, vlastností, služieb, mechanizmov a definovaných postupov. Následne dosiahnuté bezpečnostné ciele umožňujú získať záruku, že komponenty informačnej architektúry môžu byť považované za dôveryhodné a spoľahlivé.

Čo znamená slovo „opatrenia“?

Pojem opatrenia nie je možné úzko obmedziť len na implementáciu bezpečnostných technológií. Ale na druhej strane — pojem opatrenia taktiež nevymedzuje iba konanie v oblasti právnej, procesnej alebo organizačnej. Zákon správne uvádza, že **bezpečnostnými opatreniami sú úlohy, procesy, roly a technológie v organizačnej, personálnej a technickej oblasti.**

Bezpečnostné alebo ochranné opatrenia (z anglického: „measures“ alebo „controls“) — v kontexte zákona sa tento výraz používa pre praktiky, postupy, procedúry a mechanizmy technického alebo procesného charakteru, ktoré môžu pomôcť znížiť známe zraniteľnosti, chrániť systém alebo organizáciu pred kybernetickými hrozbami. V prípade, že sa hrozba už uplatnila a spôsobila škodlivú udalosť, majú bezpečnostné opatrenia túto udalosť odhaliť a obmedziť jej vplyv. Následné bezpečnostné opatrenia majú umožniť zotavenie systému alebo organizácie zo škodlivej udalosti, resp. incidentu. Pojem opatrenia sa často používa aj v zmysle právneho konania, ktoré potenciálne zaručí odškodnenie strát vyvolaných škodlivou udalosťou.

Výraz „opatrenia“ je v kontexte zákona komplexným pojmom zahrnujúcim akékoľvek konanie, ktorého účelom je podpora spôsobilosti prevádzkovateľa zaručiť a riadiť informačnú a kybernetickú bezpečnosť, zaručiť naplnenie potrebných bezpečnostných funkcií a zaručiť bezpečnostné spôsobilosti a bezpečnostné požiadavky stanovené prijatou stratégiou informačnej a kybernetickej bezpečnosti organizácie.

Na tomto mieste treba zdôrazniť, že výrazy **„prevádzkovateľ“, „organizácia“, „spoločnosť“** alebo **„podnik“** sú v celom texte tejto publikácie používané ako **synonymá pre povinné osoby.** Podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti v znení neskorších predpisov [6] sa pre povinnú osobu niekedy použije aj výraz **prevádzkovateľ základnej služby** (alebo len skratka **„PZS“**). Na niektorých miestach sú výrazy **„prevádzkovateľ“, „organizácia“, „spoločnosť“** alebo **„podnik“** použité ako synonymá pre povinnú osobu podľa Všeobecného nariadenia o ochrane údajov [8], resp. zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov [9].

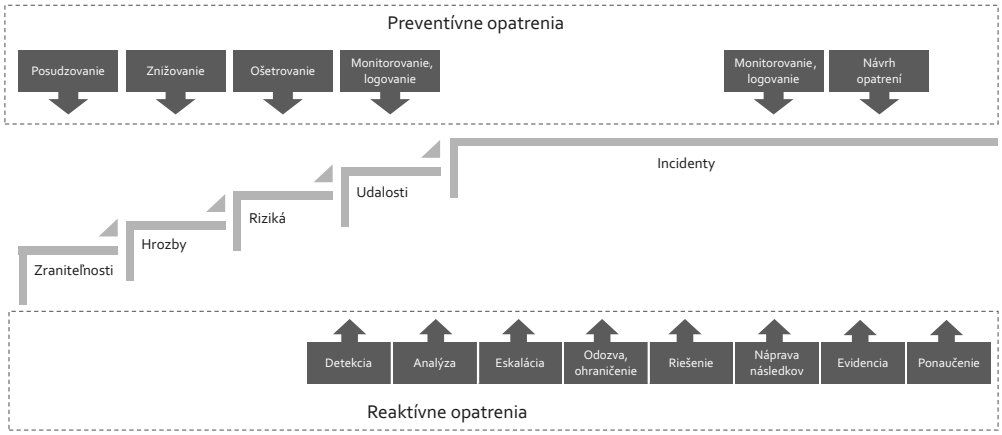
Bezpečnostné opatrenia môžu pomôcť preventívne predchádzať hrozbám, znížiť známe zraniteľnosti, chrániť systém alebo organizáciu pred kybernetickými hrozbami aj v prípade, že sa hrozba už uplatnila a jej následkom bola škodlivá udalosť.

