MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Smernica o bezpečnej prevádzke IS a sietí

Obsah

1 Správa dokumentu

Dokument „Smernica o bezpečnej prevádzke IS a sietí“ je vzorovým dokumentom slúžiacim pre potreby orgánov verejnej moci. Vytvorený vzor dokumentu nie je povinný na použitie a ani nie je záväzný. Dokument je poskytnutý voľne a bezplatne na využitie podľa potrieb konkrétnej organizácie.

Vytvorený dokument má aj svoj metodický rozmer, takže je ho možné použiť i pre potreby vzdelávania pracovníkov organizácií v oblasti kybernetickej a informačnej bezpečnosti.

Vytvorené dokument nie je určený na ďalší predaj alebo akúkoľvek inú komerčnú či obchodnú činnosť.

Tento dokument je určený sieťovým administrátorom a iným určeným zamestnancom organizácie.

Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky (ďalej aj „MIRRI“) nezodpovedá za nesprávne použitie predmetného dokumentu zo strany organizácie. Správne použitie a implementácia bezpečnostných opatrení je plne v kompetencii a zodpovednosti konkrétnej organizácie. Dokument je potrebné upraviť na základe reálnych potrieb a špecifického prostredia organizácie.

MIRRI si vyhradzuje právo na zmenu/úpravu predmetného dokumentu alebo čiastkových textov a tabuliek, a to v potrebnom rozsahu vrátane zmien verzií dokumentov. Dokument je výstupom pilotného projektu na ktorý nadväzuje Reforma Štandardizácia technických a procesných riešení kybernetickej a informačnej bezpečnosti (Plán obnovy a odolnosti).

Súčasťou každého dokumentu adaptovaného do prostredia organizácie je aj nasledovný zmenový list obsahujúci informácie minimálne v nasledovnom rozsahu:

Verzia	
Garant dokumentu	
Dátum poslednej revízie	
Dátum vydania	
Dátum účinnosti	

2 Riadenie bezpečnosti prevádzky IS a sietí

Manažér kybernetickej a informačnej bezpečnosti je v plnej miere zapojený do procesov týkajúcich sa riadenia bezpečnosti prevádzky IS a sietí. V prípade procesu riadenia zmien sa každá pripravovaná zmena predkladá manažérovi kybernetickej a informačnej bezpečnosti na vedomie. Manažér kybernetickej a informačnej bezpečnosti podrobí pripravovanú zmenu analýze za účelom identifikácie nakoľko sa konkrétna zmena týka oblasti kybernetickej a informačnej bezpečnosti. Na základe vykonanej analýzy manažér kybernetickej bezpečnosti zoberie pripravovanú zmenu na vedomie alebo, ak sa zmena týka oblasti kybernetickej a informačnej bezpečnosti, danú zmenu schváli, príp. neschváli.

2.1 Pravidlá prepájania systémov a prenosu elektronických informácií

Pravidlá prepájania systémov a prenosu elektronických informácií sú uvedené v nasledujúcich interných dokumentoch:

Bližší popis a relevantná interná dokumentácia bude doplnená zo strany organizácie. Predmetom tejto dokumentácie budú základné požiadavky na prepájanie systémov napr.:

- **využitie konfigurovateľných switchov a firewallov,**
- **vytváranie VLAN,**
- **zonácia (ideálne na vnútornú DMZ a vonkajšiu sieť).**

Taktiež sa v rámci dokumentácie uvedú bezpečnostné pravidlá prenosu elektronických informácií napr.:

- **vždy, ak je možné využiť bezpečné e-mailové protokoly (S/MIME),**
- **podpora kryptografického protokolu Transport Layer Security (TLS),**
- **pri prenose údajov v prostredí server-client využiť moderné kryptografické algoritmy (SFTP/SSH).**

2.2 Riadenie bezpečnosti sietí

Organizácia zabezpečuje ochranu informácií v sieťach a v podporných zariadeniach, ktoré ich v sieťach spracúvajú.

Siete sú v organizácii primerane riadené a spravované, čím sa zabezpečuje ochrana informácií v systémoch a aplikáciách.

