Odbor riadenia kybernetickej a informačnej bezpečnosti
Verzia 1.0 | kyberbezpecnost@mirri.gov.sk

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Špecifikácia obsahu špeciálnych bezpečnostných politík 2. úrovne

Obsah

1 Manažérske zhrnutie

Správca informačného systému verejnej správy je podľa zákona [3] povinný zaviesť vo svojej organizácii jednotný systém riadenia informačnej (a kybernetickej) bezpečnosti. Jeho základom je Bezpečnostná politika, ktorá definovala ciele kybernetickej a informačnej bezpečnosti v organizácii a rámcovo spôsoby, ako ich naplniť. Rámcové riešenia musia byť detailnejšie rozpracované, aby ich bolo možné v organizácii aj zaviesť. Štandardnou formou pre definovanie konkrétnejších pravidiel pre nejakú špecifickú oblasť KIB sú bezpečnostné politiky 2. úrovne. Na rozdiel od Politiky KIB, ktorá je pomerne všeobecná, bezpečnostné politiky 2. úrovne už musia vo väčšej miere zohľadňovať pomery v organizácii a dávať konkrétnejšie návody riešení. Bezpečnostná politika 2. úrovne sa nedá napísať bez znalosti organizácie . V tomto dokumente ktorý je určený manažérom KIB, uvádzame podrobnejšiu špecifikáciu 13 bezpečnostných politík (2.úrovne), ktoré bude organizácia potrebovať pre vytvorenie a využívanie systému riadenia informačnej (a kybernetickej) bezpečnosti. Oblasti, pre ktoré sme spracovali špecifikácie bezpečnostných politík vychádzajú z normy [9] ale ak sa ukáže potreba vypracovať ďalšie bezpečnostné politiky, alebo iné bezpečnostné dokumenty, je tento dokument možné doplniť.
Existuje niekoľko oblastí, ktoré sú natoľko zložité, že sa nebudú dať upraviť dokumentom vo forme politiky. Ide o vývoj a prevádzku systémov, správu sietí a pravidlá pre koncových používateľov. Hoci sme pre posledné dve pripravili špecifikácie špeciálnych politík, užitočnejšie bude vypracovať prevádzkový poriadok pre informačné systémy a siete a Príručku KIB pre koncového používateľa.

2 Úvod

Politika kybernetickej a informačnej bezpečnosti je základným dokumentom systému riadenia informačnej (a kybernetickej) bezpečnosti (ISMS), ktorý má organizácia prevádzkujúca informačný systém verejnej správy II. a III. kategórie podľa zákona [3] vypracovať. V dokumente [20] sme popísali, ako má správca ISVS postupovať pri vypracovaní Politiky kybernetickej a informačnej bezpečnosti (KIB). Problematika KIB je komplexná, a preto Politika KIB môže obsahovať nanajvýš rámcové vymedzenie toho, čo treba v organizácii chrániť a ako. Všeobecné ustanovenia Politiky KIB majú byť podrobnejšie rozpracované v špeciálnych politikách druhej úrovne, prípadne návodoch, metodických dokumentoch, ktoré majú pomôcť presadiť ustanovenia Politiky KIB v praxi.
Tento dokument sa zaoberá bezpečnostnými politikami druhej úrovne. Aj keď je obsah Politiky KIB stanovený všeobecne akceptovaným medzinárodným štandardom [9], bezpečnostné politiky druhej úrovne sú už viac závislé od podmienok v organizácii, pre ktorú je potrebné ich vytvoriť a hoci je známe, čo je celkovo potrebné riešiť, rozdelenie problematiky na časti podrobnejšie popísané v bezpečnostných politikách 2. úrovne je ponechané na organizáciu. Pokiaľ ide o správu ISVS, obsah bezpečnostných politík explicitne uvádza vyhláška [2], implicitne vyplýva z vyhlášky [4] a štandardný zoznam špeciálnych bezpečnostných politík čitateľ nájde v norme [9]. Keďže vo všetkých prípadoch ide o rovnaký, ale inak štruktúrovaný obsah, budeme vychádzať z normy [9].
Tento dokument obsahuje zoznam špecializovaných politík uvedených v norme [9]. Pre každú politiku uvádzame jej obsah podľa normy a vysvetľujeme, ako ho interpretovať, resp. aké požiadavky na danú oblasť kladú vyhlášky.

3 Špeciálne bezpečnostné politiky 2. úrovne

Špeciálne bezpečnostná politiky by mali mať jednotný formát a obsahovať základné informácie, ktoré ich umožnia zaradiť do bezpečnostnej dokumentácie a uviesť súvislosti s inými dokumentami.

- názov
- vecná oblasť a jej význam v kontexte KIB
- oblasť pôsobnosti (na čo sa vzťahuje)
- z čoho politika vychádza a na čo nadväzuje

- s čím súvisí
- aké okruhy problémov rieši, ako, kto je za riešenie zodpovedný, kto sa na ňom podieľa
- odkazy na informačné zdroje, z ktorých by politika mohla vychádzať
- aké dokumenty je potrebné vypracovať, resp. čo je potrebné spraviť na implementáciu politiky

Obsah špeciálnych bezpečnostných politík vychádza z ISO normy [9], vyhlášok [2][4], prípadne ďalších noriem a štandardov.

3.1.1 Riadenie prístupu

Názov	Politika riadenia prístupu
Oblasť a jej význam	Riadenie prístupu. Ide o prierezovú problematiku, bez jej spoľahlivého riešenia nie je možné zaistiť KIB v organizácii. Cieľom riadenia prístupu je zaistiť, aby k informačným aktívam organizácie mali prístup (a mohli s nimi pracovať) len oprávnené osoby, mohli s nimi alebo prostredníctvom nich vykonávať len činnosti, na ktoré majú oprávnenie a zabrániť prístupu neoprávnených osôb k aktívam organizácie.
Pôsobnosť	Celá organizácie [detailne špecifikovaná časť organizácie]
Východiská	Politika riadenia prístupu vychádza z princípov definovaných v Politike KIB a detailnejšie ich rozpracováva [mohli by sme ich vymenovať]. Obsahovo sa pridŕža časti 9 ISO normy [9]
Súvislosti	Organizácia KIB, Bezpečnosť ľudských zdrojov, Fyzická bezpečnosť, Manažment aktív, Manažment rizík, Manažment bezpečnostných incidentov, Kryptografické opatrenia, Manažment KIB vo vzťahu k tretím stranám, Klasifikácia informácie a kategorizácia systémov
Obsah	Stanovenie prístupových práv • Vlastníci aktív určia pravidlá pre riadenie prístupu k ich aktívam, prístupové práva a obmedzenia, • Tieto zohľadňujú klasifikáciu aktív a riziká vyplývajúce z neoprávneného prístupu a vzťahujú sa na bezpečnostné roly • zohľadňujú sa fyzické aj logické opatrenia na riadenie prístupu Prístup k sieťam a sieťovým službám • kto môže pristupovať k sieťam a používať sieťové služby • autorizačné procedúry pre prístup k sieťam a sieťovým službám • opatrenia a procedúry na ochranu k sieťovým spojeniam a sieťovým službám • prostriedky na prístup k sieťam a sieťovým službám (VPN, WIFI) • autentifikácia používateľov • monitorovanie využívania sieťových služieb Manažment prístupu používateľov • registrovanie a odregistrovanie používateľov • Poskytovanie prístupu používateľom • procesy udeľovania a odoberania prístupových práv • Správa privilegovaných používateľských práv • Manažment tajných autentifikačných informácií používateľov • Revízie prístupových práv používateľov