Úlohou aplikovaných **preventívnych bezpečnostných opatrení** je takéto udalosti včas odhaliť a obmedziť ich negatívny vplyv. Cieľom následných **reaktívnych bezpečnostných opatrení** je umožniť zotavenie systému alebo organizácie zo škodlivej udalosti, resp. z incidentu

a zabezpečiť zaručenie odškodnenia strát vyvolaných škodlivou udalosťou alebo získať dôkazné prostriedky pre pokračovanie v právnom konaní smerujúcom k potrestaniu páchateľov, vymoženiu škody alebo napr. vyvodenie zodpovednosti v rámci pracovnoprávneho vzťahu.

Preventívne a reaktívne opatrenia bezpodmienečne nenasledujú v tomto poradí. Niektoré opatrenia, ktoré sú vykonávané v rámci reakcie na incident, riešia opäť prevenciu — napríklad ponaučenie z incidentu, úprava architektúry, dodatočná rekonfigurácia systémov, implementácia rozšírených opatrení na zníženie rizika atď. Postupnosť opatrení sa dá schematicky zobraziť na časovej osi.

Ilustrácia č. 4: Postupnosť preventívnych a reaktívnych opatrení



Aj v súvislosti s vyššie uvedenou skúsenosťou autori novej verzie normy ISO/IEC 27002:2022 *Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia — Opatrenia informačnej bezpečnosti* okrem preventívnych a reaktívnych bezpečnostných opatrení predstavili nové rozdelenie opatrení z pohľadu toho, kedy a akým spôsobom opatrenie modifikuje riziko v kontexte výskytu incidentu. Podľa tejto normy sú opatrenia rozdelené nasledovne:

- **preventívne** (#preventive) — opatrenia, ktoré majú zabrániť vzniku bezpečnostných incidentov,
- **detektívne** (#detective) — opatrenia, ktoré majú nastať v prípade výskytu incidentu a slúžia na zistenie jeho príčin,
- **nápravné** (#corrective) — opatrenia, ktoré majú nastať po výskyte incidentu a slúžia na zotavenie systému alebo organizácie z incidentu.

Spoliehajúc sa na súčasné dobré vzťahy zákonodarcu s odbornou verejnosťou je možné optimisticky predpokladať, že sa zákonodarca bude týmto novým rozdelením inšpirovať v novelizácii zákona [6].

Generické rozdelenie opatrení

Prax informačnej a kybernetickej bezpečnosti delí opatrenia podľa ich podstaty na:

- **technické opatrenia —** t. j. opatrenia na zníženie bezpečnostných rizík pomocou prostriedkov fyzickej a technologickej povahy,
- **organizačné opatrenia —** t. j. opatrenia na zníženie bezpečnostných rizík prostredníctvom zmien procesov pomocou úpravy dokumentácie procesov.

Zvláštnou podkategóriou organizačných opatrení sú tzv. **personálne opatrenia** ako typ organizačných opatrení týkajúcich sa riadenia ľudských zdrojov. Len pre zaujímavosť, zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v § 6 ods. 4 definuje personálnu bezpečnosť ako systém opatrení súvisiacich s výberom, určením a kontrolou osôb, ktoré sa môžu v určenom rozsahu oboznamovať s utajovanými skutočnosťami.

Rozdelenie opatrení na technické a organizačné má svoj význam najmä v plánovaní finančného rozpočtu. **Technické opatrenia sú zvyčajne predmetom investičnej časti plánovaných nákladov** (tzv. CAPEX, Capital Expenditures) — čo sú typicky peňažné prostriedky vynaložené na nákup kapitálových (investičných) statkov, ako sú napríklad stroje a zariadenia, pozemky, budovy, technológie a pod. **Organizačné opatrenia sú predmetom prevádzkovej časti plánovaných nákladov** (tzv. OPEX, Operating Expenditures) — čo sú typicky peňažné prostriedky vynaložené na zaistenie bežných činností. Medzi takéto náklady patria napríklad náklady na služby, materiál, mzdy, údržbu, školenia a pod.

Opatrenia sa zároveň delia na tri kategórie vo vzťahu k životnému cyklu informačného aktíva. Tento prístup je podstatný najmä v kontexte procesu riadenia rizík:

- **existujúce opatrenia** (z angl. Existing controls) — opatrenia inherentne zabudované už v čase návrhu, resp. implementácie systému,
- **rozšírené (tiež „vylepšené") opatrenia** (z angl. Enhanced controls) — aplikované na implementovaný systém s cieľom ošetrenia rizika identifikovaného už v rámci bežnej prevádzky systému; typicky ich navrhuje manažér kybernetickej bezpečnosti alebo jeho tím,
- **dodatočné opatrenia** (z angl. Additional, Complementary controls) — odporúča ich zvyčajne interný alebo externý audítor v záverečnej správe auditu s cieľom ošetrenia rizika identifikovaného v rámci výkonu auditu.