Opatrenia sú v organizácii implementované na zaistenie bezpečnosti dát v sieťach a na ochranu pripojených služieb pred neautorizovaným prístupom. Organizácia najmä zvažuje nasledujúce opatrenia:

- určenie zodpovednosti a postupov riadenia vzdialených prostriedkov vrátane prostriedkov v používateľských oblastiach,
- zodpovednosť za prevádzku sietí tam, kde je to vhodné, je oddelená od prevádzky počítačov,
- zavedenie osobitných opatrení na zabezpečenie dôvernosti a integrity dát prenášaných verejnými sieťami alebo bezdrôtovými sieťami a na ochranu pripojených systémov a aplikácií osobitné

opatrenia môžu byť potrebné aj na udržiavanie dostupnosti sieťových služieb a pripojených počítačov,

- vykonávanie tvorby vhodných záznamov a monitorovanie, čím je zabezpečené zaznamenávanie činností, ktoré môžu ovplyvniť alebo byť relevantné pre informačnú bezpečnosť,
- aktivity manažmentu sú úzko koordinované pre optimalizáciu služieb pre organizáciu a zaisťujú to, aby sa opatrenia konzistentne aplikovali po celej infraštruktúre spracúvania informácií,
- systémy v sieti sú overené,
- systémové spojenia v sieti sú zakázané.

V prostredí organizácie je zavedená segmentácie siete, pričom detailná schéma je uvedená v topológii siete (príloha tohto dokumentu) so všetkými virtuálnymi LAN sieťami. Na perimetri organizácie sú bezpečnostné mechanizmy ako firewall, proxy server, e-mail gateway, a iné. Organizácia vnútri sietí vyžaduje monitoring sieťovej prevádzky, ktorý je zabezpečený pomocou monitorovacieho zariadenia. Logy z monitorovacieho zariadenia sa sledujú lokálne/centrálne/bezpečnostným monitoringom. Pripojenie z vonku je realizované cez VPN koncentrátor, ktorý slúži pre interných aj externých používateľov pri pripojení sa do vnútornej infraštruktúry. Administratívna budova je s pobočkami a dátovým centrom prepojená pomocou MPLS sietí poskytovaných telekomunikačným operátorom a navyše dochádza ku tunelovaniu kompletnej prevádzky. Prestupy medzi sieťami sú bližšie popísané v rámci kapitoly 2.1.

Riadenie bezpečnosti sietí je v organizácii prítomné v nasledujúcich dokumentoch:

Bližší popis a relevantná interná dokumentácia bude doplnená zo strany organizácie. Predmetom dokumentácie budú nasledovné oblasti:

- **sieťová zonácia v zmysle „leading practice“,**
- **fyzická ochrana prístupu, káblov a sieťových komponentov,**
- **separácia sietí na fyzickej vrstve,**
- **využitie firewallov,**
- **implementácie VPN prístupu,**
- **zabezpečenie bezpečnosti na transportnej vrstve (SSL, TLS),**
- **bezpečný prenos dát (SFTP),**
- **bezpečnosť webu (HTTPS),**
- **pravidelné vykonávanie penetračných testov a posudzovania zraniteľností,**
- **pravidelné audity bezdrôtových sietí.**

2.3 Riadenie zmien infraštruktúry

Základným cieľom riadenia zmien je zavedenie riadeného procesu implementácie zmenových požiadaviek do prostredia IKT s minimálnymi dopadmi na prevádzku a infraštruktúru IKT. Riadenie zmien môže v závislosti od typu a vyspelosti organizácie zahŕňať:

- formálnu inicializáciu zmeny prostredníctvom zadania požiadavky na zmenu (RFC),

- priradenie priority zmeny po posúdení dôležitosti a dopadov na infraštruktúru alebo koncových používateľov,
- proces priradenia RFC realizátorovi,
- plánovanie implementácie zmeny a proces autorizácie uvoľnenia zmeny do produkcie,
- post-implementačný proces pre vykonanie revízie či zmena splnila očakávania po nasadení.