	• Odoberanie alebo zmena prístupových práv Zodpovednosť používateľov • používanie tajnej autentifikačnej informácie Riadenie prístupu k systémom a aplikáciám • obmedzenie prístupu k informáciám • bezpečné procedúry prihlasovania • systémy na manažment hesiel • Používanie vyhradených systémových/servisných programov • riadenie prístupu k zdrojovému kódu
Špecifické	• Manažment hesiel a prípadne iných prostriedkov na autentifikáciu používateľov (ak sa v organizácii používajú), biometrické prostriedky, čipové karty, kryptografické riešenia • centrálna správa identít • SSO,...
Zodpovednosť	• používateľ (za heslo a iné autentifikačné prostriedky) • vlastník aktíva – stanovenie prístupových práv pre roly a správa prístupových práv • technická realizácia správy používateľov/identít – správca príslušného systému • personálne oddelenie – nahlasovanie vlastníkovi aktíva zmeny pracovného zaradenia • správa rol – vedúci pracovník pre svojich zamestnancov • správa politiky – manažér KIB
Informačné zdroje	• Politika KIB • norma ISO/IEC 27002, časť 9
Spraviť	• pravidlá, postupy, návody pre uvedené činnosti • do návodu pre používateľov – narábanie s heslami • materiál pre školenie zamestnancov
Poznámka	Vyhláška [4] obsahuje požiadavku na RBAC a centrálnu správu identít

3.1.2 Klasifikácia informácie a narábanie s informáciou

Názov	**Klasifikácia informácie a narábanie s informáciou**
Oblasť a jej význam	Klasifikácia informácie umožňuje štandardizovať úroveň ochrany informačných aktív organizácie, a to tak z hľadiska cieľov ako aj úrovne ochrany. Cieľom ochrany je zaistenie dôvernosti, integrity a dostupnosti informačných aktív, úroveň ochrany je nízka, stredná alebo vysoká. V prípade verejných informácií je úroveň dôvernosti nulová. Kategorizácia systémov je odvodená od klasifikácie informácií, ktoré sa v nich spracovávajú. Význam klasifikácie informácie a kategorizácie systémov je v tom, že je možné zoskupiť informácie vzhľadom na potreby ich ochrany do tried s rovnakými bezpečnostnými potrebami a navrhovať riešenia pre triedy a nie pre jednotlivé aktíva.
Pôsobnosť	Celá organizácia, informácie v akejkoľvek forme, informačné aktíva organizácie
Východiská	Politika KIB, zákony a vyhlášky [1][2][3][4]

Súvislosti	Správa rizík, správa aktív
Obsah	• podstata a význam klasifikácie • klasifikácia systémov podľa vyhlášok [2][4] a ich premietnutie do bezpečnostných požiadaviek • základné požiadavky na bezpečnosť informácie: dôvernosť, integrita, dostupnosť • typy informácie používanej v organizácii (delenie podľa vecnej stránky: údaje prislúchajúce k nejakej agende, osobné údaje, ekonomické údaje, utajované skutočnosti a pod.) • Klasifikácia typov informácie: ohodnotenie potreby chrániť dôvernosť, integritu a dostupnosť na úrovni žiadna[1], nízka, stredná, vysoká; t.j. priradenie trojice hodnôt (úroveň dôvernosti, úroveň integrity, úroveň dostupnosti) každému typu informácie. Pri klasifikácii typu informácie sa vychádza z toho aký dopad by malo narušenie dôvernosti, integrity, dostupnosti pre organizáciu • kategorizácia systémov – trojica hodnôt (úroveň dôvernosti, úroveň integrity, úroveň dostupnosti) odvodená od najvyšších hodnôt v ohodnoteniach informácií, ktoré sa v systéme spracovávajú • informácie klasifikuje vlastník (vedúci organizačného útvaru, ktorý ich spracováva) spolu s manažérom KIB • klasifikácia konkrétnej informácie zodpovedá klasifikácii typu, do ktorého patrí (ak sa reálne požiadavky na ochranu informácie výrazne líšia od typu, do ktorého patrí, možno vytvoriť nový typ) • popis procesu klasifikácie, zmeny klasifikácie • pravidlá pre revízie klasifikácie • označovanie klasifikovanej informácie prípadne informačných aktív vo fyzickej aj elektronickej podobe • procedúry alebo požiadavky na procedúry narábania s klasifikovanými informáciami (spracovanie, uchovávanie, prenášanie, archivácia, ničenie)
Špecifické	
Zodpovednosť	• klasifikácia aktív – vlastníci aktív + manažér KIB • zodpovednosť za túto politiku a zmenové konanie – manažér KIB
Informačné zdroje	• Zákony a vyhlášky [1][2][3][4] • Politika KIB • ISO norma [9] • FIPS 199 a 200 [21][22]
Spraviť	Metodika klasifikácie informácií a kategorizácie systémov Pravidlá pre narábanie s klasifikovanou informáciou
Poznámka	