Efektívnu bezpečnosť je možné dosiahnuť len pomocou kombinácie rôznych technických a organizačných opatrení. Toto tvrdenie sa dá ilustrovať na príklade požiadavky na riadenie digitálnych identít. Organizácii nepomôže, ak bude mať zakúpený najdrahší a najrobustnejší systém IAM[2)] (t. j. implementované technické opatrenie). Bez vopred navrhnutej politiky riadenia identít samotný systém úroveň bezpečnosti nezvýši. Systém IAM totiž potrebuje byť najprv „nakŕmený" informáciami o tom, aké sú požadované používateľské roly, do akých systémov majú byť riadené prístupy, ktorá rola má aké práva a ktorému zamestnancovi majú byť pridelené ktoré roly. Avšak platí to aj inverzne. Ak aj nejaký špičkový konzultant navrhne dokonalú, rozsiahlu a detailnú politiku riadenia identít (t. j. bude implementované organizačné opatrenie), v organizácii s väčším počtom používateľov nie je šanca nasadiť a vynútiť platnú politiku manuálne. Organizácia sa nevyhne potrebe implementácie systému IAM.

Právne zakotvenie bezpečnostných opatrení

Zhrňme si stručne právne normy a ich ponímanie definície bezpečnosti a jej atribútov vrátane toho, ako bezpečnosť dosiahnuť v kontexte ochrany informácií.

Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti v znení neskorších predpisov [6] (v celom ďalšom texte publikácie len **„zákon"**) je transpozíciou smernice 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 (skrátene len **„smernica NIS"**). V čase vydania tejto publikácie je už účinná novelizovaná verzia Smernice zo dňa 14. decembra 2022

2) IAM systém — systém riadenia prístupov a identít (z angl. Identity and Access Management).

o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (skrátene len „**smernica NIS 2**“) [10].

Cieľom Smernice NIS, a teda aj zákona o kybernetickej bezpečnosti je zaručiť úroveň spôsobilostí v kybernetickej bezpečnosti, ktoré budú postačujúce na zaručenie vysokej úrovne bezpečnosti sietí a informačných systémov v Únii.

„**Spôsobilosť**“ (z angl.: „capability“) je osobitná schopnosť, ktorú môže organizácia vlastniť alebo vykonávať s cieľom dosiahnuť konkrétny účel.

Podľa rámca informačnej architektúry TOGAF9 [11] je **služba** (z angl.: „service“) určitá činnosť zabezpečovaná **pomocou explicitne definovaných komponentov**, ktorými je podporovaná **niektorá spôsobilosť** spoločnosti a prostredníctvom ktorej je **dosahovaný konkrétny účel**.

Tým komponentom, ktorým je podporovaná spôsobilosť spoločnosti a prostredníctvom ktorého je dosahovaný konkrétny účel, je podľa Smernice NIS2 [10] **„sieť a informačný systém“.** Smernica NIS2 [10] definuje „sieť a informačný systém“ nasledovne:

a) elektronická komunikačná sieť v zmysle vymedzenia v článku 2 bodu 1 Smernice EÚ 2018/1972, ktorou sa stanovuje európsky kódex elektronických komunikácií [11],

b) každé zariadenie alebo skupina vzájomne prepojených alebo súvisiacich zariadení, z ktorých jedno alebo viaceré vykonávajú automatické spracúvanie digitálnych údajov na základe programu, alebo

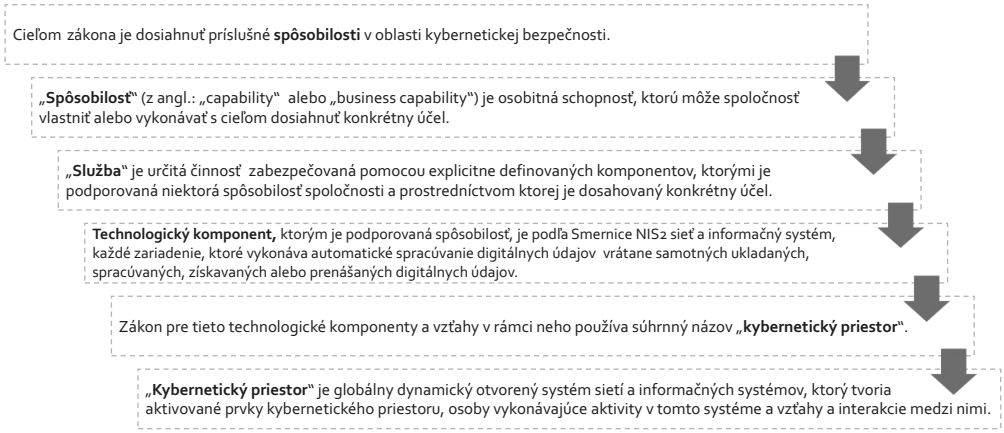
c) digitálne údaje, ktoré sa ukladajú, spracúvajú, získavajú alebo prenášajú prostredníctvom prvkov uvedených v písmenách a) a b) na účely ich prevádzkovania, používania, ochrany a udržiavania.