Vyššie uvedené však závisí od možností samotnej organizácie.

Hlavné procesné kroky riadenia zmien sú:

- inicializácia zmeny,
- požiadavka na zmenu (RFC),
- klasifikácia priority zmeny,
- autorizácia (schválenie) zmeny,
- vykonanie zmeny,
- autorizácia nasadenia zmeny,
- revízia post-implementačného stavu nasadenia zmeny.

Proces riadenia zmien infraštruktúry je bližšie popísaný v dokumente:

- Realizácia služieb podpory, údržby a rozvoja APV.

2.4 Riadenie kapacity systémov a služieb

Účelom riadenia kapacít je určiť, koľko kapacity by sa malo poskytovať na základe informácií od vlastníkov služieb o tom, čo by sa malo poskytnúť. Riadenie kapacít sa týka najmä rýchlosti a efektívnosti. Ak sú prognózy IT kapacity presné a výška IT kapacity, ktorá je v prevádzke, zodpovedá potrebám, proces riadenia kapacity je úspešný.

Činnosti riadenia kapacity zahŕňajú:

- navrhovanie služieb s SLA pre výkon a kapacitu po ich implementácii,
- riadenie výkonnosti zdrojov tak, aby služby spĺňali SLA pre výkon a kapacitu,
- diagnostika problémov súvisiacich s výkonom,
- vytváranie a udržiavanie kapacitného plánu,
- nepretržitá kontrola aktuálnej kapacity služieb a výkonnosti služieb,
- zhromažďovanie a vyhodnocovanie údajov o využívaní služieb a dokumentovanie nových požiadaviek podľa potreby,
- riadenie implementácie zmien súvisiacich s kapacitou.

Organizácia identifikuje kapacitné požiadavky zohľadňujúce kritickosť predmetných systémov. Organizácia má zavedené monitorovanie systémov, aby sa zabezpečila dostupnosť a efektívnosť systémov a tiež detekčné opatrenia na indikovanie problémov počas prevádzky. Odhady budúcej kapacity berú do úvahy nové požiadavky organizácie a systémov a aktuálne aj budúce trendy dostupnosti

spracovateľskej kapacity organizácie.

Organizácia venuje výnimočnú pozornosť všetkým zdrojom s vysokými obstarávacími nákladmi a dlhou obstarávacou lehotou. Vedúci zamestnanci monitorujú používanie kľúčových systémových zdrojov a identifikujú trendy v používaní, najmä v súvislosti s aplikáciami alebo nástrojmi riadenia informačných systémov. Vedúci zamestnanci používajú tieto informácie na identifikovanie a prevenciu potenciálnych miest preťaženia a závislosti od kľúčového personálu, ktoré by mohli predstavovať hrozbu pre bezpečnosť systému.

Poskytnutie dostatočnej kapacity sa môže dosiahnuť rastom kapacity alebo znížením požiadaviek. Príklady riadenia kapacity zahŕňajú:

- mazanie nepotrebných údajov (priestor na disku),
- vyradenie aplikácií, systémov, databáz alebo prostredí,
- optimalizáciu skupinových procesov alebo časovanie,
- optimalizáciu aplikačnej logiky alebo databázových dopytov,
- zakázanie alebo obmedzenie šírky pásma pre zdroje náročné na služby, ak tie nie sú kritické (napr. posielanie videa).

2.5 Riadenie kryptografických opatrení

Dôvernosť, integrita, dostupnosť a hodnovernosť údajov v rámci sietí a informačných systémov, prostredníctvom ktorých je poskytovaná základná služba, je zabezpečená pomocou kryptografických prostriedkov používajúcich dostatočne odolné kryptografické mechanizmy, pričom sú určené pravidlá kryptografickej ochrany údajov pri ich prenose alebo uložení v rámci sietí a informačných systémov.