[1] platí len pre dôvernosť

3.1.3 Fyzická bezpečnosť a bezpečnosť prostredia

Názov	Fyzická bezpečnosť a bezpečnosť prostredia
Oblasť **Jej význam**	Informáciu v konečnom dôsledku spracovávajú fyzické zariadenia, ktoré na svoju činnosť potrebujú primerané podmienky. Fyzická bezpečnosť a bezpečnosť prostredia sa zaoberá ochranou pred hrozbami fyzického charakteru, jej cieľom je zabrániť neoprávnenému fyzickému prístupu k informačným aktívam organizácie, ich fyzickému poškodeniu alebo zasahovaniu do nich. Zaistenie primeraných podmienok (ochrana pred prírodnými vplyvmi a technickými poruchami) je nutnou podmienkou fungovania IKS organizácie.
Pôsobnosť	Celá organizácia
Východiská	Politika KIB
Súvislosti	Správa rizík, správa aktív, riešenie bezpečnostných incidentov, kontinuita činnosti
Obsah	Zabezpečené oblasti • fyzický bezpečnostný perimeter • riadenie fyzického prístupu do zabezpečených priestorov • zabezpečenie pracovní, priestorov a budov • ochrana pred vonkajšími hrozbami a hrozbami prostredia (prírodné katastrofy, nehody, úmyselné útoky) • pravidlá práce v zabezpečených oblastiach • kontrola vstupov pre dodávateľov tovarov a služieb, nakladacích priestorov pre odvoz vecí z organizácie (napr. smeti) Zariadenie • Cieľ – zabrániť strate, poškodeniu, krádeži alebo kompromitácie aktív a prerušeniu činnosti organizácie • zaistiť vhodné umiestnenie a ochranu zariadení • spoľahlivá pomocná infraštruktúra (voda, plyn, telekomunikačné služby, ventilácia, odvoz smetí, kanalizácia, klimatizácia) • zaistenie bezpečnosti káblov (elektrické vedenie aj dátové káble) • údržba zariadení s cieľom zaistiť dostupnosť a integritu • vynášanie aktív z priestorov organizácie • bezpečnosť zariadení a aktív mimo priestorov organizácie • bezpečné vyraďovanie a opätovné používanie zariadení • opustené zariadenie používateľa • politika čistého stola a čistej obrazovky
Špecifické	
Zodpovednosť	• správca budovy za budovu a fyzickú ochranu prístupu, ochranu zariadení pred prírodnými vplyvmi • spolu s vedúcim IT oddelenia – vytvorenie zabezpečenej oblasti • pravidlá pre prácu v zabezpečenej oblasti - vedúci IT oddelenia • vynášanie aktív – majitelia aktív • vyraďovanie, opravy IKT – vedúci IT+ najitelia aktív • organizačné opatrenia a ich dodržiavanie – manažér KIB a vedúci útvarov

Informačné zdroje	• Zákony a vyhlášky [1][2][3][4] • Norma [9]
Spraviť	• skontrolovať, či má organizácia zavedené opatrenia fyzickej bezpečnosti (ochrana vstupu, hlásiče požiaru, pohybu) záložné zdroje elektriny, vody, telekomunikačných služieb, zmluvy s externými poskytovateľmi služieb v súlade s požiadavkami na dostupnosť služieb a pod.; pravidlá a postupy pri vynášaní, vyraďovaní, opravách a údržbe zariadení. Ak nie, odstrániť nedostatky • školenia nových a existujúcich zamestnancov
Poznámka	

3.1.4 Bezpečnostné pravidlá pre koncového používateľa

Názov	**Bezpečnostné pravidlá pre koncového používateľa**
Oblasť **A jej význam**	Koncový používateľ je rola s naväčším počtom členov. Koncový používateľ má najmenšie privilégiá, najmenšie vedomosti z kybernetickej a informačnej bezpečnosti a informatiky. Môže z nevedomosti spraviť chyby, ktoré ohrozia IKS organizácie. Ale zároveň je to osoba, kvôli ktorej organizácia prevádzkuje svoje IKS, lebo koncový používateľ pomocou nich vykonáva činnosť, kvôli ktorej bola organizácia zriadená. Koncový používateľ nepotrebuje špecializované vedomosti z kybernetickej a informačnej bezpečnosti, potrebuje vedieť, čo má robiť, čo nesmie robiť a na koho sa má obrátiť, keď narazí pri práci s IKS na problém, s ktorým si nevie poradiť.
Pôsobnosť	Celá organizácia, externí spolupracovníci
Východiská	Politika KIB
Súvislosti	Bezpečnosť ľudských zdrojov, fyzická bezpečnosť
Obsah	Pravidlá používania informačných aktív organizácie Pravidlo čistého stola a čistej obrazovky Pravidlá pre prenos informácie prostredníctvom všetkých komunikačných kanálov organizácie Pravidlá používania prenosných zariadení Obmedzenia na inštaláciu softvéru
Špecifické	
Zodpovednosť	Koncový používateľ Manažér KIB (školenia a kontrola)
Informačné zdroje	• Zákony a vyhlášky [1][2][3][4] • Norma [9]
Spraviť	Pripraviť materiály a školenie pre koncových používateľov
Poznámka	

3.1.5 Zálohovanie

Názov	Zálohovanie
Oblasť A jej význam	Zálohovanie je prostriedok na zabránenie straty/dostupnosti údajov.
Pôsobnosť	Informácie, ktorých strata je pre organizáciu nenahraditeľná, alebo môže spôsobiť dlhodobý výpadok činnosti organizácie.
Východiská	Politika KIB
Súvislosti	Kontinuita prevádzky, ochrana proti škodlivému kódu
Obsah	• stanovenie potrieb organizácie na vytváranie záloh informácie, softvéru a systémov • zaistenie dostatočných záložných kapacít na obnovu informácie a softvéhu po poškodení alebo zlyhaní • plán zálohovania (čo zálohovať, ako a ako často) • ukladanie záloh • ochrana záloh ekvivalentná ochrane primárnej informácie • testovanie kvality pamäťových médií použitých na uchovávanie záloh • testovanie procedúr obnovy • prípadná ochrana zálohovaných údajov (podľa klasifikácie) šifrovaním
Špecifické	
Zodpovednosť	• manažér KIB a vlastníci aktíva – čo treba zálohovať • podľa spôsobu zálohovania – vedúci IT alebo správca systému – zálohovanie • správa zálohovaných údajov a kontrola prístupu k nim • testovanie záloh, ich integrity, kompletnosti a obnoviteľnosti • tréning postupov obnovy pre konkrétne typy údajov aj celé systémy
Informačné zdroje	• Norma [9], časť 12.3 • Zákony a vyhlášky [1][2][3][4]
Spraviť	Preveriť, ako vyzerá v organizácii zálohovanie a či má organizácia dostatočné zálohovacie kapacity a v akom stave sú procesy
Poznámka	

3.1.6 Manažment bezpečnosti sietí

Názov	Manažment bezpečnosti sietí
Oblasť A jej význam	Organizácia pre svoju činnosť potrebuje zaistiť spoľahlivú komunikáciu svojich systémov navzájom a s externými systémami, na ktorú využíva komunikačné siete. Cieľom tejto politiky je zaistiť ochranu informácií v sieťach a informačných systémoch, ktoré prepája
Pôsobnosť	Celá organizácia
Východiská	Politika KIB
Súvislosti	Prenos informácií, Riadenie prístupu, Manažment bezpečnostných incidentov, Škodlivý kód, Bezpečnosť prevádzky
Obsah	Siete majú byť spravované a riadené, aby sa zaistila ochrana informácie v systémoch a aplikáciách. • stanovenie zodpovednosti za na správu sieťových zariadení a procedúr na ich správu • oddelenie zodpovednosti za prevádzku siete a prevádzku systémov • špeciálne opatrenia na ochranu dôvernosti a integrity dát prenášaných verejnými sieťami alebo WIFI sieťami • požiadavky a opatrenia na zaistenie dostupnosti sieťových služieb a počítačov pripojených k sieti • monitorovanie a vytváranie záznamov auditu o bezpečnostne relevantných aktivitách a udalostiach na sieti • autentifikácia systémov pripojených k sieti • obmedzenie pripojenia systémov k sieti. Bezpečnosť sieťových služieb • stanoviť požiadavky na bezpečnostné mechanizmy, úrovne služieb, správu služieb • zmluvy s poskytovateľmi sieťových služieb a kontrola ich dodržiavania Segregácia v sieťach • definovať požiadavky na segregáciu skupín sieťových služieb, používateľov a informačných systémov
Špecifické	
Zodpovednosť	Správca siete, manažér KIB
Informačné zdroje	Norma [9], normy ISO/IEC 27033, 27033-1 až 6
Spraviť	
Poznámka	Norma [9] komunikačnú bezpečnosť delí na technickejší manažment bezpečnosti sietí a obsahovo zameranú bezpečnosť prenosu informácií. Obe z nich upravuje špeciálnymi politikami