Elektronickou komunikačnou sieťou podľa Smernice EÚ 2018/1972 [11] sú *prenosové systémy, ktoré môžu ale nemusia byť založené na trvalej infraštruktúre alebo centralizovanej administratívnej kapacite, prípadne prepájacie alebo smerovacie zariadenie a iné prostriedky vrátane neaktívnych prvkov siete, ktoré umožňujú prenos signálov po vedení, rádiovými, optickými alebo inými elektromagnetickými prostriedkami, vrátane družicových sietí, pevných (s prepájaním okruhov a paketov vrátane internetu) a mobilných sietí, elektrických káblových systémov v rozsahu, v ktorom sa používajú na prenos signálov, sietí používaných na rozhlasové a televízne vysielanie a sietí káblovej televízie bez ohľadu na typ prenášaných informácií.*

Je potrebné si všimnúť, že podľa Smernice NIS2 [10] je komponentom aj *každé zariadenie alebo skupina vzájomne prepojených alebo súvisiacich zariadení, z ktorých jedno alebo viaceré vykonávajú automatické spracúvanie digitálnych údajov na základe programu*. Zároveň, podľa ustanovenia čl. 6 ods. 1 písm. c) Smernice NIS2 [10], sa za komponent informačnej architektúry, ktorým je podporovaná niektorá spôsobilosť, považujú aj logické komponenty, t. j. *digitálne údaje, ktoré sa ukladajú, spracúvajú, získavajú alebo prenášajú prostredníctvom prvkov uvedených v písmenách a) a b) na účely ich prevádzkovania, používania, ochrany a udržiavania.* Zjednodušene povedané, za komponenty informačnej architektúry sa podľa Smernice NIS2 [10] považuje hardvér aj softvér.

Cieľ zákona [6] je derivovaný zo smernice NIS a týmto cieľom je dosiahnuť príslušné spôsobilosti v oblasti kybernetickej bezpečnosti. **Spôsobilosti možno dosiahnuť zmenami jestvujúcich zvyklostí, postupov, procedúr alebo technológií a architektúry.**

Ilustrácia č. 5: Aplikácia cieľov zákona



Bezpečnostné opatrenia poskytujú záruky na získanie bezpečnostných spôsobilostí najmä prostredníctvom bezpečnostných funkcií, vlastností, služieb, mechanizmov a definovaných postupov. Dosiahnuté bezpečnostné ciele umožňujú získať záruku, že komponenty informačnej architektúry môžu byť považované za dôveryhodné a spoľahlivé.

Spoľahlivosť informácie je determinovaná tromi jej základnými bezpečnostnými atribútmi: dôvernosťou, dostupnosťou a integritou. Z toho vyplýva, že opatrenia zaručujúce bezpečnosť (t. j. spoľahlivosť) komponentov informačnej architektúry by mali smerovať najmä k zabezpečeniu dôvernosti, dostupnosti a integrity.

Ak by sme vyššie uvedené mali aplikovať na informačnú architektúru, vznikne výraz **„bezpečnostná architektúra",** ktorý je chápaný ako vymedzenie okolia siete a informačného systému a vzťah okolia siete informačného systému k možnému narušeniu bezpečnosti.

Bezpečnostná architektúra je medziodborová problematika, ktorá sa tiahne naprieč celou podnikovou architektúrou. Možno ju opísať ako ucelený súbor pohľadov a artefaktov informačnej a kybernetickej bezpečnosti, ochrany súkromia a operačného rizika vrátane bezpečnostných cieľov a bezpečnostných služieb. Z už spomínanej metodiky TOGAF9 [11] bol odvodený rámec bezpečnostnej architektúry Sherwood Applied Business Security Architecture so skratkou SABSA [13]. V tomto rámci existuje návrh matice, ktorá zovšeobecňuje jednotlivé artefakty informačnej architektúry (pozri tabuľku č. 1).