Systém správy kryptografických kľúčov a certifikátov je zabezpečený počas celého životného cyklu kryptografických kľúčov a certifikátov. Správa kryptografických kľúčov a certifikátov zahŕňa:

- bezpečné nakladanie s kryptografickými kľúčmi a certifikátmi,
- generovanie pseudonáhodných čísel a kľúčov, zriadenie, distribúciu, vkladanie, zmenu, obmedzenie platnosti, vyberanie, ukladanie a likvidáciu kľúčov a zrušenie certifikátov,
- umožnenie kontroly a auditu.

2.5.1 Kryptografické prostriedky

Pre zvýšenie informačnej bezpečnosti sú v prostredí IKT organizácie využívané nasledovné kryptografické prostriedky:

Bližší popis (napr. pevné disky v počítačoch s operačným systémom Windows – BitLocker alebo iný šifrovací nástroj, Unix Server – bez šifrovania, USB disky – špecializovaný šifrovací softvér, prehliadanie webu – HTTPS s TLS 3.0) a relevantná interná dokumentácia bude doplnená zo strany organizácie.

Požiadavku na použitie kryptografických prostriedkov predkladá príslušný vedúci zamestnanec.

Požiadavku na použitie kryptografických prostriedkov schvaľuje manažér kybernetickej a informačnej bezpečnosti.

2.5.2 Politika používania kryptografických opatrení

Pri vytváraní kryptografickej politiky berie organizácia do úvahy nasledovné:

- plány vedenia na používanie opatrení šifrovania v organizácii vrátane všeobecných princípov, pri ktorých by mali byť informácie chránené,
- v závislosti od posúdenia rizík požadovanú úroveň ochrany, ktorá musí byť určená tak, aby zohľadňovala typ, mohutnosť a kvalitu požadovaného šifrovacieho algoritmu šifrovania,
- používanie šifrovania na ochranu prenášaných informácií pomocou mobilných, prenosných médií alebo cez komunikačné linky,
- plány týkajúce sa riadenia kryptografických kľúčov vrátane metód ochrany kryptografických kľúčov a obnovenia zašifrovaných informácií v prípade straty, kompromitovania alebo poškodenia kryptografických kľúčov,
- roly a zodpovednosť za:
  - zavedenie politík,
  - správu kľúčov vrátane ich vytvárania,
- prijaté normy na efektívne zavedenie kryptografických opatrení,
- následky použitia šifrovaných informácií na opatrenia, ktoré organizácia prijala s cieľom kontroly obsahu (napr. detekcia škodlivého softvéru).

Kryptografické opatrenia sa môžu použiť na dosiahnutie najmä týchto cieľov informačnej bezpečnosti:

- dôvernosti - použitím šifrovania informácií na ochranu citlivých a kritických informácií, či uložených alebo prenášaných,
- integrity – použitím elektronického podpisu alebo správy o pôvodnosti kódu na overenie pôvodnosti alebo integrity uloženej alebo prenášanej citlivej alebo kritickej informácie,
- autentizácie – použitím kryptografických metód na autentizáciu používateľa a iných systémových entít, ktoré požadujú prístup alebo výmenu informácií so systémovými používateľmi, entitami a zdrojmi.

2.6 Bezpečnosť sieťových služieb

Bezpečnostné funkcie, úrovne služieb a manažérske požiadavky týkajúce sa všetkých sieťových služieb sú v organizácii identifikované a zahrnuté do ustanovení o sieťových službách v prípade, ak sa tieto služby poskytujú vnútroorganizačne alebo prostredníctvom outsourcingu.

Schopnosť poskytovateľa sieťových služieb riadiť dohodnuté služby bezpečným spôsobom je v organizácii ustanovená a pravidelne monitorovaná a je schválené právo na výkon auditu.

Bezpečnostné ustanovenia nevyhnutné pre jednotlivé služby, akými sú bezpečnostné funkcie, úrovne služieb a manažérske požiadavky, sú v organizácii identifikované. Organizácia je ubezpečená, že poskytovatelia sieťových služieb zavedú tieto opatrenia do praxe.

Sieťové služby zahŕňajú zavedenie spojení, súkromné sieťové služby a siete s pridanou hodnotou a spravované riešenia sieťovej bezpečnosti, akými sú firewally a systémy detekcie prienikov. Tieto služby siahajú od jednoduchej nespravovanej šírky pásma až po komplexné riešenia s pridanou

hodnotou.