3.1.7 Prenos informácie

Názov	Prenos informácie
Oblasť A jej význam	Toto je druhá, netechnická časť oblasti Bezpečnosti komunikácie. Prvá sa zaoberá bezpečnosťou sietí. Informácia sa málokedy spracováva a využíva na mieste, kde bola zaznamenaná (zdroj informácie), ale prenáša sa tak medzi rôznymi subjektami v rámci organizácie, ako aj medzi organizáciou a inými externými inštitúciami a jedincami. Cieľom tejto špeciálnej politiky je zaistiť bezpečnosť informácie prenášanej v organizácii a medzi organizáciou a externým subjektom.
Pôsobnosť	Celá organizácia
Východiská	Politika KIB
Súvislosti	Klasifikácia informácií, riadenie prístupu, vzťahy s tretími stranami, riadenie rizík, organizácia KIB, ochrana osobných údajov, ...
Obsah	Definícia problému, ktorý má politika riešiť a ako – politiky, procedúry a opatrenia na zaistenie ochrany informácie prenášanej ľubovoľným komunikačným kanálom. • procedúry na ochranu prenášanej informácie pred odpočúvaním, kopírovaním, modifikáciou, presmerovaním a zničením • procedúry na detekciu škodlivého kódu, ktorý sa prenáša elektronickými komunikačnými kanálmi a ochranu pred ním, • procedúry na ochranu citlivej informácie posielanej vo forme príloh elektronickej pošty • politiky/návody akceptovateľného používania komunikačných zariadení • zodpovednosť zamestnancov, externých spolupracovníkov a iných používateľov IKS organizácie, vyvarovať sa konania, ktoré by mohlo kompromitovať organizáciu • používanie kryptografických techník napr. na ochranu dôvernosti, integrity a autentickosti informácie • návody na uchovávanie a vyraďovanie úradnej korešpondencie, vrátane mailov, v súlade s predpismi o registratúrnej a archívnej agende • opatrenia a obmedzenia na používanie komunikačných zariadení (zákaz automatického presmerovania úradnej pošty na súkromnú adresu) • poučenie zamestnancov o opatreniach na ochranu dôvernej informácie • nenechávať odkazy obsahujúce citlivú informáciu na záznamníku telefónu • nerozprávať sa o dôverných problémoch na miestach, kde je možné odpočúvanie. Dohody o prenose informácie, ktoré riešia bezpečný prenos informácií medzi organizáciou a tretími stranami (podrobnosti norma [9], časť 13.2.2) Ochrana elektronických správ Dôvernosť a dohody o zachovaní mlčanlivosti
Špecifické	
Zodpovednosť	Manažér KIB, správca siete, správca registratúry, správca archívu
Informačné zdroje	Politika KIB, norma [9], časť 13.2

Spraviť	• pozrieť sa, aké komunikačné kanály sa v organizácii používajú, aká informácia sa nimi prenáša, ako je chránená, kto k nej má prístup a aké pravidlá na prenos informácie v organizácii existujú a ako sa presadzujú. • detto pre externú komunikáciu • aké bezpečnostné problémy sa v minulosti v organizácii v súvislosti s prenosom informácie vyskytli • ak je treba – cielená analýza rizík, ak nie návrh a zavedenie opatrení na pokrytie najzávažnejších zistených zraniteľností • pripraviť tému na školenie
Poznámka	Problematiku Komunikácie tvorcovia normy ISO/IEC 27002 rozdelili do dvoch čiastkových politík podľa ich predpokladaných čitateľov prvá je určená technikom, druhá netechnicky zameraným vedúcim pracovníkom a používateľom

3.1.8 Ochrana pred škodlivým kódom

Názov	**Ochrana pred škodlivým kódom**
Oblasť a jej význam	Škodlivý kód (malvér, angl. malware) označuje program, ktorý je tajne vložený do iného programu so zámerom zničiť údaje, spustiť deštruktívne alebo ďalej sa šíriace programy, alebo inak kompromitovať dôvernosť, integritu alebo dostupnosť údajov, aplikácií alebo operačných systémov obete. Škodlivý kód je najbežnejšia vonkajšia hrozba pre väčšinu systémov, ktorá spôsobuje rozsiahle na škody a vo väčšine napadnutých organizácií si vyžaduje veľké úsilie na dosiahnutie obnovy pôvodného stavu. Organizácia si je vedomá závažnosti tejto hrozby a Bezpečnostná politika je základom pre systematickú ochranu pred malvérom v organizácii
Pôsobnosť	Všetky systémy organizácie
Východiská	Politika KIB
Súvislosti	Správa rizík, Manažment bezpečnostných incidentov, Bezpečnosť komunikácie, Správa zraniteľností
Obsah	• ochrana proti škodlivému pozostáva z činností, ktoré sú popísané v iných politikách • samostatná politika je potrebná preto, aby si používatelia aj zamestnanci zodpovední za ochranu pred škodlivým kódom uvedomili súvislosti a dokázali vybudovať kompaktnú obranu • stratégia organizácie: prevencia zameraná na zníženie pravdepodobnosti infiltrácií systémom organizácie škodlivým kódom, včasná detekcia infiltrácie, ohraničenie a obnova, analýza a vyvodenie záverov Prevencia • pamäťové médiá prinesené zvonka do organizácie sa musia pred použitím skontrolovať na prítomnosť škodlivého kódu • prílohy elektronickej pošty sa pred otvorením musia skontrolovať • zákaz posielať mailom súbory, ktoré môžu obsahovať škodlivý kód (napr. exe)