Na základe tejto miery abstrakcie je možné určiť, ktoré komponenty informačnej architektúry je potrebné posúdiť a príslušným spôsobom ošetriť, pokiaľ je cieľom dosiahnuť stav, v ktorom je možné považovať informácie za dôveryhodné a spoľahlivé, t. j. zabezpečené.

Opatrenia podľa zákona o kybernetickej bezpečnosti

Zákon o kybernetickej bezpečnosti aj po novelizácii, v znení účinnom od 1. 8. 2021, naďalej zachováva princíp technickej neutrality. I keď § 20 ods. 3 rozoberá jednotlivé bezpečnostné opatrenia, v skutočnosti sú v tomto ustanovení uvedené celé oblasti bezpečnostných opatrení, ktoré je možné vykonať rôznymi nástrojmi, mechanizmami alebo postupmi. Dá sa dokonca tvrdiť, že **v § 20 ods. 3 nie sú uvedené bezpečnostné opatrenia, ale tzv. bezpečnostné ciele.** Tie by mali umožniť organizácii splniť všetky ciele hlavných činností, a to implementáciou procesov a systémov s náležitým zvážením kybernetických bezpečnostných rizík týkajúcich

Tabuľka č. 1: Matica artefaktov IB/KB podľa metodiky SABSA

	Aktívum (Čo)	Motivácia (Prečo)	Proces (Ako)	Ľudia (Kto)	Umiestnenie (Kde)	Čas (Kedy)
Kontext	Predmet činnosti	Model rizika	Model procesu	Organizačné usporiadanie	Geografia	Časové závislosti základnej prevádzkovej činnosti
Koncept	Profil činnosti	Bezpečnostné ciele	Bezpečnostná stratégia a architektonické vrstvy	Model bezpečnostných entít a stanovenie dôveryhodného rámca	Model bezpečnostných domén	Termíny a životnosť prvkov súvisiacich s bezpečnosťou
Logické členenie	Model informácií	Bezpečnostné politiky	Služby bezpečnosti	Schéma entít a profily právomocí	Definícia bezpečnostných domén a ich prepojenia	Cyklus bezpečnostných operácií
Fyzické členenie	Dátový model	Bezpečnostné štandardy	Bezpečnostné mechanizmy	Používatelia, aplikácie a používateľské rozhrania	Platformy a sieťová infraštruktúra	Výkon riadiacej štruktúry
Komponenty	Detailné dátové štruktúry	Bezpečnostné procedúry a návody	Bezpečnostné produkty a nástroje	Identity, funkcie, roly, ACL	Procesy, uzly, adresy, protokoly	Časovanie a postupnosť aktivít
Prevádzka	Zaistenie kontinuity činností	Riadenie operačného rizika	Riadenie a podpora služieb bezpečnosti	Riadenie a podpora používateľov a aplikácií	Bezpečnosť objektov, sietí a platforiem	Rozvrh výkonu bezpečnostných operácií

sa organizácie, jej partnerov a zákazníkov. Plnenie týchto oblastí bezpečnostných opatrení je možné dosiahnuť zmenou spôsobilostí, najmä zmenami zvyklostí, postupov, procedúr alebo technológií a architektúry. Je výhradne na rozhodnutí prevádzkovateľa základných služieb, aký rozsah bezpečnostných opatrení sa rozhodne implementovať vo svojom prostredí. Podstatou neskoršieho posúdenia zo strany audítora je efektivita bezpečnostných opatrení, teda posudzovanie úrovne dosiahnutých spôsobilostí.

Zákon [6] v § 20 ods. 3 stanovuje, že bezpečnostné opatrenia sa prijímajú najmä pre určité oblasti. V nasledujúcej tabuľke je uvedené mapovanie a prelínanie jednotlivých oblastí v znení zákona účinného pred a po 1. 8. 2021.

Tabuľka č. 2: Mapovanie oblastí opatrení v znení zákona účinného pred a po 1. 8. 2021

Znenie od 1. 1. 2019 do 31. 7. 2021	Znenie od 1. 8. 2021	Zmena
a) organizácia informačnej bezpečnosti	a) organizácia kybernetickej bezpečnosti a informačnej bezpečnosti	Požiadavka na vytvorenie roly manažéra KB je navyše riešená v § 20 ods. 4 písm. a).
b) riadenie aktív, hrozieb a rizík	b) riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti	Z oblasti bolo vyňaté riadenie aktív, to je však natívnou súčasťou procesu riadenia rizík.
c) personálna bezpečnosť	c) personálna bezpečnosť	Bez zmeny.
d) riadenie dodávateľských služieb, akvizície, vývoja a údržby informačných systémov	e) riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami	Akvizícia, vývoj a údržba sietí a informačných systémov sa presúva do samostatného ustanovenia v písm. j).
e) technických zraniteľností systémov a zariadení	g) hodnotenie zraniteľností a bezpečnostných aktualizácií	Zmena v názve oblastí opatrení.
f) riadenie bezpečnosti sietí a informačných systémov	i) sieťová a komunikačná bezpečnosť	Zmena v názve oblastí opatrení — zdôraznenie požiadavky na sieťovú bezpečnosť (z angl. „network security“).
g) riadenie prevádzky	f) bezpečnosť pri prevádzke informačných systémov a sietí	Zmena v názve oblasti opatrení — zdôraznenie požiadavky na prevádzkovú bezpečnosť (z angl. „operations security“).
h) riadenie prístupov	d) riadenia prístupov	Bez zmeny.
i) kryptografické opatrenia	n) kryptografické opatrenia	Bez zmeny.
j) riešenie kybernetických bezpečnostných incidentov	m) riešenie kybernetických bezpečnostných incidentov	Bez zmeny.
k) monitorovanie, testovania bezpečnosti a bezpečnostných auditov	p) audit, riadenie súladu a kontrolné činnosti	Zmena v názve a zároveň presun požiadaviek na monitorovanie ustanovenia v písm. k).
l) fyzická bezpečnosť a bezpečnosť prostredia	l) fyzická bezpečnosť a bezpečnosť prostredia	Bez zmeny.
m) riadenie kontinuity procesov	o) kontinuita prevádzky	Zmena v názve oblasti opatrení.

Znenie od 1. 1. 2019 do 31. 7. 2021	Znenie od 1. 8. 2021	Zmena
Pôvodne čiastočne j) riešenie kybernetických bezpečnostných incidentov	k) zaznamenávanie udalostí a monitorovanie	Rozdelenie pôvodného písm. j) riešenia kybernetických bezpečnostných incidentov.
Pôvodne d) riadenie dodávateľských služieb, akvizície, vývoja a údržby informačných systémov	j) akvizícia, vývoj a údržba informačných sietí a informačných systémov	Rozdelenie pôvodného písm. d) riadenie dodávateľských služieb, akvizície, vývoja a údržby informačných systémov (pozn.: legislatívno-technická chyba v názve — nie „informačných sietí“, len „sietí“).
Pôvodne e) technických zraniteľností systémov a zariadení	h) ochrany proti škodlivému kódu	Rozdelenie pôvodného písm. e) oblasť technických zraniteľností systémov a zariadení.

Zmena názvov oblastí v znení zákona [6] platného od 1. 8. 2021 bola úmyslom zákonodarcu s cieľom zladiť názvoslovie používané v zákone o kybernetickej bezpečnosti a v zákone č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov [16]. Presnejšie — názvoslovie používané vo vyhláške č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy [17]. Ide o snahu o zjemnenie právnej dvojkoľajnosti, ktorú zaviedol Úrad podpredsedu vlády Slovenskej republiky pre investície a informatizáciu (terajšie Ministerstvo investícií, regionálneho rozvoja a informatizácie SR) vydaním vyhlášky č. 179/2020 Z. z. [17]. Súvisí to s problematikou tzv. sektorových bezpečnostných opatrení.

Podľa § 19 ods. 1 zákona [6] je prevádzkovateľ základnej služby povinný prijať a dodržiavať **všeobecné bezpečnostné opatrenia** najmenej v rozsahu bezpečnostných opatrení podľa § 20 a **sektorové bezpečnostné opatrenia,** ak sú prijaté. Ako bolo citované inde, podľa § 20 ods. 1 zákona, bezpečnostnými opatreniami sú úlohy, procesy, roly a technológie v organizačnej, personálnej a technickej oblasti, ktorých cieľom je zabezpečenie kybernetickej bezpečnosti počas životného cyklu sietí a informačných systémov. Bezpečnostné opatrenia sa v zákone ďalej rozdeľujú na základe špecifikácie do dvoch kategórií:

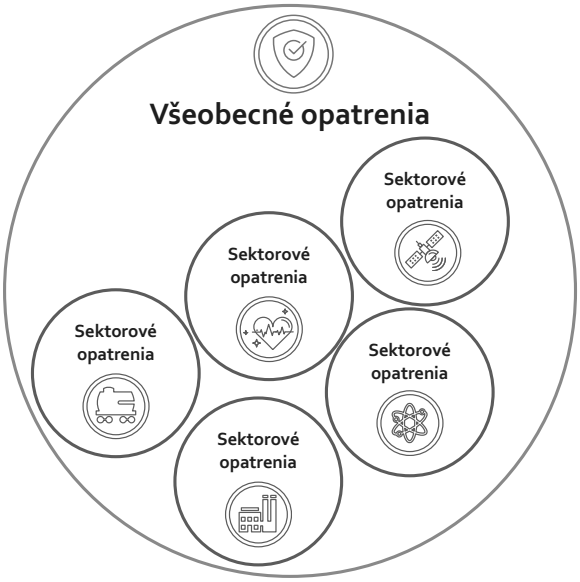
- **všeobecné** vyplývajúce z § 20 ods. 3 zákona [6], spresnené vyhláškou NBÚ č. 362/2018 Z. z. [14], ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len **„vyhláška“**), alebo
- **sektorové,** ktoré sa realizujú na základe špecifík kategorizácie sietí a informačných systémov ústredného orgánu v rozsahu svojej pôsobnosti.

Koncept sektorových opatrení

Ústredné orgány sú zákonom splnomocnené na vydanie všeobecne záväzného právneho predpisu, ktorým ustanovia sektorové bezpečnostné opatrenia v rozsahu svojej pôsobnosti podľa § 32 ods. 2 zákona. **Cieľom sektorových bezpečnostných opatrení má byť riešenie špecifík kybernetického priestoru v sektore v rámci pôsobnosti príslušného ústredného**

orgánu, nie nahradenie všeobecných bezpečnostných opatrení, ale len ich prípadné doplnenie sektorovými opatreniami. Toto splnomocňovacie ustanovenie zákona o sektorových bezpečnostných opatreniach má riešiť reálne špecifiká niektorých odvetví (napríklad energetiky, leteckej dopravy, zdravotníctva, telekomunikácií alebo priemyselnej výroby), ktoré vykazujú zásadné odlišnosti informačnej architektúry.

Ilustrácia č. 6: Vzťah množiny všeobecných a sektorových opatrení



Je teda možné tvrdiť, že **ku dňu vydania tejto publikácie nie sú účinné žiadne všeobecne záväzné vykonávacie právne predpisy, ktorými by boli stanovené špecifické sektorové opatrenia.**

Dalo by sa namietať, že predsa Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z. [17] (ďalej aj ÚPVII), ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy, určuje sektorové opatrenia. Avšak po podrobnejšej analýze zistíme, že táto vyhláška efektívne neidentifikuje špecifické odlišnosti informačných aktív v sektore Verejná správa.

Ak odhliadneme od množstva formálnych požiadaviek, vyhláška ÚPVII č. 179/2020 Z. z. [17] neprináša v porovnaní s vyhláškou NBÚ č. 362/2018 Z. z. [14] žiadne reálne bezpečnostné opatrenia navyše. Formálne požiadavky sú však len zbytočnou administratívnou záťažou pre povinné osoby. Príliš extenzívne povinnosti v oblasti administratívy a organizačné opatrenia, bez implementácie technických opatrení, nikdy nemôžu prispieť k zvýšeniu úrovne bezpečnosti. V konečnom dôsledku, existencia vyhlášky ÚPVII č. 179/2020 Z. z. [17] vnáša do regulácie kybernetickej bezpečnosti právnu dvojkoľajnosť, ktorá spôsobuje množstvo nedorozumení.

Tieto konštatovania sa dajú objektívne zdôvodniť reálnou aplikačnou praxou.

V zmysle § 29 ods. 2 zákona je prevádzkovateľ základnej služby povinný preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených zákonom vykonaním auditu kybernetickej bezpečnosti v rozsahu stanovenom podľa všeobecne záväzného právneho predpisu, ktorý vydá Národný bezpečnostný úrad. Audítor kybernetickej bezpečnosti posudzuje primárne zhodu prijatých bezpečnostných opatrení a požiadaviek daných vyhláškou NBÚ č. 362/2018 Z. z. [14] Až následne audítor posudzuje sektorové bezpečnostné opatrenia (ak sú

prijaté). V prípade vyhlášky č. 179/2020 Z. z. [17] však niet čo posudzovať. **V kontexte kybernetického priestoru architektúra systémov a služieb verejnej správy žiadne špecifiká nevykazuje** napriek tomu, že zákonodarca v § 23 zákona č. 95/2019 Z. z. o ITVS [16] uvádza *osobitné opatrenia na úseku bezpečnosti informačných technológií verejnej správy.*

Všeobecné princípy návrhu bezpečnostných opatrení

Návrh bezpečnostných opatrení nie je vecou subjektívneho vnímania. Mal by byť založený na určitých zásadách, ktoré sú odvodené od bezpečnostnej stratégie organizácie, pričom bezpečnostná stratégia by mala kopírovať obchodné (prevádzkové) ciele a obchodnú (prevádzkovú) stratégiu organizácie.

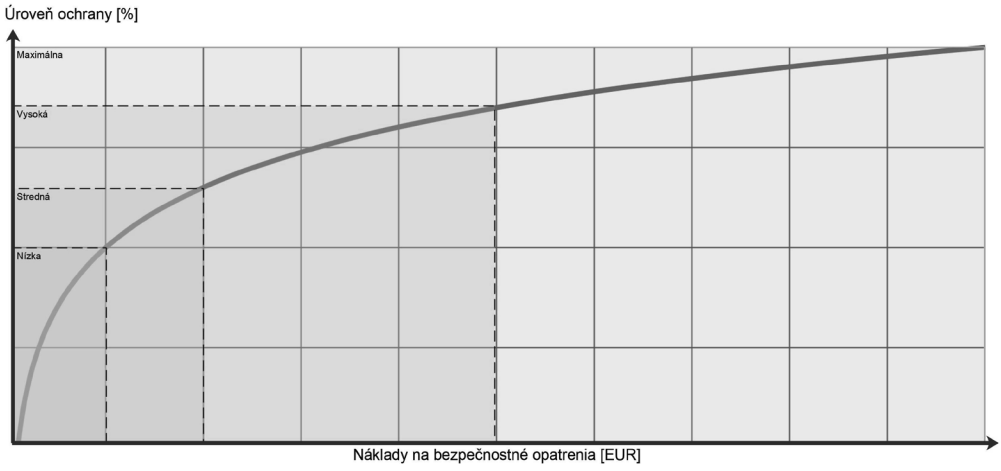
Predovšetkým — **opatrenia majú byť primerané pre ošetrovanie identifikovaných rizík.** To je racionálna požiadavka, ktorá bola prvýkrát legislatívne ukotvená v čl. 32 GDPR [8], podľa ktorého *prevádzkovateľ a sprostredkovateľ prijmú so zreteľom na najnovšie poznatky, náklady na vykonanie opatrení a na povahu, rozsah, kontext a účely spracúvania, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb, primerané technické a organizačné opatrenia, s cieľom zaistiť úroveň bezpečnosti primeranú tomuto riziku.*

Výraz „primerané“ opatrenia má dvojaký význam.

Prvý z významov smeruje k tomu, aby prevádzkovateľ vynaložil na ošetrenie identifikovaných rizík aspoň určité minimálne úsilie a aby nezanedbal žiadnu príležitosť na ošetrenie rizík, berúc do úvahy najnovšie dostupné odborné poznatky.

Druhý z významov je možné interpretovať tak, že zdroje (najmä náklady a čas) vynaložené na implementáciu bezpečnostného opatrenia by nemali prekročiť kvantifikovanú hodnotu samotného rizika. Pretože v tom prípade by už boli opatrenia neefektívne, teda neprimerané.

Ilustrácia č. 7: Efektivita opatrení v závislosti od nákladov implementácie



Pri návrhu a implementácii opatrení by mal prevádzkovateľ vychádzať z nasledovných základných princípov:

- opatrenia sú navrhované v kontexte identifikovaných zraniteľností a hrozieb a z nich vyplývajúcich rizík,
- opatrenia sú navrhované tak, aby napomohli splniť stanovené bezpečnostné spôsobilosti,

- priorita implementácie opatrení by mala byť prispôsobená hodnote a charakteru výsledného rizika určeného podľa stanovenej metodiky,
- cieľom návrhu opatrení by malo byť navrhnúť vhodné bezpečnostné funkcie (t. j. systém bezpečnostných mechanizmov, služieb a postupov) takým spôsobom, aby po ich implementácii boli identifikované riziká znížené na úroveň zodpovedajúcu akceptovateľným zvyškovým rizikám,
- pre každé výsledné riziko, ktoré nie je akceptovateľné, je popísaný spôsob jeho ošetrenia pomocou navrhovaných bezpečnostných opatrení.

Publikácia približuje podstatu jednotlivých oblastí všeobecných bezpečnostných opatrení vyžadovaných podľa § 20 ods. 3 zákona č. 69/2019 Z. z. [6] o kybernetickej bezpečnosti, spresnených vyhláškou Národného bezpečnostného úradu č. 362/2018 Z. z. [14], ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení **v znení platnom a účinnom ku dňu vydania tejto publikácie.** S výnimkou spornej vyhlášky ÚPVII č. 179/2020 Z. z. [17] nie sú ku dňu vydania tejto publikácie platné a účinné žiadne ďalšie všeobecne záväzné právne predpisy, ktorými by boli stanovené špecifické sektorové opatrenia.

• • • •