Za bezpečnostné funkcie sieťových služieb sú považované:

- technológie aplikované na zaistenie bezpečnosti sieťových služieb, akými sú opatrenia týkajúce sa autentifikácie, šifrovania a sieťových pripojení,
- technické parametre nevyhnutné na realizáciu bezpečného pripojenia k sieťovým službám v súlade s pravidlami bezpečnosti a pravidlami sieťového pripojenia,
- v prípade potreby postupy týkajúce sa využívania sieťových služieb s cieľom obmedziť prístup k sieťovým službám alebo aplikáciám.

2.7 Oddeľovanie sietí

Skupiny informačných služieb, používateľov a informačných systémov sú v organizácii na sieťach segregované (oddeľované). Oddeľovanie je v organizácii vykonávané pomocou fyzicky rozdielnych sietí alebo pomocou oddelenia logickými sieťami (napr. virtuálne privátne siete).

Perimeter každej domény je v rámci organizácie správne definovaný. Prístup medzi sieťovými doménami je povolený, ale je riadený pomocou brány (napr. firewallu, smerovača s filtrom). Kritériá pre oddeľovanie sietí a povolený prístup sú založené na posúdení bezpečnostných požiadaviek každej domény. Posúdenie v organizácii je jednotné s bezpečnostnou politikou prístupov, s požiadavkami na prístupy, s úrovňou a klasifikáciou informácií, ktoré sa spracúvajú, a tiež s ohľadom na relatívne náklady a parametre výkonu po zapracovaní vhodnej technológie brán.

Pre citlivé prostredie je v organizácii prijaté pristupovanie k bezdrôtovým sieťam ako k prístupom zvonku a ich oddelenie od vnútorných sietí, ak prístup prešiel cez bránu v súlade s politikou riadenia sietí skôr, ako sa mu poskytol prístup do vnútornej siete.

Autentizácia, šifrovanie a stupeň používateľských prístupov poskytované modernými technológiami a normami pre bezdrôtové siete sú v organizácii dostatočné na priamy prístup do vnútorných sietí, a sú správne implementované.

2.8 Pravidlá bezpečnosti prevádzky

IT administrátori môžu vykonávať zmeny majúce vplyv na bezpečnosť len so súhlasom manažéra kybernetickej a informačnej bezpečnosti.

V prípade, ak má v konkrétnom informačnom systéme IT administrátor vytvorený aj bežný používateľský účet, tak všetky aktivity musia byť striktne oddelené a vykonávané pod príslušným účtom.

Organizácia v rámci svojich možností má zavedený bezpečnostný monitoring aktivít privilegovaných účtov. Organizácia takisto dbá na oddelenie právomocí a vedie prevádzkové záznamy na úrovni operačného systému, databáz a aplikácií.

Organizácia tiež zabezpečuje jasné pridelenie vlastníkov k IKT aktívam (informačné systémy, softvér, hardvér a pod.).

Inštalácie softvéru a hardvéru, ako aj riadenie záplat a ochrana pred škodlivým kódom sú súčasťou typických kontinuálnych procesov organizácie.

Privilegované prístupové oprávnenia sa do produkčného prostredia IS štandardne nepridelujú ani interným ani externým používateľom. Pre vývojové, testovacie a produkčné prostredie každého IS

musia byť formálne popísané a zdokumentované pravidlá pre prideľovanie privilegovaných oprávnení, ktoré musia obsahovať minimálne:

- popis postupov pridelenia oprávnení, resp. zriadenia účtov s takýmito oprávneniami,
- popis postupov aktivácie a deaktivácie oprávnení správcami IS,
- popis postupov nastavenia časových obmedzení pre platnosť oprávnení, resp. účtov,
- popis spôsobu monitorovania, zaznamenávania a zdokumentovania vykonaných aktivít privilegovanými používateľmi
- popis postupov finálneho zrušenia/odstránenia oprávnení, resp. účtov.