	• obmedzenie alebo úplný zákaz používania vlastných aplikácií a nepotrebného softvéru • zákaz používania pamäťových médií v externom prostredí (USB kľúče v internetovej kaviarni) • špecifikácia, aké sw nástroje na ochranu pred škodlivým kódom sa pre jednotlivé typy zariadení vyžadujú, vysokoúrovňové požiadavky na konfiguráciu a udržiavanie sw • obmedzenie alebo zákaz používania vlastných zariadení v sieti organizácie, alebo pre prácu na diaľku • zvyšovanie bezpečnostného povedomia koncových používateľov a ľudí zodpovedných za riešenie bezpečnostných incidentov (Ako nezamoriť organizáciu škodlivým kódom) • redukovanie zraniteľností (včasné identifikovanie nových zraniteľností a inštalácia záplat), konfigurácia systémov, uplatňovanie princípu najmenších privilégií • redukcia hrozieb (pozri [25]) • príprava reakcie na bezpečnostný incident (infiltráciu škodlivého kódu) • postup pri identifikácii zasiahnutého systému • stanovenie priorít pre zásah • analýza škodlivého kódu • lokalizácia škodlivého kódu (containment) • eradikácia škodlivého kódu • obnova • vyhodnotenie a závery vyvodené z bezpečnostného incidentu (zmeny bezpečnostnej politiky, zmeny vzdelávacích programov a školení, rekonfigurácia programového vybavenia, inštalácia antivírového sw, prípadne jeho rekonfigurácia)
Špecifické	
Zodpovednosť	Manažér KIB, vedúci IT oddelenia, technickí správcovia systémov, koncoví používatelia
Informačné zdroje	Politika KIB, Norma [9], Metodické materiály NIST [23][25]
Spraviť	• prečítať časť 12.2 z [9], dokument [25], preveriť, ako je v organizácii riešená ochrana pred škodlivým kódom, spraviť korekcie, napísať politiku • školenia pre používateľov, kapitola do Manuálu KIB pre koncového používateľa
Poznámka	Norma [9] ale najmä dokument NIST [23][25] je dosť podrobný, technicky orientovaný ale ešte zrozumiteľný. Väčšina opatrení sa vzťahuje na správu systémov a aplikácií, resp. má organizačný charakter. Asi bude rozumnejšie najprv revidovať existujúce a doplniť chýbajúce opatrenia a potom napísať politiku

3.1.9 Manažment technických zraniteľností

Názov	Manažment technických zraniteľností
Oblasť A jej význam	Zraniteľnosť je chyba, nedostatok alebo len spôsob použitia informačného aktíva, ktorá umožňuje, aby sa voči aktívu uplatnila nejaká hrozba. Zraniteľnosti svojich aktív bude organizácia skúmať pri analýze rizík a navrhovať opatrenia, ktoré ich odstránia, alebo aspoň zmenšia možnosti ich využitia. Niektoré zraniteľnosti organizácia nebude schopná odstrániť a časom sa môžu objaviť nové zraniteľnosti (najčastejšie sú to chyby v programovom vybavení). Tvorcovia programového vybavenia reagujú na objavenie sa nových zraniteľností okamžitými riešeniami (záplatami) a z času na čas aj novými verziami (väčších častí) programov. Cieľom tejto politiky je zabrániť využitiu technických zraniteľností
Pôsobnosť	celá organizácia
Východiská	Politika KIB
Súvislosti	Správa rizík, správa systémov a aplikácií
Obsah	Získavať včas informácie o technických zraniteľnostiach systémov, vyhodnotiť relevantnosť a závažnosť týchto zraniteľností pre organizáciu a prijať primerané opatrenia na ošetrenie rizika • organizácia by mala definovať roly a zodpovednosť za úlohy spojené s manažmentom technických zraniteľností (monitorovanie zraniteľností • identifikácia a sledovanie zdrojov informácií o zraniteľnostiach, udržiavanie aktuálneho zoznamu informačných aktív organizácie • definovať postupnosť krokov, ktorými organizácia reaguje na informáciu o potenciálnej technickej zraniteľnosti • po identifikácii technickej zraniteľnosti – vyhodnotenie rizík s ňou spojených a rozhodnutie o opatreniach (napr. inštalácia bezpečnostných záplat, alebo iné opatrenia) • podľa toho, ako rýchlo treba ošetriť technickú zraniteľnosť, postupovať buď podľa procedúr zmenového manažmentu, alebo podľa procedúr reakcie na bezpečnostné incidenty • ak je k dispozícii bezpečnostná záplata zo spoľahlivého zdroja posúdiť riziko inštalácie záplaty a riziko vyplývajúce zo zraniteľnosti, prípadne iného opatrenia na pokrytie zraniteľnosti (vypnutie ohrozených služieb, sprísnenie riadenia prístupu, zvýšené monitorovanie na zistenie možných útokov, informovanie zainteresovaných o existencii zraniteľnosti) • pred inštaláciu by záplaty mali byť testované, aby sa nestalo, že budú neúčinné, alebo budú mať nežiadúce vedľajšie efekty • vytvárať a uchovávať záznam auditu pre všetky činnosti, ktoré boli v súvislosti s riešením zraniteľnosti vykonané • monitorovanie, revízie procesu manažmentu technických zraniteľností • stanovenie priorít – ohrozené systémy budú ošetrené skôr

	• zosúladenie procesov manažmentu technických zraniteľností a manažmentu bezpečnostných incidentov, aby ľudia riešiaci bezpečnostný incident dostali včas informácie o technických zraniteľnostiach a prijatých opatreniach • definovať postup pre prípad, keď nie sú k dispozícii vhodné opatrenia na ošetrenie objavenej technickej zraniteľnosti.
Špecifické	
Zodpovednosť	• treba stanoviť (manažér KIB a vedúci IT oddelenia stanovia úlohy)
Informačné zdroje	• Zákony a vyhlášky [1][2][3][4] • Norma [9]
Spraviť	• kompletný a aktuálny zoznam informačných aktív (z ktorého sa dá zistiť, aký sw je inštalovaný na jednotlivých systémoch, kto je dodávateľ, kto je v organizácii zodpovedný za sw) • Manažér KIB spolu s informatikmi organizácie by mal preveriť, ako je zaistené sťahovanie a inštalácia bezpečnostných aktualizácií programov a doriešiť problematické prípady (napr. chýbajúce licencie). • v prípade dostatočnej komplexity zvážiť nasadenie dedikovaného softvérového riešenia na tzv. Patch Management
Poznámka	• Manažér KIB by mal mať po analýze rizík prehľad o všetkých odhalených a nedostatočne ošetrených zraniteľnostiach aktív organizácie, zabezpečiť monitorovanie týchto (a nielen týchto) aktív a raz za 6 mesiacov o stave zraniteľností informoval bezpečnostný výbor organizácie. Bezpečnostný výbor môže požadovať vykonanie analýzy rizík zameranej na detailné posúdenia závažnosti zistených problémov (napr. zvýšenie rizika vyplývajúceho z neošetrenej zraniteľnosti) a iniciovať predloženie záverov analýzy rizík s návrhom opatrení vedeniu organizácie. • manažment technických zraniteľností je v podstate súčasťou manažmentu zmien

3.1.10 Kryptografické opatrenia

Názov	**Kryptografické opatrenia**
Oblasť **A jej význam**	Kryptografické[2] riešenia sú základom kybernetickej a informačnej bezpečnosti; pomocou kryptografických funkcií sa zaisťuje dôvernosť, integrita a dôvernosť informácie/údajov. Kryptografické funkcie sú postavené na ťažkých matematických problémoch a modifikácie alebo nesprávne použitie týchto funkcií vytvára takmer isto zraniteľnosti v systéme, v ktorom sa používajú. Organizácie používajú štandardné kryptografické riešenia (šifrovanie na ochranu dôvernosti, digitálne odtlačky na zaistenie integrity a elektronické podpisy, pečate na zaistenie autentickosti dokumentov/údajov.
Pôsobnosť	Používatelia kryptografických funkcií a riešenia ktoré kryptografické funkcie využívajú

[2] kryptografia je náuka o kryptosystémoch (šifrách), šifrovaní tvorbe a využívaní šifier; kryptoanalýza je náuka zameraná na rozbíjanie šifier a kryptológia (náuka o kryptosystémoch) je spoločný názov pre kryptografiu a kryptoanalýzu

Východiská	Politika KIB
Súvislosti	Klasifikácia informácií, kategorizácia systémov, správa rizík, komunikácia, e-government
Obsah	• Organizácia využíva štandardné aplikácie so zabudovanými kryptografickými funkciami na zaistenie dôvernosti, integrity a autentickosti údajov. • [***Organizácia tiež využíva špeciálne systémy a aplikácie na tieto účely: …***] • Používanie kryptografických opatrení vychádza z klasifikácie údajov a analýzy rizík. • na aké účely sa budú kryptografické opatrenia používať, • prístup k manažmentu kryptografických kľúčov, z • zodpovednosti za implementáciu politiky a manžmentu kľúčov, • použité algoritmy a štandardy a dopad používania šifrovania na iné bezpečnostné opatrenia (detekcia škodlivého kódu), kontrola a audit.
Špecifické	Ak by organizácia vo zvýšenej miere využívala nejaké špecifické riešenie (napr. mala vlastnú certifikačnú autoritu)
Zodpovednosť	Za koordináciu využívania kryptografických opatrení zodpovedá manažér KIB, ktorý v spolupráci s externými odborníkmi sleduje informácie o zistených zraniteľnostiach kryptografických funkcií a navrhuje potrebné úpravy kryptografických opatrení.
Informačné zdroje	Politika KIB Norma [9] Učebnica [17]
Spraviť	Pozrieť sa, aké štandardné kryptografické riešenia sa v organizácii používajú, ako, kto za ne zodpovedá a či sú zdokumentované.
Poznámka	Organizácia nebude mať odborníkov na nejaké vlastné kryptografické riešenia. Bude používať štandardné kryptografické riešenia s odporúčanými nastaveniami. Manažér KIB bude nanajvýš dohliadať na dodržiavanie postupov a bude komunikovať s externým odborníkom o problémoch, ktoré si vyžadujú špecifické know-how

3.1.11 Ochrana súkromia a osobných údajov

Názov	**Ochrana súkromia a osobných údajov**
Oblasť A jej význam	Organizácia spracováva a je povinná primerane chrániť aj osobné údaje. Nemá zmysel vypracovávať paralelné bezpečnostné projekty; ochranu osobných údajov je možné zakomponovať do projektu KIB aj politiku ochrany osobných údajov vydať ako špeciálnu bezpečnostnú politiku
Pôsobnosť	Systémy v ktorých sa spracovávajú osobné údaje, jednoduchšie, celá organizácia
Východiská	Politika KIB, GDPR
Súvislosti	Súlad s legislatívou

Obsah	• čo sú osobné údaje, všeobecné dôvody, prečo ich organizácia spracováva, potreba ich ochrany • z čoho Politika vychádza (GDPR) a ako súvisí s Politikou KIB, resp. kybernetickou a informačnou bezpečnosťou v organizácii • základné princípy pri spracovaní osobných údajov (podľa GDPR) • Zodpovednosť za ochranu osobných údajov v organizácii (kto za čo zodpovedá – vedenie, Zodpovedná osoba, personálne oddelenie, právne oddelenie, vlastníci a technickí správcovia systémov, v ktorých sa spracovávajú osobné údaje, vedúci pracovníci,...) • Aké osobné údaje sa v organizácii spracovávajú, na aký účel, v ktorých systémoch, kto k nim má prístup • postupy (treba sa pozrieť na doposiaľ používané štandardné postupy spracovania osobných údajov a porovnať ich s požiadavkami GDPR a prípadne upraviť) • opatrenia – všeobecné (KIB) a špecifické (nahlasovanie bezpečnostných incidentov Úradu na ochranu osobných údajov, oboznamovanie dotknutých osôb, dohody s tretími stranami a pod.) • zverejnenie typov osobných údajov, ktoré organizácia spracováva a dôvodov, pre čo to robí (aby nemusela odpovedať na dotazy jednotlivcov, aké údaje o nich spracováva) • postupy v mimoriadnych situáciách (bezpečnostné incidenty) • analýza rizík (KIB a osobné údaje), audit • správa Politiky ochrany osobných údajov
Špecifické	
Zodpovednosť	Vedenie organizácie, osoba zodpovedná za ochranu osobných údajov a osoby spracovávajúce osobné údaje
Informačné zdroje	• GDPR [6] • Zákon [5] • Norma [9]
spraviť	• ak ho organizácia ešte nemá, bezpečnostný projekt na ochranu osobných údajov, v opačnom prípade overenie povinností, ktoré pre organizáciu vyplývajú z nariadenia GDPR [6] a zákona [5] minimálne zistenie, aké osobné údaje, z akých dôvodov, v akých systémoch, kto k nim má prístup, aké všeobecné a špeciálne bezpečnostné opatrenia sú v organizácii zavedené na ochranu údajov/osobných údajov, zodpovednosti • zosúladenie požiadaviek na ochranu osobných údajov s požiadavkami na KIB a koordinácia činnosti manažéra KIB a osoby zodpovednej za ochranu osobných údajov