Pravidlá pre prideľovanie privilegovaných prístupových oprávnení do vývojových, testovacích a produkčných prostredí jednotlivých IS navrhuje príslušný administrátor IS.

Manažér kybernetickej a informačnej bezpečnosti posudzuje návrh pravidiel pre prideľovanie privilegovaných úplných administrátorských oprávnení.

Pravidlá pre prideľovanie privilegovaných prístupových oprávnení schvaľuje príslušný vedúci zamestnanec.

Schválené pravidlá uchováva príslušný administrátor IS.

Pravidlá sú aktualizované podľa potreby na základe podnetov administrátora IS.

Požiadavku na pridelenie privilegovaných prístupových oprávnení uplatňuje príslušný administrátor IS na svojho priameho nadriadeného.

Požiadavku na pridelenie privilegovaných prístupových oprávnení pre externých pracovníkov uplatňuje príslušný vlastník údajov alebo vlastník procesu na svojho priameho nadriadeného.

Požiadavka musí obsahovať minimálne:

- dôvody pre pridelenie úplných administrátorských oprávnení resp. dôvody pre zriadenie účtu (účtov) s takýmito oprávneniami,
- stručný popis aktivít, ktoré budú na IKT vykonávané,
- stručný popis kto, kedy a ako bude aktivity realizovať,
- časové obmedzenie pre platnosť oprávnení resp. účtu (účtov),
- identifikáciu IKT, v ktorých majú byť oprávnenia resp. účty zriadené,
- v prípade externých pracovníkov preukázateľné splnenie požiadaviek na zabezpečenie ochrany dôverných informácií (napr. doloženie príslušnej časti zmluvy, podpísaných prehlásení pracovníkov tretej strany, NDA a pod.).

Požiadavku na pridelenie oprávnení schvaľuje / zamieta príslušný vedúci zamestnanec.

Pri riadení prístupu v IS je potrebné zohľadniť:

- požiadavku na sprístupnenie len tých informácií, na ktoré má používateľ autorizáciu,
- požiadavku na realizáciu len tých operácií, na ktoré má používateľ autorizáciu,
- možnosti riadenia prístupu prostredníctvom dynamického menu IKT.

Používanie privilegovaných programov (utilít), ktoré môžu mať schopnosť obísť systémové a aplikačné

opatrenia, musí byť obmedzené a prísne riadené. V súvislosti s ich použitím je potrebné zohľadniť:

- používanie identifikačných, autentifikačných a autorizačných postupov pre systémové utility,
- oddelenie systémových utilít od aplikačného softvéru,
- obmedzenie používania systémových utilít na minimálny počet dôveryhodných a autorizovaných používateľov,
- autorizácia len pre konkrétne použitie systémových utilít,
- obmedzenie dostupnosti systémových utilít (napr. len po dobu trvania autorizovanej zmeny),
- zaznamenávanie každého použitia systémových utilít,
- definovanie a dokumentovanie autorizačných úrovní systémových utilít,
- odstraňovanie všetkých nepotrebných, na softvéri založených utilít zo systémového softvéru,
- nesprístupňovanie systémových utilít osobám, ktoré majú prístup k aplikáciám na systémoch, na ktorých sa vyžaduje uplatnenie segregácie povinností.

Pri riadení prístupu do LAN je potrebné zohľadniť:

- požiadavku na prístup do sietí, na ktoré má používateľ autorizáciu,
- požiadavku na sprístupnenie sieťových služieb, na ktoré má používateľ autorizáciu,
- obmedzenie sieťového prístupu stanovením zvláštnych logických domén,
- používanie špecifických aplikačných systémov a bezpečnostných brán pre externé pripojenia do siete a oddelenie sietí na zabránenie neobmedzenému / nekontrolovanému prechádzaniu po sieti a riadenie povolených komunikácií zdroja s cieľom cez bezpečnostné brány (firewall),
- smerovanie komunikácie v sieti,
- primeranú autentizáciu vzdialených užívateľov,
- stanovenie vyhradených liniek a telefónnych čísel a použitie vyhradených liniek alebo prostriedkov kontroly adresy používateľa siete (napr. procedúr spätného volania),
- využívanie bezpečnostných atribútov komunikačných protokolov.

V prípade ak organizácia využíva služby vládneho cloudu / DCOM musí sa riadiť príslušnými zmluvnými ustanoveniami upravujúcimi tento vzťah.

3 Bezpečnostný monitoring a ochrana pred škodlivým kódom

Cieľom monitorovania je zabezpečiť dostatočne rozsiahlu databázu údajov o prevádzke IS, aby bolo možné v krátkom čase realizovať opatrenia vedúce k zníženiu rizika výskytu bezpečnostných incidentov.

3.1 Určenie rozsahu monitorovania

Manažér kybernetickej a informačnej bezpečnosti spolu s administrátorom IS, príp. inými relevantnými technickými pracovníkmi sú zodpovední za určenie rozsahu monitorovania informačných aktív.

Monitorovanie informačných aktív poskytujúcich prístup do Internetu a elektronickej pošty sa vykonáva vždy.

Všetky informačné aktíva podliehajúce monitorovaniu, musia mať pridelený jednoznačný identifikátor.

Manažér kybernetickej a informačnej bezpečnosti spolu s administrátorom IS, príp. inými relevantnými technickými pracovníkmi vykonáva revíziu stanoveného rozsahu informačných aktív a monitorovania minimálne raz ročne.

3.2 Monitorovanie a zaznamenávanie činností

Súčasťou (výstupom) monitorovania sú auditné záznamy (logy), pričom ich sledovanie, ukladanie, vyhodnocovanie a zabezpečenie je v kompetencii administrátora IS a príslušného vedúceho zamestnanca.

Monitorovanie prevádzky informačného systému zabezpečuje administrátor IS alebo iná poverená osoba.

Osoby poverené monitorovaním prevádzky zároveň zabezpečujú a spravujú nástroje pre monitorovanie IKT/IS (HW aj SW).

3.3 Postupy ochrany proti škodlivému kódu

Riadením technickej zraniteľnosti organizácia znižuje zraniteľnosť, ktorú môže malvér zneužiť. Cieľom riadenia technickej zraniteľnosti je zhromažďovanie včasných informácií o technickej zraniteľnosti využívaných informačných systémov. Miera vystavenie sa zraniteľnosti je v organizácii pravidelne zhodnocovaná a sú zavedené príslušné opatrenia na potlačenie rizík.

Organizácia má implementované kontrolné mechanizmy, ktoré zabezpečujú, že systémy sú zabezpečené proti hrozbám a majú povolenú antivírusovú a antimalvérovú ochranu.

Kontrolné mechanizmy sú v organizácii vyvíjané, implementované a udržiavané za účelom zabezpečenia centrálnej správy ochrany proti škodlivému kódu. Za správu týchto kontrolných mechanizmov je v organizácii zodpovedný manažér kybernetickej a informačnej bezpečnosti.

Ochrana proti škodlivému kódu je založená na:

- detegovaní škodlivého softvéru,
- opravnom softvéri,
- primeranom systéme prístupu,

- opatreniach na riadenie zmien,
- dostatočnom bezpečnostnom povedomí pracovníkov.

Organizácia zabezpečuje ochranu všetkých informačných aktív, ktoré sú bežne postihnuteľné škodlivým kódom. Implementované kontrolné mechanizmy v organizácii poskytujú ochranu pred všetkými známymi typmi malvéru. Ide najmä o nasledovné:

- vírus,
- trojský kôň,
- červ,
- spyware,
- adware,
- ransomware,
- rootkit.

V rámci procesu ochrany proti škodlivému kódu využíva organizácia nástroje a techniky, ktoré analyzujú vlastnosti a správanie škodlivého kódu. Medzi takéto postupy patrí najmä:

- manuálne reverzné inžinierstvo,
- analýza kódu s využitím verejných, ale aj privátnych databáz obsahujúcich informácie o škodlivom kóde,
- analýza kódu uskutočnená tretími stranami,
- využitie spravodajských informácií,
- prediktívne strojové učenie.

Organizácia má jasne definované postupy a zodpovednosti v procese ochrany proti škodlivému softvéru. Tieto postupy a roly sú pravidelne aktualizované za účelom zabezpečenia účinného riadenia ochrany. Medzi takéto postupy patrí najmä:

- zabránenie šírenia malvéru,
- izolácia prostredia, kde môžu nastať katastrofické následky,
- implementácia plánov kontinuity na zabezpečenie obnovy činností po útoku malvéru (vrátane všetkých potrebných opatrení na zálohovanie a obnovu dát).

3.4 Kontrolné a monitorovacie aktivity

Ochrana pred škodlivým kódom je v organizácii viacúrovňová a zabezpečuje všetky vstupné body do IKT. Organizácia deteguje a zaznamenáva systémové činnosti a udalosti, ktoré sa odohrávajú na vstupných bodoch. Ide najmä o nasledovné aktivity:

- vyhľadávanie a vyšetrovanie údajov o incidentoch,
- triedenie upozornení a overovanie podozrivej aktivity,
- detekcia podozrivej aktivity,

- hľadanie hrozieb a zraniteľností.

Kontrolné a monitorovacie aktivity za účelom odhalenia prítomnosti škodlivého kódu sa v organizácii vykonávajú na pravidelnej báze. Monitorované sú najmä:

- servery,
- pracovné stanice,
- prenosné počítače,
- mobilné zariadenia.

Programy a súbory prístupné z internetu a vymeniteľných médií a tiež prichádzajúce e-maily podliehajú kontrole v reálnom čase. Organizácia má implementované kontrolné mechanizmy zabezpečujúce umiestnenie súborov, u ktorých bol zistený škodlivý kód, do karantény.

Organizácia vykonáva pravidelné revízie softvérového a dátového obsahu systémov na podporu kritických procesov. Prítomnosť akýchkoľvek neschválených súborov alebo neautorizovaných záplat je v organizácii formálne prešetrovaná.

Organizácia má ako preventívne opatrenie nainštalovaný a pravidelne aktualizovaný antivírusový detekčný a nápravný softvér na prezeranie pracovných staníc, prenosných počítačov a médií. Vykonávané kontroly zahŕňajú najmä:

- kontrolu všetkých súborov na elektronických alebo optických médiách ako aj súborov prijatých prostredníctvom siete z hľadiska prítomnosti škodlivého kódu ešte pred používaním,
- kontrolu príloh elektronickej pošty a stiahnutých súborov z hľadiska výskytu malvéru ešte pred ich spustením,
- kontrolu webových stránok z hľadiska výskytu malvéru.

Softvérové programy určené na ochranu pred škodlivým kódom sú v organizácii pravidelne aktualizované. V prípade aplikácie softvérových záplat, tzv. patches, je zabezpečené ich testovanie pred nasadením za účelom zabezpečenia, že tieto záplaty nebudú v konflikte so žiadnymi existujúcimi konfiguračnými nastaveniami.

Sú zavedené primerané plány kontinuity činnosti na obnovu po vírusových infekciách vrátane zálohovania všetkých potrebných dát a softvéru a dohôd týkajúcich sa obnovy.

Bližší popis konkrétnych nastavení bude doplnený zo strany organizácie.

4 Revízia dokumentu

Tento dokument sa reviduje a aktualizuje najmenej raz ročne.

Tento dokument sa aktualizuje aj častejšie, ak:

- vzíde požiadavka na jeho aktualizáciu,
- nastanú zásadné zmeny v organizácii a štruktúre,
- nastanú zásadné zmeny v legislatíve Slovenskej republiky s vplyvom na niektorú oblasť tohto dokumentu.

Za pravidelnú revíziu a aktualizáciu tohto dokumentu zodpovedá manažér kybernetickej a informačnej bezpečnosti.

Tento dokument a všetky jeho aktualizácie schvaľuje vedenie organizácie.

5 Prílohy

5.1 Príloha č. 1 – Popis prostredia

Bližší popis technickej schémy prostredia a relevantnej IT architektúry bude doplnený zo strany organizácie.