3.1.12

3.1.13 KIB vo vzťahoch s tretími stranami

Názov	KIB vo vzťahoch s tretími stranami
Oblasť A jej význam	K informačným aktívam organizácie majú okrem vlastných zamestnancov a anonymných klientov prístup a svojou činnosťou ich ovplyvňujú aj dodávatelia, poskytovatelia rôznych informačných služieb a zamestnanci tretích strán. Tieto cudzie osoby sú povinné dodržiavať Bezpečnostnú politiku KIB a predpisy KIB, ale organizácia nemá také možnosti presadzovania bezpečnostných politík voči zamestnancom tretích strán, ako voči vlastným zamestnancom
Pôsobnosť	Celá organizácia
Východiská	Politika KIB
Súvislosti	So všetkými oblasťami, v ktorých môžu tretie strany pôsobiť: Personálna bezpečnosť, Fyzická bezpečnosť, Riadenie prístupu, Prevádzková bezpečnosť, Vývoj systémov, Kontinuita činnosti,...
Obsah	Definícia problému a prístup organizácie k jeho riešeniu: • organizácia zvlášť analyzuje riziká vyplývajúce z prístupu cudzích osôb k jej informačným aktívam, zavádza a udržiava opatrenia na minimalizáciu týchto rizík • opatrenia a povinnosti pre tretie strany pristupujúce k informačným aktívam organizácie, organizácia prerokováva so zainteresovanými stranami a zahŕňa do zmlúv. • Tieto povinnosti sa týkajú aj subdodávateľov a v primeranej miere aj ostatných článkov dodávateľského reťazca Konkrétne [9], časť 15.1.: • identifikácia a zdokumentovanie všetkých typov tretích strán (poskytovateľov služieb a dodávateľov), ktorí majú prístup k informačným aktívam organizácie • zásady a postupy manažovania vzťahov s tretími stranami • definovanie aké typy prístupov rôznych tretích strán ku ktorým informačným aktívam sú povolené a ako bude monitorovaný a riadený prístup • minimálne bezpečnostné požiadavky na prístup k informáciám (typ prístupu × typ informácie), ktoré sa potom aplikujú na konkrétne tretie strany • procesy a procedúry na monitorovanie dodržiavania dohodnutých pravidiel a bezpečnostných požiadaviek • opatrenia na zaistenie integrity, presnosti a úplnosti informácie poskytovanej treťou stranou a spôsobu spracovania informácie treťou stranou • typy povinností použiteľné vo vzťahu k tretím stranám na zaistenie ochrany informácie organizácie • riešenie incidentov a mimoriadnych situácií súvisiacich s prístupom tretích strán k informačným aktívam organizácie, vrátane zodpovedností organizácie a tretej strany • opatrenia/širšie riešenia na zaistenie odolnosti, obnovy a núdzovej prevádzky na zaistenie dostupnosti informácie a spracovania informácie v organizácii a u tretej strany • školenia zamestnancov organizácie, zodpovedných za verejné obstarávanie, tých, ktorí priamo prichádzajú do kontaktu so zamestnancami tretích strán o pravidlách prístupu zamestnancov tretích strán

	• dokumentácia dohodnutých pravidiel • prenos informácie, prenos spracovania informácie na iné systémy, cloudové služby a ochrana informácie. • Tretie strany často poskytujú organizácii aj služby, ktoré priamo nesúvisia s jej informačnými aktívami, ale nepriamo od nich závisí bezproblémový chod organizácie (dodávky vody, elektriny, dopravné, komunikačné, servisné služby, dodávky tovarov a pod.)
Špecifické	
Zodpovednosť	• Manažér KIB, právne oddelenie, oddelenie VO, IT oddelenie, vedúci oddelení spolupracujúcich s tretími stranami
Informačné zdroje	Politika KIB Norma [9], časť 15
Spraviť	• zistiť, ktoré (bezpečnostne relevantné) činnosti pre organizáciu vykonávajú tretie strany, akú riziká pre organizáciu sú s týmito činnosťami spojené, aké opatrenia by bolo možné prijať na ich odstránenie, analyzovať uzavreté zmluvy a snažiť sa ich dodatkovať tak, aby sa jasne vymedzili povinnosti tretej strany voči organizácii v KIB a upravilo riešenie bezpečnostných problémov • vyhodnotiť bezpečnostné riziká doterajšej spolupráce, keď povinnosti KIB neboli formálne uvedené v zmluvách • pri nových zmluvách zohľadniť bezpečnostné požiadavky KIB na tretie strany
Poznámka	V tejto časti Bezpečnostná politika rieši dva okruhy problémov. Prvým je prístup (potenciálne neznámych) zamestnancov tretích strán k informačným aktívam organizácie, vrátane outsourcingu informačných služieb a vývoja systémov. Druhým sú služby, ktoré nepriamo ovplyvňujú informačné aktíva FO, ale primárne za ne nezodpovedajú ani informatici, ani manažér KIB. V oboch prípadoch FO musí analyzovať riziká vyplývajúce z nedodržania povinností tretích strán a opatrenia pre takéto prípady zakomponovať do zmluvy s treťou stranou. V prípade, keď ide o služby, ktoré majú nepriamy dopad na informačné aktíva sa manažér KIB ani nemusí o nich dozvedieť. Preto je potrebná jeho spolupráca s ostatnými organizačnými útvarmi FO, ktoré takéto dohody pripravujú a poznajú aj problémy, ktoré sa pri ich plnení vyskytujú. Norma [9] v časti 15.2 obsahuje aj návrh podmienok, ktoré by organizácia mohla uviesť v zmluve: • Opis informácie, ktorá sa má poskytnúť, alebo sa k nej má pristupovať a metódy poskytovania tejto informácie, alebo prístupu k nej • klasifikácia informácie podľa klasifikačnej schémy organizácie a prípadne porovnanie klasifikačnej schémy organizácie a tretej strany • právne a iné záväzné požiadavky (na ochranu údajov, práv duševného vlastníctva, autorských práv) apopis, ako zmluvné strany zaistia ich naplnenie, • povinnosť každej zo zmluvných strán zaviesť (u seba) dohodnutý súbor opatrení, vrátane riadenia prístupu, revízie výkonu, monitorovania, hlásení a auditovania, • pravidlá akceptovateľného a neakceptovateľného použitia/používania informácie

	• buď zoznam zamestnancov tretej strany, ktorí majú pristupovať k informáciám organizácie, alebo tieto informýcie dostávať; alebo procedúry/podmienky získania a odnímania takýchto oprávnení • bezpečnostné politiky, ktoré sú relevantné pre daný kontrakt • požiadavky a procedúry manažmentu bezpečnostných incidentov (špeciálne informovanie a spolupráca pri riešení bezpečnostných incidentov) • požiadavky na školenia a bezpečnostné povedomie • relevantné požiadavky na sub-kontraktorov • zodpovedné osoby, vrátane kontaktnej osoby pre riešenie KIB, • požiadavky na skríning personálu tretej strany • právo na audit procesov a opatrení tretej strany, vzťahujúcich sa na kontrakt • procesy riešenia chýb a konfliktov • povinnosť tretej strany periodicky poskytovať organizácii správu vypracovanú nezávislou štvrtou (?) stranou o efektívnosti opatrení a riešení zistených nedostatkov • povinnosť tretej strany dodržiavať bezpečnostné požiadavky organizácie. Norma tiež podrobne popisuje postupy organizácie, zamerané na to, aby sa dodržala dohodnutá úroveň KIB a poskytovania služieb v súlade so zmluvou medzi organizáciou a dodávateľom.

3.1.14 Zaznamenávanie udalostí a monitorovanie

Názov	Zaznamenávanie udalostí a monitorovanie
Oblasť **A jej význam**	Aby sa zabezpečilo dodržiavanie bezpečnostnej politiky, umožnilo stanovovať zodpovednosť za aktivity v systémoch organizácie a včas odhalili pokusy o narušenie informačných aktív, bezpečnostne relevantné aktivity v systémoch organizácie sú kontinuálne monitorované a vytvára sa o nich záznam auditu. Cieľ: zaznamenávať udalosti a vytvárať dôkazový materiál (evidence)
Pôsobnosť	Všetky systémy organizácie
Východiská	Politika KIB
Súvislosti	Riadenie prístupu, manažment bezpečnostných incidentov, organizácia KIB
Obsah	• Pre každý systém technický správca systému spolu s vlastníkom systému a manažérom KIB v súlade s politikou riadenia prístupu k danému systému a informáciám v ňom spracovávaným stanovia, ktoré udalosti v systéme sa budú monitorovať a čo bude obsahovať záznam o týchto aktivitách. [9] • Záznamy auditu sú chránené proti narušeniu, úniku osobných údajov, ktoré obsahujú a sú uchovávané po primeranú vytýčenú a odôvodnenú retenčnú dobu. Záznamy auditu o činnostiach privilegovaných používateľov (správcov systémov) sú uchovávané mimo dosahu príslušných správcov. • Údaje zo záznamov auditu sú vyhodnocované priebežne [***pomocou automatických nástrojov ak tieto v organizácii existujú***] a detailne analyzované po bezpečnostných incidentoch. [***Ak "automatický vyhodnocovací systém"***

	odhalí podozrivú aktivitu v monitorovanom systéme, vydá výstrahu, v prípade bezpečnostného incidentu spustí alarm.] • aby bola jasná časová následnosť udalostí, hodiny jednotlivých systémov v organizácii sú zosynchronizované • Všeobecné pravidlá pre monitorovanie a vytváranie záznamov auditu upravuje predpis o prevádzke systémov v časti o monitorovaní, špecifické požiadavky na monitorovanie sú súčasťou bezpečnostnej dokumentácie konkrétnych systémov.
Špecifické	
Zodpovednosť	Za politiku manažér KIB, za systémy – technický správca, za záznamy auditu privilegovaných používateľov – treba ustanoviť zodpovedného
Informačné zdroje	Norma [9], časť 12.4
Spraviť	Skontrolovať, či sa v organizácii robia záznamy auditu a či sa spracovávajú požadovaným spôsobom
Poznámka	Záznam auditu je záznam o bezpečnostne relevantných udalostiach v systéme, obsahujúci minimálne údaje o čase a výsledku aktivity (napr. neúspešné prihlásenie) a jej pôvodcovi. Slúži najmä na dohľadávanie udalostí, ktoré viedli k bezpečnostnému incidentu v systéme a k pôvodcovi týchto aktivít (teda k identite, pod ktorou pôvodca aktivít vystupoval). Monitorovanie systému spojené s vytváraním záznamu auditu umožňuje (niekedy) identifikovať podozrivé aktivity a spustiť poplach ešte pred vznikom bezpečnostného incidentu. Informácia v Politike KIB o tom, že sa vytvára záznam auditu a požiadavky na dostatočne silné metódy autentifikácie používateľom dávajú najavo, že FO je schopná vyvodiť zodpovednosť za aktivity v systéme. Privilegovaný používateľ (správca systému) má oprávnenia zasahovať aj do záznamu auditu. Aby nemohol vykonať nejakú nekalú aktivitu a následne upraviť záznam auditu, musí sa záznam auditu o činnosti privilegovaných používateľov vytvárať a uchovávať tak, aby k nemu nemali prístup. Pri vytváraní a spracovaní záznamov auditu je potrebné riešiť viacero technických podrobností, ktoré je vhodné popísať v technickejšom dokumente.

4 Referencie

[1] Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov
[2] Vyhláška Národného bezpečnostného úradu č. 362/2018, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení
[3] Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov
[4] 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
[5] Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (v znení č. 35/2019 Z. z.(nepriamo), 221/2019 Z. z.)
[6] Nariadenie európskeho parlamentu a rady (EÚ) 2016/679 z 27. apríla 2016 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 údajov) https://dataprotection.gov.sk/uoou/sites/default/files/nariadenie_2016_679_text_sk.pdf
[7] Povinnosti správcu ISVS v kybernetickej a informačnej bezpečnosti a postup pri ich napĺňaní. Metodický materiál MIRRI SR, jún 2021
[8] ISO/IEC 27001 — Information security management systems — Requirements.
[9] ISO/IEC 27002 — Code of practice for information security management.
[10] ISO/IEC 27005 — Information security risk management.
[11] BSI Standard 200-1 Information Security Management Systems (ISMS) www.bsi.bund.de/grundschutz
[12] BSI Standard 200-2 IT Grundschutz Methodology, www.bsi.bund.de/grundschutz
[13] IT-Grundschutz Compendium, BSI 2019 BSI - IT-Grundschutz (bund.de)
[14] BSI Standard 200-3 Risk Analysis based on IT-Grundschutz https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2003_en_pdf.html?nn=409850
[15] BSI Standard 100-4 Business Continuity Management https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-4_e_pdf.pdf?__blob=publicationFile&v=1
[16] Stratégia kybernetickej a informačnej bezpečnosti organizácie – metodický materiál MIRRI, 2021
[17] Olejár D. a kol. Základy kybernetickej a informačnej bezpečnosti, Univerzita Komenského v Bratislave, 2021 https://dspace.uniba.sk/handle/123456789/20
[18] Olejár D. Krátky úvod do informačnej a kybernetickej bezpečnosti a Malý výkladový slovník, MIRRI 2021
[19] Olejár D. Povinnosti správcu ITVS v kybernetickej a informačnej bezpečnosti a postup pri ich napĺňaní, MIRRI 2021
[20] Olejár D. Čo má obsahovať Politika kybernetickej a informačnej bezpečnosti pre II. a III. kategóriu ISVS a ako ju vypracovať, MIRRI 2021
[21] FIPS 199 Standards for Security Categorization of Federal Information and Information Systems
[22] FIPS 200 Minimum Security Requirements for Federal Information and Information Systems
[23] Computer Security Incident Handling Guide, NIST SP 800-61 Rev. 2 https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

[24]Information technology – Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response

[25]M. Souppaya, K. Scarfone Guide to Malware Incident Prevention and Handling for Desktops and Laptops, NIST Special Publication 800-83 Revision 1, NIST 2013
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf

5 Príloha. Zoznam použitých skratiek

BSI	Bundesamt für Sicherkeit in der Informationstechnik
FIPS	Federal Information processing Standard (us)
IEC	International Electrotechnical Commission
IKT	informačné a komunikačné technológie
IS	informačný systém
ISMS	Systém manažmentu informačnej bezpečnosti (Information security management system)
ISO	International Organization for Standardization
ISVS	informačný systém verejnej správy
IT	informačné technológie
KIB	kybernetická a informačná bezpečnosť
MIRRI	Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky