V Y H L Á ŠK AÚradu podpredsedu vlády SR pre investície a informatizáciu

z dd. mesiac 2019,  
ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy

Úrad podpredsedu vlády SR pre investície a informatizáciu podľa § 31 písm. a) a i) zákona č. xx/2019 Z. z. o informačných technológiách verejnej správy a o zmene a doplnení niektorých zákonov (ďalej len „zákon“) ustanovuje:

§ 1Základné ustanovenia

1. Táto vyhláška upravuje jednotlivé kategórie informačných technológií verejnej správy (ďalej len „ITVS“) a podrobnosti o spôsobe zaraďovania do týchto kategórií s použitím klasifikácie informácií a kategorizácie sietí a informačných systémov podľa osobitného predpisu[[1]](#footnote-1) na účely podľa § 11 ods. 4 zákona.
2. Táto vyhláška upravuje podrobnosti o bezpečnosti informačných technológií verejnej správy podľa § 18 až 23 zákona, obsahu bezpečnostných opatrení, obsahu a štruktúre bezpečnostného projektu a rozsah bezpečnostných opatrení v závislosti od klasifikácie informácií a od kategorizácie sietí a informačných systémov.
3. Orgán riadenia vo vzťahu k ITVS zavedie základné bezpečnostné opatrenia.
4. Orgán riadenia vo vzťahu k ITVS v jeho pôsobnosti vykoná klasifikáciu informačných aktív a kategorizáciu ITVS z hľadiska ich dôvernosti, integrity a dostupnosti.
5. Orgán riadenia vo vzťahu k ITVS zavedie špecifické bezpečnostné opatrenia pre jednotlivé kategórie dôvernosti, integrity a dostupnosti.
6. Orgán vedenia pre potreby implementácie požiadaviek zákona a tejto vyhlášky orgánu riadenia poskytne súbor materiálov, ktorý bude obsahovať šablóny a vzory dokumentácie bezpečnosti ITVS, návody, školiace materiály a ukážky podľa Prílohy č. 8.

§ 2

Klasifikácia informačných aktív

1. Informačné aktíva sa zaraďujú do klasifikačných stupňov na základe posúdenia dopadu narušenia ich dôvernosti, integrity a dostupnosti v zmysle ustanovení tejto vyhlášky. Mapovanie klasifikačných stupňov na klasifikačné stupne v zmysle osobitného predpisu1 je uvedené v Prílohe 11.
2. Z hľadiska dôvernosti sa informačné aktíva zaradia do klasifikačného stupňa:

C0 (verejné) pokiaľ neexistuje žiadna požiadavka na dôvernosť informačného aktíva,

C1 (interné) v prípade, ak narušenie dôvernosti aktíva môže mať obmedzený negatívny vplyv na orgán riadenia,

C2 (chránené) v prípade, ak narušenie dôvernosti aktíva môže mať závažný negatívny vplyv na orgán riadenia a

C3 (vysoko chránené) v prípade, ak narušenie dôvernosti aktíva môže mať obzvlášť závažný negatívny vplyv na orgán riadenia.

1. Z hľadiska integrity sa informačné aktíva zaradia do klasifikačného stupňa:

I0 (nepodstatná) pokiaľ narušenie integrity nemá žiadny vplyv na orgán riadenia,

I1 (nízka) pokiaľ narušenie integrity aktíva môže mať obmedzený negatívny vplyv na orgán riadenia

I2 (stredná) pokiaľ narušenie integrity aktíva môže mať závažný negatívny vplyv na orgán riadenia a

I3 (vysoká) pokiaľ narušenie integrity aktíva môže mať obzvlášť závažný negatívny vplyv na orgán riadenia.

1. Z hľadiska dostupnosti sa informačné aktíva zaradia do klasifikačného stupňa:

A0 (nepodstatná) pokiaľ narušenie dostupnosti nemá žiadny vplyv na orgán riadenia,

A1 (nízka) pokiaľ narušenie dostupnosti aktíva môže mať obmedzený negatívny vplyv na orgán riadenia,

A2 (stredná) pokiaľ narušenie dostupnosti aktíva môže mať závažný negatívny vplyv na orgán riadenia a

A3 (vysoká) pokiaľ narušenie dostupnosti aktíva môže mať obzvlášť závažný negatívny vplyv na orgán riadenia.

1. Príklady informačných aktív, negatívnych vplyvov na orgán riadenia a usmernenia pri klasifikácii informačných aktív sa nachádzajú v Prílohe 1.
2. Klasifikácia informačných aktív je zdokumentovaná a pri zmenách aktualizovaná a poskytnutá orgánu vedenia.
3. Pre klasifikačné stupne C2, I2, A2 a vyššie je zabezpečené označovanie informačných aktív.

§3

Kategorizácia informačných technológií verejnej správy

1. Zaradenie ITVS do jednotlivých kategórii dôvernosti, integrity a dostupnosti sa vykonáva na základe informačného aktíva v rámci ITVS s najvyšším klasifikačným stupňom.
2. Kategória ITVS je vyjadrená jednotlivými klasifikačnými stupňami dôvernosti, dostupnosti a integrity v tvare C(0,1,2,3)I(0,1,2,3)A(0,1,2,3)
3. Orgán riadenia zašle orgánu vedenia zoznam svojich ITVS s uvedenými kategóriami.

§4

Bezpečnostné opatrenia

(1) Bezpečnostné opatrenia tvoria základné bezpečnostné opatrenia štyroch úrovní a špecifické bezpečnostné opatrenia.

(2) Orgán riadenia pre tie ITVS, ktoré sú kategorizované ako C0I0A0 nie je povinný aplikovať bezpečnostné opatrenia.

(3) V prípade rozporu základných bezpečnostných opatrení rôznych úrovní, ktoré majú byť aplikované na konkrétne ITVS, majú prednosť ustanovenia opatrenia vyššej úrovne. V prípade rozporu základného bezpečnostného opatrenia so špecifickým bezpečnostným opatrením, ktoré majú byť aplikované na konkrétne ITVS, majú prednosť ustanovenia špecifického bezpečnostného opatrenia.

(3) Orgán riadenia vypracuje bezpečnostný projekt v rozsahu podľa Prílohy č. 10.

§5

Základné bezpečnostné opatrenia

1. Základné bezpečnostné opatrenia sú upravené v Prílohe č.2 a sú rozdelené do skupín Z0, Z1, Z2 a Z3.
2. Základné bezpečnostné opatrenia zo skupiny Z0 zavedie, okrem prevádzkovateľa základnej služby podľa osobitného predpisu2:
   1. Obec do 10000 obyvateľov,
   2. Miestny úrad obce do 10000 obyvateľov,
   3. Právnická osoba v zriaďovateľskej alebo zakladateľskej pôsobnosti orgánu riadenia uvedeného v §10 písmenách a) až d) zákona,
   4. fyzická osoba a iná právnická osoba, ako je uvedená v písmenách a) až f) zákona, okrem Národnej banky Slovenska, na ktorú je prenesený výkon verejnej moci alebo ktorá plní úlohy na úseku preneseného výkonu štátnej správy podľa osobitného predpisu,
   5. komora regulovanej profesie a komora, na ktorú je prenesený výkon verejnej moci s povinným členstvom.
3. Základné bezpečnostné opatrenia zo skupiny Z0 a Z1 zavedie, okrem prevádzkovateľa základnej služby podľa osobitného predpisu[[2]](#footnote-2):
   1. Obec nad 10000 obyvateľov,
   2. Miestny úrad obce nad 10000 obyvateľov,
   3. Úrady samosprávneho kraja,
   4. DataCentrum elektronizácie územnej samosprávy Slovenska,
   5. Úrad pre Slovákov žijúcich v zahraničí,
   6. komora regulovanej profesie a komora, na ktorú je prenesený výkon verejnej moci s povinným členstvom,
   7. Kancelária verejného ochrancu práv,
   8. Úrad komisára pre deti,
   9. Úrad komisára pre osoby so zdravotným postihnutím,
   10. Rada pre vysielanie a retransmisiu.
4. Základné bezpečnostné opatrenia zo skupiny Z0, Z1 a Z2 zavedie, okrem prevádzkovateľa základnej služby podľa osobitného predpisu2:
   1. Obec nad 100000 obyvateľov,
   2. Úrad pre reguláciu sieťových odvetví,
   3. Úrad pre reguláciu elektronických komunikácií a poštových služieb,
   4. Najvyšší kontrolný úrad SR,
   5. Úrad pre dohľad nad zdravotnou starostlivosťou,
   6. Úrad na ochranu osobných údajov SR,
   7. Ústav pamäti národa,
   8. Tlačová agentúra Slovenskej republiky,
   9. Rozhlas a televízia Slovenska,
   10. Generálna prokuratúra SR,
   11. Kancelária Súdnej rady Slovenskej republiky,
   12. Kancelária Najvyššieho súdu SR,
   13. Kancelária Ústavného súdu SR,
   14. Dopravný úrad,
   15. Kancelária prezidenta SR,
   16. Národná rada SR.
5. Základné bezpečnostné opatrenia zo skupiny Z0, Z1, Z2 a Z3 zavedie prevádzkovateľ základnej služby podľa osobitného predpisu2 a:
   1. ministerstvo,
   2. ostatný ústredný orgán štátnej správy,
   3. Sociálna poisťovňa,
   4. zdravotná poisťovňa,
6. Orgán riadenia podľa ods. (3) pre tie ITVS, ktoré sú kategorizované ako C2, I2 alebo A2, zavedie aj základné bezpečnostné opatrenia skupiny Z2.
7. Orgán riadenia podľa ods. (3) pre tie ITVS, ktoré sú kategorizované ako C3, I3 alebo A3 zavedie aj základné bezpečnostné opatrenia skupiny Z2 a Z3.
8. Orgán riadenia podľa ods. (4) pre tie ITVS, ktoré sú kategorizované ako C3, I3 alebo A3 zavedie aj základné bezpečnostné opatrenia skupiny Z3.
9. V prípade uplatnenia postupu podľa §28 ods. (2) orgán riadenia uvedený v §5 písmenách a) až d) zákona, môže právnickej osobe v svojej zriaďovateľskej alebo zakladateľskej pôsobnosti, okrem prevádzkovateľa základnej služby podľa osobitného predpisu2, uložiť aj zavedenie základných bezpečnostných opatrení skupín Z1-Z3 pre tie ITVS, ktoré sú kategorizované ako C1, I1, A1 a vyššie.

§6

Špecifické bezpečnostné opatrenia

Orgán riadenia podľa §5 ods. (5), právnická osoba, ktorej bolo uložené zavedenie základných bezpečnostných opatrení skupiny Z3 podľa §5 ods. (9) a prevádzkovateľ základnej služby podľa osobitného predpisu2 pre tie ITVS, ktoré sú kategorizované ako C3, I3 alebo A3 zavedie aj špecifické bezpečnostné opatrenia, ktoré sú upravené v Prílohe č.3.

§7

Výnimky

Akékoľvek výnimky z implementácie bezpečnostných opatrení sú orgánom vedenia zdokumentované, odôvodnené, schválené štatutárom a zaslané orgánu vedenia na schválenie.

**Príloha č. 1**

**k vyhláške č. xx/2019 Z. z.**

**PRÍKLADY INFORMAČNÝCH AKTÍV A NEGATÍVNYCH DOPADOV NA ORGÁN RIADENIA**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Klasifikačný stupeň** | **Príklad aktíva** | | | | | **Príklad incidentu** | | **Usmernenie** |
| **Papier** | **Dáta** | **Hardvér** | **Softvér** | **Nehmotné** | **Typ incidentu** | **Dopad** |
| **C0 - verejné** | Informačné brožúry, publikácie, formuláre, vizitky. | Informácie na web stránke, povinne zverejňované informácie. | Informačný kiosk, počítač pre hosťov. | Operačné systémy a aplikácie v DMZ. | Dobré meno, patenty, copyright, trademark. | Neaplikuje sa. | Neaplikuje sa. | Pre ochranu dôvernosti aktív v tomto stupni nie je potrebné aplikovať žiadne opatrenia, pretože ide o verejné aktíva, ktoré zo svojej povahy nie je potrebné nijako utajovať alebo inak chrániť pred vyzradením. |
| **C1 - interné** | Interné formuláre, interné listy, telefónny zoznam a bežná agenda. | Interné formuláre, interné listy, telefónny zoznam a bežná agenda. | PC, notebooky, USB kľúče, servery a iný HW obsahujúce dáta v klasifikačnom stupni C1. | Operačné systémy a aplikácie v internej sieti. | Interné jednania a postupy. | Útočník nájde v smetnom koši neaktuálny interný telefónny zoznam, ktorý nebol skartovaný. | Útočník má znalosť o internom usporiadaní orgánu riadenia, vie ju použiť pre útoky sociálnym inžinierstvom. | Pre ochranu aktív v tomto stupni je potrebné aplikovať aspoň súbor základných bezpečnostných opatrení kategórie Z1, pretože sa už nejedná o verejné informácie a aktíva, ale o aktíva určené na interné použitie, ktoré majú byť prístupné len osobám zvnútra orgánu riadenia. |
| **C2 - chránené** | Daňové tajomstvo, obchodné tajomstvo, informácie zmluvne označené za citlivé a požadujúce ochranu | Zdrojové kódy, proprietárne informácie, prihlasovacie údaje k používateľským účtom. | PC, notebooky, USB kľúče, servery a iný HW obsahujúce dáta v klasifikačnom stupni C2. | Operačné systémy, databázy a aplikácie na HW obsahujúcom dáta v klasifikačnom stupni C2. | Stratégie a plány, znalosti zamestnancov. | Útočník po prieniku do ITVS exfiltruje obchodné tajomstvo tretej strany. | Možný právny postih orgánu riadenia. | Aktíva v tomto stupni vyžadujú ochranu dôvernosti v rozsahu opatrení Z1 a Z2 a  ich vyzradením by orgán vedenia mohol byť sankcionovaný alebo by mohla byť ohrozená bezpečnosť ITVS. |
| **C3 - vysoko chránené** | Heslo k súkromnému kľúču, správy z auditov a penetračných testov. | Prihlasovacie údaje k administrátorským účtom. | PC, notebooky, USB kľúče, servery a iný HW obsahujúce dáta v klasifikačnom stupni C3. | Operačné systémy, databázy a aplikácie na HW obsahujúcom dáta v klasifikačnom stupni C3. | Know-how, obchodné tajomstvo, znalosti zamestnancov. | Útočník po prieniku do ITVS exfiltruje obchodné tajomstvo tretej strany. | Útočník získa kompletnú kontrolu nad ITVS a má prístup k vysoko chráneným informáciám. | Aktíva v tomto stupni vyžadujú najvyššiu možnú úroveň ochrany, pretože ich vyzradením by mohla byť vážne narušená bezpečnosť ITVS. |
| **I1 - nízka** | Poznámky, pomocné dokumenty, neaktuálne verzie dokumentov. | Poznámky, pomocné dokumenty, neaktuálne verzie dokumentov. | PC, notebooky, USB kľúče, servery a iný HW obsahujúce dáta v klasifikačnom stupni I1. | Operačné systémy, databázy a aplikácie na HW obsahujúcom dáta v klasifikačnom stupni I1. | Neformálne plány a návrhy. | Napadnutie pracovnej stanice obsahujúcej len dáta v klasifikačnom stupni I1 ransomvérom. | Zamedzený prístup k dátam na pracovnej stanici. |  |
| **I2 - stredná** | Bežná agenda, interné formuláre a dokumentácia. | Bežná agenda, interné formuláre a dokumentácia, informácie na webovej stránke. | PC, notebooky, USB kľúče, servery a iný HW obsahujúce dáta v klasifikačnom stupni I2. | Operačné systémy, databázy a aplikácie na HW obsahujúcom dáta v klasifikačnom stupni I2. | Znalosti zamestnancov. | Defacement webovej stránky, napadnutie pracovnej stanice obsahujúcej dáta v klasifikačnom stupni I2 ransomvérom. | Poškodenie dobrého mena inštitúcie, nedostupnosť dát a nemožnosť vykonávať bežnú agendu. |  |
| **I3 - vysoká** | Publikovaná legislatíva, rozhodnutia, havarijné plány, plány obnovy. | Prístupové oprávnenia, pravidlá na firewalle, kritické databázy. | PC, notebooky, USB kľúče, servery a iný HW obsahujúce dáta v klasifikačnom stupni I3, diagnostické prístroje | Webová stránka s právne záväznou legislatívou, webové aplikácie pre služby občanom | Know-how, obchodné tajomstvo. | Neoprávnená modifikácia dát o bankových účtoch. | Platby zaslané na nesprávne bankové účty. |  |
| **A1 - nízka** | Archivované dokumenty. | Zálohy dát, informácie na páskach. | PC, notebooky, USB kľúče, servery a iný HW obsahujúce dáta v klasifikačnom stupni A1. | Operačné systémy, databázy a aplikácie na HW obsahujúcom dáta v klasifikačnom stupni A1. | Neaplikuje sa. | Poškodenie zálohových médií. | Nedostupnosť záloh a nemožnosť rýchlej obnovy. |  |
| **A2 - stredná** | Bežná agenda, interné formuláre a dokumentácia. | Webová stránka | PC, notebooky, USB kľúče, servery a iný HW obsahujúce dáta v klasifikačnom stupni A2.  Mail server, Doménový radič | Operačné systémy, databázy a aplikácie na HW obsahujúcom dáta v klasifikačnom stupni A2. | Znalosti zamestnancov, know-how. | DDoS webovej stránky. | Nedostupnosť údajov na webovej stránke, poškodenie dobrého mena. |  |
| **A3 - vysoká** | Heslá k súkromnému kľúču | Elektronické služby občanom | Doménový radič, Mail server | Operačné systémy, databázy a aplikácie na HW obsahujúcom dáta v klasifikačnom stupni A3. | Know-how, postupy, znalosti a schopnosti zamestnancov. | DDoS na elektronické služby občanom. | Nedostupnosť služieb. |  |

**Príloha č. 2**

**k vyhláške č. xx/2019 Z. z.**

**ZÁKLADNÉ BEZPEČNOSTNÉ OPATRENIA**

**SKUPINA Z0**

Základným bezpečnostným opatrením je

a) automatická aktualizácia operačného systému a aplikácií,

b) používanie a automatická aktualizácia antivírusového softvéru, automatické skenovanie koncovej stanice aspoň raz mesačne,

c) práca pod používateľským kontom chráneným menom a heslom bez administrátorských privilégií, používanie administrátorského konta chráneného iným menom a heslom na vykonávanie činností súvisiacich so správou koncovej stanice,

d) používanie unikátnych hesiel s dĺžkou aspoň 9 znakov, ktoré je zložené z aspoň jedného veľkého písmena, jedného malého písmena, jedného čísla, jedného znaku a ktoré neobsahuje slovníkové slovo alebo jeho obmeny a jeho zmena aspoň raz ročne,

e) ochrana koncovej stanice prostredníctvom softvérového nástroja sieťovej bezpečnosti (ďalej len „firewall“),

f) zabezpečenie internetového smerovača pravidelnou aktualizáciou firmvéru, zmenou pôvodného mena a hesla, použitím WPA2 šifrovania, vypnutím WPS a vypnutím možnosti správy na diaľku,

g) odhlásenie sa alebo zamknutie koncovej stanice pri každom odchode z pracoviska.

**SKUPINA Z1**

**Z1-A Riadenie informačnej bezpečnosti**

Základným bezpečnostným opatrením pre riadenie informačnej bezpečnosti je

a) vypracovanie a schválenie bezpečnostnej politiky orgánu riadenia, ktorej obsahom je, okrem požiadaviek uvedených v zákone, aj :

1. určenie interného predpisu pre zálohovanie a určenie ktoré skupiny údajov, v akom rozsahu, akým spôsobom a s akou periodicitou sa zálohujú v prevádzkovej zálohe a archivačnej zálohe,

2. určenie dokumentov, ktoré orgán riadenia na zaistenie informačnej bezpečnosti vypracuje a uvedie ich zoznam,

3. určenie postupu pri revízii bezpečnostnej politiky orgánu riadenia vrátane periodicity pravidelných a dôvodov mimoriadnych revízií bezpečnostnej politiky a súvisiacich smerníc a dokumentov orgánu riadenia,

b) zabezpečenie realizácie a dodržiavania schválenej bezpečnostnej politiky orgánu riadenia,  
c) vypracovanie inventáru informačných aktív a určenie vlastníkov aktív zodpovedných za jednotlivé aktíva orgánu riadenia a ich zdokumentovanie.

**Z1-B Personálna bezpečnosť**

Základným bezpečnostným opatrením pre personálnu bezpečnosť je

a) zabezpečenie, aby boli všetci zamestnanci orgánu riadenia a osoby, ktoré vykonávajú činnosti pre orgán riadenia vyplývajúce zo zmluvných záväzkov (ďalej len „tretia strana“) poučení o schválenej bezpečnostnej politike orgánu riadenia a o povinnostiach z nej vyplývajúcich,  
b) zabezpečenie, aby boli zamestnanci orgánu riadenia a tretia strana poučení o svojich právach a povinnostiach predtým, ako získajú prístup k ITVS; v prípade rozdielnych práv a povinností pre rôzne ITVS sa poučenie zopakuje a jeho obsah sa primerane upraví,  
c) zabezpečenie, aby povinnosti vyplývajúce z bezpečnostnej politiky orgánu riadenia a z pracovného zaradenia zamestnanca boli uvedené v jeho pracovnej zmluve alebo inom dokumente týkajúcom sa jeho právneho vzťahu s orgánom riadenia,  
d) vypracovanie postupu pre disciplinárne konanie vo vzťahu k zamestnancovi alebo vo vzťahu k tretej strane, ktorí porušia bezpečnostnú politiku orgánu riadenia alebo niektorý zo súvisiacich predpisov,

e) zabezpečenie povinnosti zamestnancov oznamovať bezpečnostné incidenty v súlade so základnými bezpečnostnými požiadavkami Z1-I Monitorovanie a manažment bezpečnostných incidentov,  
f) vypracovanie postupu pri ukončení pracovného pomeru vlastného zamestnanca a pri ukončení spolupráce s externým pracovníkom alebo treťou stranou, ktorým sa pred ukončením pracovného pomeru zabezpečí

1. prípadné obmedzenie vo vzťahu k bývalému zamestnancovi, ktorým je najmä mlčanlivosť a obmedzenie na výkon činností po istú dobu po ukončení zamestnania,  
2. navrátenie pridelených zariadení, ktorými sú najmä počítače, smartfóny, pamäťové médiá, čipové karty a navrátenie informačných aktív, ktorými sú najmä programy, dokumenty a údaje,   
3. odstránenie informácií orgánu riadenia zo zariadení pridelených zamestnancovi, ktorými sú najmä počítače, notebooky, pamäťové médiá a ďalšie mobilné elektronické zariadenia,  
4. zrušenie prístupových práv do ITVS,

5. odovzdanie výsledkov práce v súvislosti s ITVS, ktorými sú najmä programy vrátane dokumentácie a vlastné elektronické dokumenty,

g) zabezpečenie, aby všetci zamestnanci absolvovali školenie na zvýšenie povedomia o informačnej bezpečnosti v rozsahu aspoň 2 hodiny ročne a v rozsahu špecifikovanom v Prílohe 7, novo prijatí zamestnanci absolvujú takéto školenie pred udelením prístupu k ITVS.

h) vedenie záznamov o absolvovaných a plánovaných školeniach podľa písmena g).

**Z1-D Kontrolný mechanizmus informačnej bezpečnosti**

Základným bezpečnostným opatrením pre kontrolný mechanizmus informačnej bezpečnosti je

a) dodržiavanie bezpečnostnej politiky orgánu riadenia a zabezpečenie, vykonávanie a dokumentácia internej kontroly informačnej bezpečnosti, ktorej periodicita sa určuje v bezpečnostnej politike orgánu riadenia,

b) zabezpečenie archivácie, ochrany a vyhodnocovania správ z interných kontrol

c) umožnenie orgánu vedenia vykonať pravidelné, neinvazívne hodnotenie zraniteľnosti podľa §23 ods. (5) písm. c, ktoré pozostáva prevažne z:

1. overenia prítomnosti špecifických hostov v sieti,

2. preverenia DNS záznamov na prítomnosť informácií o sieťovej infraštruktúre,

3. preverenia dostupnosti špecifických služieb, ich typov a verzií,

4. preverenia prítomnosti špecifických súborov a overenie ich verzie,

5. preverenia špecifických hodnôt v registri a identifikáciu inštalovaného softvéru, jeho verzií a aktualizácií,

6. preskúmania hlavičiek paketov zo vzorky sieťovej prevádzky zachytenej počas bežnej prevádzky,

7. skenovania portov,

8. overenia použitia výrobných hesiel bez použitia útoku hrubou silou,

9. automatickej identifikácie zraniteľností,

10. použitia maximálne 10 súčasne spustených procesov skenovania.

**Z1-E Ochrana proti škodlivému kódu**

Základným bezpečnostným opatrením pre ochranu proti škodlivému kódu je

a) zavedenie ochrany ITVS pred škodlivým kódom najmenej v rozsahu

1. kontroly prichádzajúcej elektronickej pošty na prítomnosť škodlivého kódu a nepovolených typov príloh,

2. detekcie prítomnosti škodlivého kódu na všetkých používaných zariadeniach ITVS,  
3. kontroly súborov prijímaných zo siete internet a odosielaných do siete internet na prítomnosť škodlivého softvéru,

4. detekcie prítomnosti škodlivého kódu na všetkých webových sídlach orgánu riadenia,

b) zavedenie ochrany pred nevyžiadanou elektronickou poštou,

c) používanie len aktuálneho a legálneho softvéru, ktorý je povolený príslušnými internými predpismi orgánu riadenia,

d) vypracovanie interného predpisu upravujúceho pravidlá pre sťahovanie súborov prostredníctvom externých sietí.

**Z1-F Sieťová bezpečnosť**

Základným bezpečnostným opatrením pre sieťovú bezpečnosť je

a) zabezpečenie ochrany vonkajšieho a interného prostredia prostredníctvom hardvérového alebo softvérového firewallu filtrovaním prichádzajúcej a odchádzajúcej sieťovej prevádzky na princípe najnižšieho privilégia,

b) vedenie evidencie o všetkých miestach prepojenia sietí v správe orgánu riadenia vrátane prepojení s externými sieťami,

c) zabezpečenie, aby pre každé prepojenie podľa písmena b) bol vypracovaný interný akt riadenia prístupu medzi týmito sieťami v súlade so základnými bezpečnostnými požiadavkami Z1-M Riadenie prístupu,

d) vypracovanie dokumentácie o sieti vrátane topológie siete a využitia IP rozsahov a udržiavanie dokumentácie v aktuálnom stave.

**Z1-G Fyzická bezpečnosť a bezpečnosť prostredia**

Základným bezpečnostným opatrením pre fyzickú bezpečnosť a bezpečnosť prostredia je  
a) umiestnenie ITVS v takom priestore, aby ITVS alebo aspoň jeho najdôležitejšie komponenty boli chránené pred nepriaznivými prírodnými vplyvmi a vplyvmi prostredia, možnými dôsledkami havárií technickej infraštruktúry a fyzickým prístupom nepovolaných osôb (ďalej len „zabezpečený priestor“), zabezpečeným priestorom je najmä serverovňa,

b) oddelenie zabezpečeného priestoru od ostatných priestorov fyzickými prostriedkami najmä stenami a zábranami,

c) zabezpečenie, aby sa v okolí zabezpečeného priestoru nevyskytovali zariadenia, ktorými sú najmä kanalizácia a vodovod alebo materiály, ktorými sú najmä horľaviny, ktoré by mohli ohroziť ITVS umiestnený v tomto zabezpečenom priestore,

d) vypracovanie a implementácia interného predpisu upravujúceho pravidlá pre prácu v zabezpečenom priestore,

e) zabezpečenie, aby bola prevádzka, používanie a manažment ITVS v súlade s osobitnými predpismi, internými predpismi orgánu riadenia a jej zmluvnými záväzkami,

f) vypracovanie, zavedenie a kontrola dodržiavania pravidiel pre:

1. údržbu, uchovávanie a evidenciu technických komponentov ITVS a zariadení ITVS,

2. používanie zariadení ITVS na iné účely, na aké boli pôvodne určené,

3. používanie zariadení ITVS mimo určených priestorov,

4. vymazávanie, vyraďovanie a likvidovanie zariadení ITVS a všetkých typov relevantných záloh,

5. prenos technických komponentov ITVS alebo zariadení ITVS mimo priestorov orgánu riadenia,  
6. narábanie s elektronickými dokumentmi, dokumentáciou systému, pamäťovými médiami, vstupnými a výstupnými údajmi ITVS tak, aby sa zabránilo ich neoprávnenému zverejneniu, odstráneniu, poškodeniu alebo modifikácii.

**Z1-H Aktualizácia softvéru**

Základným bezpečnostným opatrením pre aktualizáciu softvéru je

a) vykonávanie pravidelnej aktualizácie softvéru, predovšetkým operačných systémov, kancelárskych balíkov, webových prehliadačov a inštalovaných aplikácií bez zbytočného odkladu,

b) pravidelné vykonávanie aktualizácie inštalovaného ochranného softvéru, zabezpečujúceho ochranu v súlade so základnými požiadavkami Z1-E Ochrana proti škodlivému kódu a Z1-F Sieťová bezpečnosť, vrátane zabezpečenia všetkých ostatných komponentov a pripájaných prostriedkov bez zbytočného odkladu.

**Z1-I Monitorovanie a manažment bezpečnostných incidentov**

Základným bezpečnostným opatrením pre monitorovanie a manažment bezpečnostných incidentov je

a) vypracovanie interného predpisu obsahujúceho postup pri ohlasovaní, riešení a evidencii bezpečnostných incidentov a odhalených zraniteľností ITVS, najmä za účelom včasného prijatia preventívnych a nápravných opatrení a jeho dodržiavanie,

b) zabezpečenie, aby o postupoch podľa písmena a) boli primeraným spôsobom informovaní všetci používatelia ITVS, a aby boli tieto postupy dodržiavané,

c) vytvorenie a prevádzka kontaktného miesta orgánu riadenia pre ohlasovanie bezpečnostných incidentov a odhalených zraniteľností ITVS v správe orgánu riadenia.

**Z1-K Zálohovanie**

Základným bezpečnostným opatrením pre zálohovanie je

a) zabezpečenie vytvorenia archivačnej zálohy a prevádzkovej zálohy podľa periodicity určenej v bezpečnostnej politike orgánu riadenia v závislosti na klasifikácii dotknutých aktív,

b) fyzické ukladanie prevádzkových záloh, jednej kópie archivačnej zálohy a kópií inštalačných médií s plateným softvérom do uzamykateľného priestoru.

**Z1-M Riadenie prístupu**

Základným bezpečnostným opatrením pre riadenie prístupu je

a) zavedenie identifikácie používateľa a následnej autentifikácie pri vstupe do ITVS,  
b) vypracovanie interného predpisu upravujúceho riadenie prístupu k údajom a funkciám ITVS založenom na zásade, že používateľ má prístup iba k tým údajom a funkciám, ktoré sú potrebné na vykonávanie jeho úloh,

c) určenie postupu a zodpovednosti v súvislosti s prideľovaním prístupových práv používateľom,  
d) určenie požiadaviek, ktoré majú používatelia v súlade s bezpečnostnou politikou orgánu riadenia dodržiavať pri používaní ITVS,

e) zaznamenávanie zmien v pridelenom prístupe a ich archivácia podľa bezpečnostnej politiky orgánu riadenia,

f) určenie bezpečnostných zásad pre mobilné pripojenie do ITVS a pre prácu na diaľku; mobilným pripojením je najmä prenosný počítač, smartfón alebo tablet,

g) umožniť fyzickým osobám zodpovedným za správu a prevádzku ITVS prístup iba k takým údajom a funkciám v týchto ITVS, ktoré nevyhnutne potrebujú na vykonávanie pridelených úloh,  
h) automatické zaznamenávanie každého prístupu administrátora do ITVS a automatické zaznamenávanie prístupu používateľa pokiaľ je to technicky možné,

i) vedenie formalizovanej dokumentácie prístupových práv všetkých používateľov ITVS,

j) ukladanie všetkých hesiel v nereverzibilnom formáte vždy, keď je to možné, pričom prípady, kedy to nie je možné musia byť odôvodnené a zdokumentované.

**Z1-N Aktualizácia informačno-komunikačných technológií**

Základným bezpečnostným opatrením pre aktualizáciu informačno-komunikačných technológií je

a) stanovenie bezpečnostných požiadaviek pri zavádzaní nových alebo pri zmenách v existujúcich ITVS,

b) nasadzovanie bezpečnostných záplat na klientskych systémoch, serveroch a na sieťových a bezpečnostných prvkoch bez zbytočného odkladu,

c) vymenovanie zodpovedného zástupcu dodávateľa, ak je dodávateľom činnosti podľa písmena a) a b) tretia strana.

**Z1-O Účasť tretej strany**

Základným bezpečnostným opatrením pre účasť tretej strany je

a) zabezpečenie, aby boli v zmluvách s treťou stranou o poskytovaní služieb súvisiacich s ITVS uvedené bezpečnostné požiadavky na tieto služby,

b) zamedzenie prístupu tretích strán ku všetkým údajom v ITVS, ktoré sa považujú za aktíva, alebo umožnenie prístupu tretích strán k takýmto údajom len na základe zmluvy tak, aby nebola narušená bezpečnosť ITVS a bezpečnostná politika orgánu riadenia,

c) zabezpečenie kontroly plnenia bezpečnostných požiadaviek podľa písmena b).

**Z1-Q Kryptografia**

Základným bezpečnostným opatrením pre kryptografiu je:

a) webový portál musí byť prístupný prostredníctvom protokolu HTTPS, len s využitím TLS od verzie 1.1[[3]](#footnote-3) a vyššie.

**SKUPINA Z2**

**Z2-A Riadenie informačnej bezpečnosti**

Základným bezpečnostným opatrením pre riadenie informačnej bezpečnosti je

a) vypracovanie a schválenie bezpečnostnej politiky orgánu riadenia, ktorej obsahom je

1. určenie všeobecných a špecifických zodpovedností a povinností v oblasti informačnej bezpečnosti a stanovenie potrebných pozícií pre manažment informačnej bezpečnosti,

2. určenie privilegovaných používateľských rolí v ITVS, určenie bezpečnostných požiadaviek na jednotlivé privilegované používateľské roly a určenie, ktoré používateľské roly nie je možné navzájom zlúčiť; privilegovanými používateľskými rolami je najmä správca systému,

3. určenie rámca pre manažment rizík u orgánu riadenia v súvislosti s aktívami, od ktorých závisí činnosť ITVS, alebo ktoré závisia od činnosti ITVS; rámec určí, najmä ktoré aktíva sú pre orgán riadenia kritické, čo ich ohrozuje a zásady ich ochrany,

b) určenie jednotlivých úloh osoby alebo osôb zodpovedných za informačnú bezpečnosť v súlade s bezpečnostnou politikou orgánu riadenia,

c) zabezpečenie koordinácie aktivít organizačných zložiek orgánu riadenia pri zaisťovaní informačnej bezpečnosti v súlade s bezpečnostnou politikou.

**Z2-B Personálna bezpečnosť**

Základným bezpečnostným opatrením pre personálnu bezpečnosť je absolvovanie školenia všetkých zamestnancov orgánu riadenia na zvýšenie povedomia o informačnej bezpečnosti v rozsahu aspoň 4 hodiny ročne v rozsahu špecifikovanom v Prílohe 7 a preverovanie ich vedomostí aspoň raz za rok písomným alebo elektronickým testovaním a vedenie záznamov o školeniach a testovaní; novoprijatí zamestnanci absolvujú takéto školenie a testovanie pred udelením prístupu k ITVS. Toto opatrenie nahrádza opatrenie Z1-B písm. g) a h).

**Z2-C Manažment rizík pre oblasť informačnej bezpečnosti**

Základným bezpečnostným opatrením pre manažment rizík pre oblasť informačnej bezpečnosti je

a) implementácia systému riadenia a monitorovania rizík v súvislosti s ITVS, a to najmä podľa relevantných technických noriem a pravidelné zbieranie relevantných údajov súvisiacich s rizikami,

b) identifikácia, analýza a hodnotenie rizík spojených s využívaním aktív a ITVS mimo priestorov orgánu riadenia a zavedenie primeraných postupov a opatrení na redukciu týchto rizík.

**Z2-D Kontrolný mechanizmus informačnej bezpečnosti**

Základným bezpečnostným opatrením pre kontrolný mechanizmus informačnej bezpečnosti je

a) dodržiavanie bezpečnostnej politiky orgánu riadenia a zabezpečenie a vykonávanie interného auditu informačnej bezpečnosti, ktorého periodicita sa určuje v bezpečnostnej politike orgánu riadenia,

b) zabezpečenie archivácie, ochrany a vyhodnocovania auditných správ.

**Z2-F Sieťová bezpečnosť**

Základným bezpečnostným opatrením pre sieťovú bezpečnosť je

a) umiestnenie sieťového firewallu na perimetri siete a prepojeniach s verejne dostupnými sieťami s filtrovaním prichádzajúcej a odchádzajúcej sieťovej prevádzky na princípe najnižšieho privilégia,

b) zabezpečenie ochrany pracovných staníc prostredníctvom lokálnych softvérových firewallov na princípe najnižšieho privilégia aspoň pre prichádzajúcu komunikáciu,

c) zabezpečenie ochrany serverov prostredníctvom lokálnych softvérových firewallov na princípe najnižšieho privilégia pre prichádzajúcu aj odchádzajúcu komunikáciu,

d) vykonanie hardeningu všetkých serverov, sieťových a bezpečnostných prvkov,

e) synchronizácia času všetkých ITVS v sieti s dôveryhodným NTP serverom,

f) zabezpečenie prístupu používateľov k Internetu a k službám mimo siete orgánu riadenia cez proxy server a uchovávanie prístupových logov aspoň 4 mesiace,

g) uchovávanie log záznamov o autentifikácii používateľov aspoň 6 mesiacov,

h) používanie výhradne interného DNS servera a uchovávanie logov DNS dopytov aspoň 4 mesiace,

i) uchovávanie logov o IP adresách pridelených prostredníctvom DHCP aspoň 4 mesiace,

j) rozdelenie siete do jednotlivých segmentov podľa účelu aspoň na sieť perimetra (DMZ), klientsky segment, segment interných serverov a manažment segment,

k) zabezpečenie logovania sieťových spojení s externými sieťami na sieťových prvkoch a to minimálne na úrovni šestice časová pečiatka, zdrojová IP adresa, cieľová IP adresa, protokol, zdrojový port, cieľový port a ich uchovávanie aspoň 4 mesiace,

l) konfigurácia maximálneho počtu aktívnych MAC adries na potrebný počet (maximálne 3) pre klientske porty na prístupových switchoch.

**Z2-G Fyzická bezpečnosť a bezpečnosť prostredia**

Základným bezpečnostným opatrením pre fyzickú bezpečnosť a bezpečnosť prostredia je

a) zaistenie prístupu k serverovým a sieťovým komponentom iba oprávneným osobám napr. pomocou uzamykateľných serverových skríň,

b) udelenie prístupu do zabezpečeného priestoru len osobám, ktorý tento prístup nevyhnutne potrebujú na výkon svojich pracovných činností,

e) vedenie sieťovej kabeláže iba v priestoroch pod kontrolou orgánu riadenia alebo použitie šifrovania dát,

g) stanovenie parametrov pre ITVS, ktoré definujú maximálnu prípustnú dobu výpadku ITVS a vytvorenie a zavedenie opatrení, ktoré sú zamerané na riešenie obnovy prevádzky v prípade výpadku ITVS,

h) zabezpečenie ochrany pred výpadkom zdroja elektrickej energie pre tie časti ITVS, ktoré vyžadujú nepretržitú prevádzku a zabezpečenie, aby takýto výpadok nenastal, pomocou UPS.

**Z2-I Monitorovanie a manažment bezpečnostných incidentov**

Základným bezpečnostným opatrením pre monitorovanie a manažment bezpečnostných incidentov je

a) vypracovanie interného aktu obsahujúceho

1. postup pri riešení jednotlivých typov[[4]](#footnote-4) bezpečnostných incidentov a spôsob ich vyhodnocovania,

2. spôsob evidencie bezpečnostných incidentov a použitých riešení,

b) implementácia prevádzkového dohľadu počas bežnej pracovnej doby,

c) denná kontrola, preverovanie a riešenie hlásení bezpečnostných nástrojov, ktorými sú najmä nástroj na detekciu škodlivého kódu a IDS/IPS.

**Z2-J Periodické hodnotenie zraniteľností**

Základným bezpečnostným opatrením pre periodické hodnotenie zraniteľností je pravidelné hodnotenie slabých miest a ohrození ITVS v rozsahu podľa bezpečnostnej politiky orgánu riadenia s periodicitou najmenej raz ročne.

**Z2-K Zálohovanie**

Základným bezpečnostným opatrením pre zálohovanie je

a) vyhotovenie archivačnej zálohy v dvoch kópiách,

b) zabezpečenie vykonania testu funkcionality dátového nosiča archivačnej zálohy a prevádzkovej zálohy a v prípade nefunkčnosti, najmä pri nečitateľnosti alebo chybách pri čítaní, opätovné vytvorenie zálohy na inom dátovom nosiči,

c) zabezpečenie vykonania testu obnovy ITVS a údajov z prevádzkovej zálohy najmenej raz za jeden rok,

d) fyzické ukladanie druhej kópie archivačnej zálohy v inom objekte ako sa nachádzajú technické prostriedky ITVS, ktorého údaje boli archivované tak, aby bolo minimalizované riziko poškodenia alebo zničenia dátových nosičov archivačnej zálohy v dôsledku požiaru, záplavy alebo inej živelnej pohromy.

**Z2-M Riadenie prístupu**

Základným bezpečnostným opatrením pre riadenie prístupu je

a) implementácia centrálnej správy identít (IDM),

b) vypracovanie a pravidelná aktualizácia zoznamu privilegovaných prístupových oprávnení a ich preskúmavanie aspoň jeden krát ročne.

**Z2-N Aktualizácia informačno-komunikačných technológií**

Základným bezpečnostným opatrením pre aktualizáciu informačno-komunikačných technológií je

a) vypracovanie a zavedenie interných postupov upravujúcich riadenie zmien s počiatočným stanovením a zahrnutím bezpečnostných požiadaviek a schvaľovacieho procesu pre

1. zmenu konfigurácie, zavádzanie nových alebo aktualizáciu a rozširovanie funkcionality existujúcich ITVS alebo ich častí; v prípade automatizovanej on-line aktualizácie sa schvaľovanie zavádza iba, ak si vyžaduje finančné zdroje alebo je aktualizácia príliš rozsiahla,  
2. zavádzanie nových informačno-komunikačných technológií u orgánu riadenia najmä s ohľadom na zaistenie kompatibility a zachovanie potrebnej úrovne bezpečnosti,

b) vymenovanie zástupcu správcu alebo prevádzkovateľa ITVS, zodpovedného za informačnú bezpečnosť a činnosti podľa písmena a),

c) vypracovanie a zavedenie interných postupov upravujúcich manažment záplat na klientskych systémoch, serveroch a na sieťových a bezpečnostných prvkoch,

d) pre podpornú infraštruktúru ITVS kategórie A3 zaistenie náhradných komponentov ITVS a SLA s dodávateľmi na opravu poškodených častí ITVS do 48 hodín.

e) uchovávanie a aktualizácia dokumentácie o ITVS alebo ich častiach, ktorá obsahuje

1. používateľskú dokumentáciu, ktorou je návod na používanie ITVS,

2. administrátorskú dokumentáciu, ktorou je návod na správu a prevádzku ITVS v takom rozsahu, aby na jej základe mohla byť vykonávaná plnohodnotná administrácia ITVS,  
3. prevádzkovú dokumentáciu, ktorou je dokumentácia o architektúre ITVS alebo jeho časti, jeho konfigurácii a väzbách na existujúce ITVS v takom rozsahu, aby na jej základe mohla byť vykonávaná plnohodnotná prevádzka ITVS,

f) vykonanie testovania implementácie požiadaviek podľa Z1-N písmena a) a vytvorenie dokumentácie o spôsobe testovania a o dosiahnutých výsledkoch, a to najmenej vykonanie interného používateľského testovania v rozsahu najmenej jedného týždňa pred odovzdaním ITVS, jeho časti alebo súvisiacej aplikácie dodávateľom a zahrnutie jeho výstupov do dokumentácie o spôsobe testovania a o dosiahnutých výsledkoch.

**Z2-O Účasť tretej strany**

Základným bezpečnostným opatrením pre účasť tretej strany je analýza rizík v súvislosti s ITVS v súlade s požiadavkami v Z1-C Manažment rizík pre oblasť informačnej bezpečnosti, vyplývajúcich z činnosti tretích strán v týchto ITVS, najmä dodávateľov, externých spolupracovníkov, orgánov verejnej správy, fyzických osôb a zaistenie takých technických, organizačných a právnych podmienok pre činnosť tretích strán v ITVS, aby nebola narušená bezpečnosť ITVS a bezpečnostná politika orgánu riadenia.

**Z2-P Federácia identít**

Základným bezpečnostným opatrením pre federáciu identít je používanie protokolu Security Assertion Markup Language (SAML) vo verzii 2.0 podľa Organization for the Advancement of Structured Information Standards (OASIS) pri federácii identít ITVS, pričom ak je poskytovateľom identít správca ústredného portálu verejnej správy

a) pre protokol Security Assertion Markup Language (SAML) sa používa

1. profil Web Browser Single Sign-On Profile s technickým spôsobom jeho vykonania prostredníctvom HTTP-POST alebo HTTP-Redirect, alebo

2. profil Single Logout Profile s technickým spôsobom jeho vykonania prostredníctvom HTTP-POST, HTTP-Redirect alebo Simple Object Access Protocol (SOAP) minimálne vo verzii 1.2,

b) dátová štruktúra Security Assertion Markup Language (SAML) Assertion pre prenos autentifikačných informácií medzi poskytovateľom služby a poskytovateľom identity má atribúty podľa Prílohy č.4 a

c) v prípade používania federácie identít je zaistené, že všetci poskytovatelia identity v rámci federácie spĺňajú bezpečnostné požiadavky orgánu riadenia.

**Z2-Q Kryptografia**

Základným bezpečnostným opatrením pre kryptografiu je

a) podpora zabezpečenia autenticity a integrity súborov pomocou kryptografických prostriedkov, ktorým je najmä elektronický podpis,

b) podpora zabezpečenia dôvernosti elektronických dokumentov prostredníctvom šifrovania,

c) šifrovanie dát na všetkých prenosných zariadeniach, ktoré sú vynášané mimo priestorov orgánu riadenia,

d) podpora elektronického podpisovania emailovej komunikácie,

e) podpora asymetrického šifrovania emailovej komunikácie.

**Z2-R Používateľské účty**

Základným bezpečnostným opatrením pre používateľské účty je

a) zavedenie pravidiel zakazujúcich zdieľanie používateľských hesiel do ITVS, pokiaľ je to technicky možné,

b) zavedenie pravidiel pre zmenu používateľských hesiel s frekvenciou aspoň 1 rok.

**SKUPINA Z3**

**Z3-A Riadenie informačnej bezpečnosti**

Základným bezpečnostným opatrením pre riadenie informačnej bezpečnosti je

a) implementácia systému riadenia kontinuity činností na základe analýzy rizík a analýzy dopadov,

b) vypracovanie, pravidelné testovanie a aktualizácia interných predpisov upravujúcich riadenie kontinuity činností, havarijných plánov a plánov obnovy.

**Z3-B Personálna bezpečnosť**

Základným bezpečnostným opatrením pre personálnu bezpečnosť je

a) určenie rolí, zodpovedností a komunikačných matíc pre zaistenie kontinuity činností,

b) zaistenie a formálne definovanie zastupiteľnosti zamestnancov,

c) absolvovanie školenia všetkých zamestnancov orgánu riadenia na zvýšenie povedomia o informačnej bezpečnosti v rozsahu aspoň 6 hodín ročne v rozsahu špecifikovanom v Prílohe 7 a preverovanie ich vedomostí aspoň raz za rok písomným alebo elektronickým testovaním a vedenie záznamov o školeniach a testovaní; novoprijatí zamestnanci absolvujú takéto školenie a testovanie pred udelením prístupu k ITVS. Toto opatrenie nahrádza opatrenie Z1-B písm. g) a h) a Z2-B.

**Z3-D Kontrolný mechanizmus informačnej bezpečnosti**

Základným bezpečnostným opatrením pre kontrolný mechanizmus informačnej bezpečnosti je

a) vykonávanie penetračného testovania a ohodnotenia zraniteľností v pravidelných intervaloch, pri zavádzaní nových ITVS alebo pri významných zmenách v ITVS,

b) vykonávanie pravidelných testov odolnosti zamestnancov orgánu riadenia voči útokom sociálnym inžinierstvom, predovšetkým voči útokom typu phishing, spearphishing, vishing a baiting.

**Z3-E Ochrana proti škodlivému kódu**

Základným bezpečnostným opatrením pre ochranu proti škodlivému kódu je

a) implementácia centrálneho antivírusového riešenia a monitorovanie jeho hlásení,

b) zavedenie hardeningu pracovných staníc a pravidelné preverovanie jeho účinnosti a aktuálnosti raz ročne.

**Z3-F Sieťová bezpečnosť**

Základným bezpečnostným opatrením pre sieťovú bezpečnosť je

a) implementácia HIPS (Host Intrusion Prevention System) na všetkých pracovných staniciach a serveroch,

b) implementácia druhého sieťového firewallu od iného výrobcu tak, aby interné servery a klientske stanice boli vo vzťahu k externým sieťam chránené dvomi sieťovými firewallmi,

c) implementácia Intrusion Prevention Systému (IPS) na perimetri siete a jeho umiestnenie medzi firewall a chránenú časť siete,

d) implementácia Web Application Firewallu (WAF) na všetkých verejne dostupných a kritických webových aplikáciách,

e) implementácia manažmentu logov,

f) v prípade používania bezdrôtových sietí (WIFI) ich umiestnenie do segmentu bez prístupu k aktívam klasifikovaným ako C3 alebo I3,

g) synchronizácia času všetkých ITVS v sieti s interným NTP serverom,

h) zaistenie vysokej dostupnosti ITVS kategórie A3 pomocou redundancie a load balancingu,

i) implementácia DNSSEC a jeho využitie pre všetky externe dostupné služby orgánu riadenia,

j) konfigurácia a izolovanie klientskych portov na prístupových switchoch tak, aby pracovné stanice spolu nemohli priamo komunikovať(technológia PVLAN). Táto požiadavka nahrádza požiadavku zo Z2-Fl) o maximálnom počte MAC adries,

k) zabezpečenie prístupu používateľov k Internetu a k službám mimo siete orgánu riadenia cez proxy server a uchovávanie prístupových logov aspoň 6 mesiacov,

l) používanie výhradne interného DNS servera a uchovávanie logov DNS dopytov aspoň 4 mesiace,

m) uchovávanie logov o IP adresách pridelených prostredníctvom DHCP aspoň 6 mesiacov,

n) rozdelenie siete do jednotlivých segmentov podľa účelu, pričom v rovnakých segmentoch môžu byť len zariadenia s rovnakými požiadavkami na úroveň zabezpečenia,

o) zabezpečenie logovania sieťových spojení s externými sieťami na sieťových prvkoch a to minimálne na úrovni šestice časová pečiatka, zdrojová IP adresa, cieľová IP adresa, protokol, zdrojový port, cieľový port a uchovávanie týchto logov aspoň 6 mesiacov.

**Z3-G Fyzická bezpečnosť a bezpečnosť prostredia**

Základným bezpečnostným opatrením pre fyzickú bezpečnosť a bezpečnosť prostredia je

a) zabezpečenie budovy strážnou službou s kontrolou vstupov, ktorá je schopná byť na mieste incidentu do 3 minút od spustenia poplachu,

b) umiestnenie serverových a sieťových komponentov do miestností opatrených certifikovanými bezpečnostnými dverami, tehlovými alebo betónovými dverami bez okien, alebo do miestností s nerozbitnými nepriehľadnými sklami s detektormi rozbitia,

c) zaistenie miestností alebo serverových skríň, v ktorých sú umiestnené serverové a sieťové komponenty senzormi teploty, vlhkosti, dymu, úniku vody, prachu, detektormi pohybu a vibrácií,

d) vyvedenie všetkých elektronických zabezpečovacích prostriedkov podľa písm. c) do agregačných bodov s možnosťou zasielania varovaní a notifikácií do centrálneho monitorovacieho systému s možnosťou varovania, automatizovanej akcie na základe vopred nastavaných prahových hodnôt a možnosťou analýzy a reportovania,

e) umožnenie prístupu tretích strán do priestorov orgánu riadenia len v sprievode interného zamestnanca,

f) zabezpečenie vstupu na pracovisko prostredníctvom prístupových tokenov, ukladanie a zálohovanie záznamov o vstupoch aspoň 6 mesiacov,

g) implementácia pravidelnej technickej revízie jednotlivých komponentov,

h) pre podpornú infraštruktúru ITVS kategórie A3 zabezpečenie ochrany pred výpadkom zdroja elektrickej energie pomocou diesel generátorov a zabezpečenie, aby takýto výpadok nenastal,

i) zabezpečenie, aby boli existujúce záložné kapacity ITVS, zabezpečujúce funkčnosť alebo náhradu ITVS, umiestnené v sekundárnom zabezpečenom priestore, dostatočne vzdialenom od zabezpečeného priestoru.

**Z3-I Monitorovanie a manažment bezpečnostných incidentov**

Základným bezpečnostným opatrením pre monitorovania a manažment bezpečnostných incidentov je

a) používanie systému na detekciu prienikov, ktorý monitoruje bezpečnosť najmenej v rozsahu Intrusion Detection System (IDS),

b) implementácia Security information and event manažmentu (SIEM),

c) implementácia prevádzkového dohľadu 24 hodín denne 7 dní v týždni,

d) implementácia automatickej notifikácie o hláseniach podozrivých bezpečnostných udalostí a zabezpečenie ich preverenia a riešenia bez zbytočného odkladu.

**Z3-M Riadenie prístupu**

Základným bezpečnostným opatrením pre riadenie prístupu je

a) implementácia, vynucovanie a pravidelné auditovanie prístupového modelu RBAC, DAC alebo MAC,

b) zamedzenie možnosti zmeny log záznamov prístupu každého používateľa vrátane administrátora do ITVS, zamedzenie možnosti vymazania týchto záznamov bez schválenia zodpovednou osobou určenou v súlade s Z1-A Riadenie informačnej bezpečnosti a uchovávanie týchto záznamov po dobu aspoň 6 mesiacov.

**Z3-N Aktualizácia informačno-komunikačných technológií**

Základným bezpečnostným opatrením pre aktualizáciu informačno-komunikačných technológií je

a) vytvorenie a implementácia interných predpisov upravujúcich manažment kapacít ITVS,

b) zaistenie náhradných komponentov ITVS a SLA s dodávateľmi na opravu poškodených častí ITVS do 24 hodín.

**Z3-Q Kryptografia**

Základným bezpečnostným opatrením pre kryptografiu je

a) implementácia šifrovania emailovej komunikácie prostredníctvom PGP alebo S/MIME,

b) implementácia šifrovania diskov na pracovných staniciach a serveroch metódou full disk encryption,

c) implementácia šifrovania centrálnych úložísk,

d) implementácia šifrovania všetkých záloh,

e) implementácia manažmentu kryptografických kľúčov,

f) udržiavanie kópie šifrovacieho kľúča v trezore pre požitie autorizovanou osobou v prípade núdze

g) vytvorenie a implementácia interných predpisov upravujúcich činnosti podľa písm. a) – f).

**Príloha č. 3**

**k vyhláške č. xx/2019 Z. z.**

**ŠPECIFICKÉ BEZPEČNOSTNÉ OPATRENIA**

(1) V tejto prílohe sú použité nasledujúce operátory podľa uvedeného významu:

1. „musí“ – špecifikuje povinnú požiadavku (platí aj pre „je nutné“),
2. „nesmie“ – špecifikuje povinný zákaz,
3. „malo by [byť]” – špecifikuje požiadavku, ktorá je povinná pokiaľ neexistuje pádny dôvod prečo nemôže byť splnená. V prípade výnimky zo splnenia požiadavky s týmto operátorom orgán riadenia postupuje podľa ustanovení v §7,
4. “nemalo by [byť]” - špecifikuje zákaz, ktorý je povinný pokiaľ neexistuje pádny dôvod prečo nie je možné ho splniť. V prípade výnimky zo splnenia požiadavky s týmto operátorom orgán riadenia postupuje podľa ustanovení v §7,
5. “odporúča sa” – špecifikuje odporúčanú požiadavku (platí aj pre “je vhodné”).

(2) Ak je rozdiel medzi operátorom (musí / malo by byť / odporúča sa) v konkrétnom opatrení a jeho nadradeným číslovaným bodom, tak platí operátor v konkrétnej odrážke (to znamená posledný špecifikovaný). V nasledujúcom príklade pre bod b) platí operátor „malo by byť“:

*1.1 Orgán riadenia musí vykonávať pravidelné monitorovanie a preskúmavanie bezpečnosti ITVS v rozsahu:*

*a) Pravidelné preskúmavanie plnenia cieľov bezpečnostnej politiky aspoň raz za 12 mesiacov vedením orgánu riadenia.*

*b) Malo by byť vykonávané pravidelné testovanie záloh ITVS na kontrolu funkčnosti.*

**1 Organizačné opatrenia**

**Všeobecné požiadavky**

* 1. Orgán riadenia musí zaviesť aspoň nasledovné opatrenia personálnej bezpečnosti:

1. Sú určené roly a zodpovednosti za informačnú bezpečnosť aspoň pre tieto roly: vrcholný predstaviteľ organizácie, manažér pre bezpečnosť, vedúci pracovník, administrátor, audítor, používateľ.
2. Roly manažéra pre bezpečnosť, výkonnej zložky informačnej bezpečnosti a audítora musia byť oddelené od oddelenia správy IKT.
   1. Orgán riadenia musí zaviesť riadenie informačných aktív s nasledovnými požiadavkami:
3. Orgán riadenia musí vypracovať inventár informačných aktív, ktorý je úplný, aktuálny, preskúmavaný a aktualizovaný pri zmenách v IS, minimálne však každých 12 mesiacov.
4. Na vedenie, údržbu a aktualizáciu inventáru aktív by mala byť stanovená zodpovedná osoba.
5. Inventár aktív v rozsahu podľa Prílohy č. 9 musí byť orgánu vedenia odoslaný raz ročne a pri významných zmenách.
6. Pre každý klasifikačný stupeň musí byť definovaný súbor opatrení, ktoré popisujú požiadavky na ich ochranu pri ukladaní, prenose a spracúvaní.
7. Inštalácia softvéru a hardvéru musí byť vykonávaná len povereným administrátorom.
8. Orgán riadenia musí vypracovať zoznam autorizovaného softvéru a je dovolené inštalovať výhradne legálny softvér z tohto zoznamu získaný z dôveryhodných zdrojov.
9. Orgán riadenia by mal vypracovať zoznam autorizovaného hardvéru na základe sériového čísla a zaviesť pravidlá dovoľujúce používať výhradne hardvér z tohto zoznamu, pričom výnimky by mali byť schválené manažérom bezpečnosti.
10. Nepotrebné informácie a ich dátové nosiče musia byť mazané a ničené bezpečným spôsobom, napr. ich skartovaním alebo viacnásobným prepísaním.
    1. Orgán riadenia musí implementovať systém manažmentu rizík, ktorý spĺňa aspoň nasledovné požiadavky:
11. Identifikácia a ohodnotenie rizík je založené na identifikácii a klasifikácii aktív, ich zraniteľností a hrozieb, ktoré majú potenciál tieto zraniteľnosti zneužiť, a potenciálnych dopadov pri zneužití zraniteľností.
12. Identifikácia a ohodnotenie rizík je vykonávané konzistentným, systematickým, vopred stanoveným a dokumentovaným spôsobom, ktorý zaručí pokrytie všetkých známych rizík a opakovateľnosť výsledkov.
13. Je stanovená a vedením schválená miera akceptovateľných rizík a všetky riziká s vyššou hodnotou ako je miera akceptovateľných rizík sú ošetrené tak, aby zvyškové riziko nepresiahlo mieru akceptovateľných rizík.
14. Je stanovené, čo orgán riadenia pre adekvátne ošetrenie rizika vyžaduje: môže ísť o jeho okamžité odstránenie, resp. je stanovená lehota, počas ktorej môže byť riziko prítomne, nakoľko ešte nie je dostupné riešenie (napríklad vydanie záplaty dodávateľom IS, v ktorom sa objavila nová kritická zraniteľnosť).
15. Je vedený zoznam zostatkových rizík a tieto riziká sú v pravidelných intervaloch a pri zmenách v ITVS a prostredí orgánu riadenia preskúmavané.
16. Riziká sú ošetrované podľa Plánu pre ošetrovanie rizík so stanovenými konkrétnymi opatreniami, zodpovednosťami za implementáciu týchto opatrení, termínmi a potrebnými zdrojmi na ošetrenie rizík.
    1. Orgán riadenia musia stanoviť a dodržiavať aspoň nasledovné pravidlá pre používateľov ITVS:
17. Pri odchode od pracovnej stanice je zamestnanec povinný ju uzamknúť.
18. Pri zadávaní hesla musí zamestnanec dbať na to, aby nebolo náhodne odpozorované.
19. Heslá musia byť rôzne pre rôzne ITVS s výnimkou SSO (Single Sign-On).
20. Heslá by nemali byť zdieľané.
21. Heslá nesmú byť voľne dostupné prostredníctvom fyzických alebo dátových prostriedkov.
    1. Orgán riadenia by mal stanoviť a dodržiavať aspoň nasledovné pravidlá pre používateľov ITVS:
22. Je zakázané používať súkromné IT prostriedky na služobné účely.
23. Je zakázané používať služobné IT prostriedky na súkromné účely.
24. Pri práci s e-mailom je zakázané otvárať nevyžiadanú poštu, ako aj prílohy e-mailov a odkazy obsiahnuté v tele e-mailov z nedôveryhodných zdrojov.
25. Je zakázané pristupovať k webovým portálom, ktoré môžu ohroziť bezpečnosť pracovnej stanice (známe škodlivé webové stránky, pornografické stránky, stránky poskytujúce akúkoľvek formu sťahovania pirátskeho obsahu, stránky poskytujúce akúkoľvek formu hazardu, stránky o hackingu a podobne)
26. Je zakázané pristupovať k sociálnym sieťam a chatovacím programom s výnimkou sociálnych sietí a chatovacích programov používaných pre pracovné účely.
27. Pre prácu s Internetom je povolené používať len zabezpečený prehliadač s nainštalovanými a vhodne nakonfigurovanými bezpečnostnými doplnkami blokujúcimi JavaScript, reklamy a Adobe Flash. V odôvodnených prípadoch pokiaľ bezpečnostné doplnky bránia vo výkone pracovných povinnosti, je možné pre dôveryhodné webové stránky udeliť dočasnú výnimku pre konkrétnu doménu. Zamestnanci orgánu riadenia by mali byť vyškolení v používaní týchto doplnkov.
    1. Orgán riadenia musí stanoviť a dodržiavať aspoň nasledovné pravidlá pre administrátorov ITVS:
28. V prípade odchodu a po ukončení práce so stanicou (resp. konzolou alebo terminálom) je potrebné sa odhlásiť.
29. Heslá k privilegovaným a administrátorským účtom musia spĺňať požiadavky uvedené v Prílohe 5.
30. Je zakázané zaznamenávať a zasielať heslá v otvorenom a reverzibilnom tvare.
31. Zdieľanie hesiel by malo byť zakázané[[5]](#footnote-5).
32. Akékoľvek zmeny v systémovej konfigurácii sú dokumentované.
33. Používateľom je možné poskytnúť len prístup v minimálnom rozsahu nevyhnutnom na vykonávanie ich pracovných činností.
34. Pri ukončení pracovného pomeru s administrátorom musí byť zablokované jeho konto na autentifikačnom serveri ako aj na zariadeniach, ktoré boli pod jeho správou a odporúča sa vykonať zmeny jemu známych autentifikačných údajov (príklad: SNMP community strings, failover kľúče, kľúče smerovacích protokolov, VPN kľúče).
35. Pri ukončení pracovného pomeru s administrátorom je nutné zablokovať jeho účet na prístup cez VPN a zmeniť akékoľvek zdieľané správcovské prístupové údaje.
36. Pri ukončení pracovného pomeru s administrátorom by mala byť skontrolovaná integrita konfigurácií všetkých prvkov (napr. konfigurácia SNMP, Syslog), konfigurácia správcovských prístupových údajov a konfigurácia správcovských prístupových metód.
    1. Orgán riadenia musí zabezpečiť dohľad nad všetkými stavebnými otvormi, ktorými sú predovšetkým dvere a okná a pri ktorých je možné predpokladať, že by mohli byť použité na získanie neoprávneného prístupu do chránených priestorov, prostredníctvom CCTV.
    2. Orgán riadenia musí zaviesť riadenie fyzického a logického prístupu s nasledovnými pravidlami:
37. Prideľovanie oprávnení sa vykonáva v nasledovných krokoch: návrh, schválenie, dokumentácia a nastavenie prístupových oprávnení.
38. Prístupy sú prideľované len v rozsahu nevyhnutnom na vykonávanie pracovných činností.
39. Je vypracovaný a aktualizovaný zoznam privilegovaných prístupových oprávnení a pravidelný ročný audit ich potreby.
40. Všetky heslá k privilegovaným prístupovým účtom musia spĺňať kritériá pre administrátorské účty uvedené v Prílohe 5.
    1. Orgán riadenia musí zaviesť a dodržiavať postupy pre zálohovanie v nasledujúcom rozsahu:
41. Frekvencia a rozsah zálohovania musí byť schválená vedením orgánu riadenia a musí byť dokumentovaná.
42. Zamestnanci zodpovední za zálohovanie sú určení a sú poučení o svojich povinnostiach.
43. Musí byť stanovený interval, čas, rozsah dát, dátové médium a vedenie dokumentácie o zálohovaní.
44. Zálohy musia byť umiestnené v zabezpečenom priestore s riadením vstupu.
45. Zálohy informácií a ITVS musia byť uložené aj na fyzicky dostatočne vzdialenej lokalite a musia byť šifrované.
46. Musí byť pravidelne vykonávaný test obnovy záloh.
    1. Orgán riadenia musí byť zaviesť systém riadenia kontinuity činností s nasledovnými požiadavkami:
47. Musia byť stanovené roly a zodpovednosti pre plnenie havarijných plánov a plánov obnovy.
48. Musí byť stanovená cieľová doba obnovy (RTO) a cieľový bod obnovy (RPO) pre jednotlivé procesy, ITVS a aplikácie.
49. Jednotlivé postupy pri riadení kontinuity činností by mali byť pravidelne testované prostredníctvom ohlásených alebo neohlásených cvičení.
    1. Orgán riadenia musí zaviesť a dodržiavať postupy pre nahlasovanie a riešenie počítačových bezpečnostných incidentov aspoň v nasledovnom rozsahu:
50. Je stanovené kontaktné miesto pre nahlasovanie incidentov a roly a zodpovednosti pre zamestnancov poverených ich riešením.
51. Kontaktné údaje pre nahlasovanie počítačových incidentov sú nahlásené Vládnej jednotke CSIRT a pri zmenách kontaktných údajov sú nové kontaktné údaje opätovne nahlásené.
52. Je vedená a udržiavaná evidencia kontaktných údajov tretích strán potrebných na riešenie počítačových incidentov a je určená osoba zodpovedná za jej vedenie a udržiavanie.
53. Zamestnanci poverení riešením incidentov sú odborne spôsobilí, pravidelne školení a zastupiteľní.
54. Incidenty sú klasifikované podľa klasifikačnej schémy definovanej v smernici pre riešenie počítačových incidentov.
55. Na detekciu a riešenie incidentov sú vyhradené dostatočné zdroje.
56. Incidenty sú riešené bez zbytočného odkladu podľa vopred stanovených postupov.
57. Sú vytvorené eskalačné postupy.
58. Je vedená evidencia bezpečnostných incidentov a je určená osoba zodpovedná za jej vedenie.
59. Po vyriešení incidentu je vykonaná následná analýza a sú implementované opatrenia na predchádzanie incidentom podobného typu.
60. Po vyriešení incidentu je vykonané preskúmanie postupu jeho riešenia, sú identifikované nedostatky a návrhy na zlepšenie (napr. vhodnosť alebo potreba nových nástrojov, dostatok personálu, potreba školení a podobne), tieto sú prediskutované na stretnutí relevantných zamestnancov orgánu riadenia a závery z tohto stretnutia sú dokumentované.
61. Sú vytvorené plány pre riešenie počítačových incidentov aspoň tohto typu: prienik, nákaza škodlivým kódom, DoS útok, sociálne inžinierstvo (phishing, baiting, impersonácia a pod.) Odporúča sa implementovať postupy pre riešenie incidentov – napríklad postupy zverejnené národnou, vládnou alebo rezortnou jednotkou CSIRT / CERT.
    1. Orgán riadenia musí vykonávať audity bezpečnosti ITVS aspoň raz za 36 mesiacov podľa nasledovných požiadaviek:
62. Je vypracovaný program auditov na obdobie troch rokov, ktorý zahŕňa interné audity, posúdenie zraniteľností a penetračné testy.
63. Pre každý interný audit je vypracovaný plán auditu, ktorý obsahuje ciele auditu, referenčné dokumenty, dátumy a miesta vykonania auditu, organizačné útvary, ktoré sú predmetom auditu, roly a zodpovednosti.
64. Audítor musí byť nezávislý[[6]](#footnote-6), skúsený, musí byť znalý príslušnej legislatívy a štandardov a musí mať vhodné osobnostné predpoklady.
65. Správa z auditu musí obsahovať aspoň zoznam účastníkov auditu, zoznam zistených nezhôd, pozorovaní a príležitostí na zlepšenie, vyjadrenie audítora k rozsahu v akom Orgán riadenia plní bezpečnostné požiadavky a návrh opatrení vyplývajúcich zo zistení auditu.
66. Pre implementáciu opatrení na odstránenie zistených nedostatkov je potrebné vypracovať plán implementácie opatrení podľa ich priority s určením zodpovedností, termínov plnenia a zdrojov.
    1. Prístup tretích strán ako aj ich vzdialený prístup musí byť riadený, kontrolovaný a prístupové oprávnenia musia byť udelené len v minimálnom rozsahu potrebnom na vykonávanie pracovných činností.
    2. Tretie strany musia orgánu riadenia na požiadanie poskytnúť správu o stave zabezpečenia a funkčnosti zverených aktív v rozsahu stanovenom orgánom riadenia na základe povahy predmetných aktív.
    3. Pre ITVS by malo byť implementované monitorovanie dostupnosti služieb a detekcia anomálií.
    4. Pred nasadením IPv6 do prevádzky musí byť vytvorený plán nasadenia, ktorý obsahuje aj analýzu rizík spojených s IPv6 a požiadavky na bezpečnostné mechanizmy a konfiguráciu infraštruktúry.
    5. Ak sa používa IPv6, musí byť zabezpečené, že sieťoví administrátori, operátori monitoringu aj bezpečnostný tím majú dostatočné technické znalosti špecifík IPv6 protokolu aj podporných protokolov ako ICMPv6, DHCPv6, DNS.
    6. Pred nasadením VOIP alebo telepresence musí byť vytvorený plán nasadenia, ktorý obsahuje aj analýzu rizík spojených s VOIP a telepresence a požiadavky na bezpečnostné mechanizmy a konfiguráciu infraštruktúry.

**Mechanizmus kontroly**

* 1. Orgán riadenia musí vykonávať pravidelné monitorovanie a preskúmavanie bezpečnosti ITVS v rozsahu:

1. Pravidelné preskúmavanie plnenia cieľov bezpečnostnej politiky aspoň raz za 12 mesiacov vedením orgánu riadenia.
2. Kontinuálne monitorovanie účinnosti bezpečnostných opatrení na ošetrenie rizík.
3. Pravidelné preskúmavanie zostatkových rizík aspoň raz za 12 mesiacov a v prípade zmien v ITVS.
4. Pravidelné monitorovanie log záznamov a ich analýza aspoň raz za týždeň.
5. Pravidelná kontrola technického stavu zariadení a funkčnosti aplikácií aspoň raz za mesiac.
6. Pre ITVS v kategórii I3 a A3 musí byť vykonávané monitorovanie funkčnosti aplikácií v reálnom čase.
7. Malo by byť vykonávané pravidelné testovanie záloh ITVS na kontrolu funkčnosti.
8. Je vykonávaná pravidelná kontrola prístupových oprávnení a deaktivovanie nepotrebných prístupových účtov aspoň každých 12 mesiacov.
9. Pravidelné meranie účinnosti programu vzdelávania zamestnancov a testovanie úrovne ich bezpečnostného povedomia.
10. Pravidelné preskúmavanie jednotlivých stratégií a plánov pre kontinuitu činností aspoň raz za 12 mesiacov.
    1. Každých 24 mesiacov by malo byť vykonávané interné a externé penetračné testovanie ITVS a následné odstránenie zistených zraniteľností. V prípade, že posledný penetračný test znamenal kompromitáciu ITVS alebo kompromitáciu značnej časti infraštruktúry, mal by byť vykonať ďalší penetračný test hneď po odstránení zraniteľností – najneskôr však o 12 mesiacov.

**Technické opatrenia**

1. **Minimálne požiadavky na zabezpečenie implementovaného riešenia**

**Bezpečnosť životného cyklu ITVS**

Pri vývoji riešenia je potrebné zaoberať sa bezpečnosťou už od počiatočnej fázy životného cyklu ITVS a prispôsobiť tomu návrh aj implementáciu samotného riešenia počas jednotlivých fáz.

**Návrh riešenia**

* 1. Navrhnuté riešenie musí mať modulárnu štruktúru, pričom

1. Pri návrhu jednotlivých komponentov riešenia musí byť splnený princíp least privilege a všetky entity (t.j. používatelia aj systémy) musia mať prístup iba k údajom / aktívam, ktoré pre svoju činnosť nevyhnutne potrebujú.
2. Odporúča sa, aby architektúra riešenia bola trojvrstvová – mala by pozostávať z prezentačných serverov, aplikačných serverov a databázových serverov,
3. Odporúčané je použitie overených návrhových vzorov, napr. MVC, resp. MVP
   1. Musia byť identifikované všetky súčasti (interné aj externé[[7]](#footnote-7)), od ktorých závisí riešenie. Pre jednotlivé súčasti musia byť identifikované zraniteľnosti, ktoré sa v nich môžu vyskytnúť a vyhodnotiť riziká zneužitia týchto zraniteľností na základe
4. prístupového vektoru útočníka (lokálny prístup/sieť),
5. náročnosti získania prístupu,
6. potreby autentifikácie,
7. dopadov úspešného útoku na dostupnosť, integritu a dôvernosť riešenia a údajov v ňom spracovávaných.
   1. Na základe analýzy rizík musia byť navrhnuté opatrenia, ako predchádzať možným incidentom a ako postupovať v prípade vzniku incidentu. Tieto opatrenia musia byť zapracované v návrhu riešenia.

**Implementácia riešenia**

* 1. Riešenie musí byť vyvíjané vo vývojovom prostredí, ktoré spĺňa bezpečnostné požiadavky zodpovedajúce klasifikačnému stupňu riešenia a ktoré musí byť oddelené od predprodukčného, produkčného a testovacieho prostredia, pričom sa odporúča, aby nedisponovalo možnosťou testovania.
  2. Pri implementácii by mali byť použité dôveryhodné (a zároveň široko rozšírené) frameworky / knižnice, ktoré kladú dôraz na bezpečnosť a predchádzanie bežným programátorským chybám a zároveň často a rýchlo zverejňujú opravy bezpečnostných chýb.
  3. V prípade, že implementované riešenie potrebuje spracovávať dôverné údaje (napr. osobné údaje), počas vývoja aj testovania musia byť použité anonymizované, resp. fiktívne údaje.
  4. Pri písaní zdrojového kódu by mal byť použitý systém na verzionovanie[[8]](#footnote-8), pričom

1. jednotlivé zmeny (commity) by mali byť digitálne podpísané privátnym kľúčom autora daného commitu,
2. commity by mali mať zmysluplné popisy,
3. mala by byť implementovaná automatická kontrola zdrojového kódu na prítomnosť chýb a testovanie po každom commite.
   1. Nemali by byť použité funkcie/volania/nástroje, ktoré sú podľa ich dokumentácie v dobe implementácie zastarané (angl. deprecated) alebo nebezpečné (angl. unsafe) a mali by byť nahradené odporúčanými alternatívami.
   2. Počas vývoja riešenia musia byť povolené všetky bezpečnostné vlastnosti použitých nástrojov, najmä však
4. zapnuté všetky varovania a ochrany vývojových nástrojov[[9]](#footnote-9),
5. varovania vývojového prostredia
   1. Všetky varovania z predchádzajúceho bodu by mali byť opravené.
   2. Počas vývoja musí byť vedená vývojárska dokumentácia:
6. dokumentácia musí obsahovať bližší popis kľúčových častí riešenia až na prípadné výnimky chránené obchodným tajomstvom; tieto výnimky však musia byť zaznamenané v dokumentácii
7. v dokumentácii musí byť zaznamenaná každá zmena oproti pôvodnej špecifikácií a jej dôvody a každá takáto zmena musí byť schválená objednávateľom.
   1. Dokumentácia aj zdrojové kódy riešenia musia byť odovzdané objednávateľovi spolu so samotným riešením.
   2. Pokiaľ je súčasťou riešenia aj databáza obsahujúca dôverné údaje:
8. autentifikačné údaje musia byť uložené iba v podobe osolených hashov (salted hash), pričom použitá hashovacia funkcia by mala byť minimálne sha256,
9. ostatné osobné údaje (adresy, čísla platobných kariet, čísla občianskych preukazov,...) je odporúčané neukladať v čistej podobe, ale chránené šifrovaním[[10]](#footnote-10).
   1. Musí byť implementované logovanie a logy by mali zaznamenávať minimálne úspešné a neúspešné:
10. prihlásenie a odhlásenie,
11. vytvorenie, modifikáciu alebo zmazanie používateľa alebo skupiny,
12. pokusy pristúpiť k citlivým údajom,
13. pokusy o kritické operácie.
    1. Logy musia byť centrálne ukladané a archivované minimálne 6 mesiacov.
    2. Riešenie musí podporovať aj logovanie vo formáte syslog a musí podporovať preposielanie týchto logov na externý syslog server. V odôvodnených prípadoch môžu byť výnimkou logy veľkého množstva prístupov k údajom zaznamenávané v databáze.

**Testovanie a verifikácia riešenia**

* 1. Riešenie musí byť testované v testovacom prostredí, ktoré spĺňa bezpečnostné požiadavky zodpovedajúce klasifikačnému stupňu riešenia, je nakonfigurované v súlade s produkčným prostredím a ktoré musí byť oddelené od predprodukčného, produkčného a vývojového prostredia.
  2. Riešenie musí byť testované používateľmi za účelom akceptácie riešenia v predprodukčnom prostredí, ktoré spĺňa bezpečnostné požiadavky zodpovedajúce klasifikačnému stupňu riešenia, je nakonfigurované v súlade s produkčným prostredím a ktoré musí byť oddelené od testovacieho, produkčného a vývojového prostredia.
  3. Po ukončení vývoja musí prejsť aplikácia testovaním a verifikáciou:

1. Vývojári by mali overiť aspoň pomocou automatizovaných nástrojov štandardné zraniteľnosti. Odporúča sa vykonať testovanie vstupov (fuzzing) a kontrolu práce s pamäťou (memory leaky, memory corruption).
2. Vývojári musia zabezpečiť realizáciu opatrení vyplývajúcich z analýzy rizík vypracovanej pri návrhu riešenia.
3. Musí byť vykonané penetračné testovanie externou organizáciou.
4. Zraniteľnosti a problémy zistené na základe testovania musia byť odstránené a ich oprava musí byť potvrdená opakovaným testovaním.

**Nasadenie a prevádzka riešenia**

* 1. Hotové riešenie s odstránenými nájdenými zraniteľnosťami musí byť nasadené v prostredí zabezpečenom na základe odporúčaní v kapitolách o zabezpečení služieb a infraštruktúry.
  2. Musí byť zabezpečené pravidelné monitorovanie nových zraniteľností jednotlivých (najmä externých) súčastí riešenia a pravidelné aplikovanie bezpečnostných záplat vydaných vývojármi, resp. tretími stranami. Aplikovanie týchto záplat musí podliehať opatreniam uvedeným v smernici pre riadenie záplat.

**Interná infraštruktúra a vývojové prostredie**

**Interná infraštruktúra riešenia**

* 1. Jednotlivé vrstvy (databázová, aplikačná, prezentačná) by mali byť umiestnené v separátnych segmentoch a komunikácia medzi nimi musí byť filtrovaná
  2. Jednotlivé servery musia byť hardenované minimálne v nasledovnom rozsahu:

1. sú vypnuté všetky nepotrebné procesy a služby,
2. je implementovaný host-based firewall, ktorý kontroluje všetku prichádzajúcu a odchádzajúcu komunikáciu na princípe „least privilege“,
3. všetky administrátorské účty spĺňajú požiadavky politiky hesiel pre administrátorské účty uvedenú v Prílohe 5,
4. servery a všetok softvér je aktualizovaný minimálne raz za 6 mesiacov, odporúča sa aktualizovať aspoň raz za mesiac,
5. na serveroch by malo byť implementované anti-malware riešenie, ktoré je centrálne spravované a centrálne logované,
6. všetky servery majú nastavený lokálny NTP server ako autoritatívny zdroj času a pre preklad doménových mien na IP adresy používajú lokálne DNS servery a
7. všetky zariadenia sú hardenované podľa odporúčaní výrobcu.

**Vývojové prostredie**

* 1. Vo vývojovom prostredí musia byť použité iba nástroje, ktoré:

1. sú získané legálnym spôsobom z dôveryhodných zdrojov,
2. sú stále podporované výrobcom (t.j. výrobca poskytuje bezpečnostné aktualizácie) nástroja a nesmú byť označené ako zastarané,
3. sú aktualizované minimálne raz za 6 mesiacov a bezpečnostné záplaty vydané výrobcom nástroja sú aplikované.
   1. Vo vývojovom prostredí (vývojárske nástroje a podporné informačné systémy vrátane použitých knižníc tretích strán), v ktorom bude vyvíjané riešenie, musia byť implementované tieto opatrenia:
4. sú implementované príslušné opatrenia na zabezpečenie integrity vyvíjaného riešenia na základe najvyššej požadovanej úrovne ochrany dôvernosti, integrity a dostupnosti informácií, ktoré budú spracovávané vo vyvíjanom riešení.
5. ak samotné vyvíjané riešenie obsahuje informácie, ktoré je potrebné chrániť z hľadiska dôvernosti[[11]](#footnote-11), musia byť vo vývojovom prostredí implementované opatrenia na zaistenie dôvernosti na základe požadovanej úrovne ochrany dôvernosti týchto údajov.

**Mechanizmus kontroly**

* 1. Kontrola vykonaných opatrení sa vykonáva dvoma spôsobmi:

1. pri odovzdávaní projektu na mieste dohodnutom medzi objednávateľom a dodávateľom,
2. počas implementácie projektu na mieste, kde prebieha vývoj riešenia.
   1. Kontrola pri odovzdávaní projektu pozostáva z:
3. kontroly projektovej dokumentácie obsahujúcej minimálne návrh riešenia s popisom jednotlivých súčastí, vývojársku dokumentáciu a dokumentáciu pre používateľov a správcov,
4. kontroly analýzy rizík a implementácie navrhnutých opatrení,
5. kontroly verzionovanej histórie vývoja projektu pozostávajúcej minimálne z kontroly podpísaných commitov a z kontroly, či zmeny vykonané v danom commite súvisia s jeho popisom,
6. kontroly zdrojových kódov na použité zastarané/nebezpečné funkcie a kontroly použitých knižníc,
7. kontroly formátu citlivých údajov v databáze,
8. kontroly výsledkov testovania implementovaného riešenia.
   1. Kontrola počas implementácie projektu na mieste, kde prebieha vývoj riešenia, pozostáva z:
9. kontroly použitých vývojárskych nástrojov, ich pôvodu, legálnosti a aktuálnosti,
10. kontroly implementovaných opatrení na zabezpečenie integrity vyvíjaného riešenia, prípadne aj jeho dôvernosti,
11. kontroly anonymizácie použitých testovacích údajov počas implementácie riešenia,
12. kontroly zapnutých bezpečnostných vlastností použitých nástrojov (varovania, ochrany),
    1. Kontrolu by mala vykonávať osoba, ktorá je dostatočne technicky zdatná a má minimálne 5 rokov prax v IT odbore, je bezúhonná a nezávislá.
    2. Odporúča sa aspoň raz ročne auditovať komplexitu hesiel účtov z Active Directory a pre identifikované účty so slabými heslami vynútiť ich zmenu.

**3 Minimálne požiadavky na zabezpečenie služieb dostupných z externých sietí –**

**Webové aplikácie**

**Bezpečný návrh**

* 1. Webová stránka by mala pozostávať z verejných a neverejných zón a navigácia medzi nimi by nemala umožniť tok citlivých informácií medzi týmito zónami.
  2. Citlivé informácie by mali byť uchovávané v zašifrovanej podobe s použitím kryptograficky silných algoritmov.
  3. Validácia vstupov musí byť vykonávaná na strane servera a odporúča sa, aby bola vykonávaná aj na strane klienta.
  4. Prezentačný server musí byť umiestnený v zabezpečenej demilitarizovanej zóne (DMZ), ku ktorej môžu pristupovať len autorizované osoby. Aplikačný a databázový server by mali byť umiestnené v internej sieti neprístupnej z Internetu.
  5. Kód musí byť udržiavaný, prehľadný a dokumentovaný. Viď sekciu 5.11.
  6. Prezentačná vrstva musí byť oddelená od aplikačnej a databázovej vrstvy.

**Šifrovanie**

* 1. Webový portál musí byť prístupný prostredníctvom protokolu HTTPS s použitím HSTS.
  2. K webovému portálu by sa nemalo pristupovať prostredníctvom HTTP.
  3. Identita webového portálu musí byť zabezpečená platným, dôveryhodným certifikátom vydaným na doménu, na ktorej je dostupný webový portál.
  4. Identita webového portálu by mala byť zabezpečená certifikátom s Extended Validation.
  5. Webový portál nesmie používať nedôveryhodné alebo vypršané SSL/TLS certifikáty.
  6. Údaje, ktoré sú citlivé z hľadiska integrity alebo dôvernosti sa musia prenášať iba prostredníctvom zašifrovaného spojenia SSL/TLS.
  7. Webový portál by nemal ukladať citlivé informácie v nezašifrovanej podobe na strane klienta, ani na strane servera.
  8. Webový portál by nemal vkladať nešifrované zdroje bez SSL/TLS do stránok používajúcich SSL/TLS.

**Šifrovacie kľúče a protokoly**

* 1. Webový server nesmie podporovať protokoly SSLv2, SSLv3, TLS 1.0.
  2. Webový server môže podporovať TLS 1.1, TLS 1.2.
  3. Odporúča sa, aby webový server podporoval  TLS 1.3.
  4. Webový server by nemal podporovať šifry s kľúčom kratším ako 112 bitov a blokom kratším ako 64bitov.
  5. Webový server nesmie podporovať NULL ciphers a anonymný Diffie-Hellman algoritmus.
  6. Webový server nesmie podporovať tzv. Export (EXP) šifry
  7. Použité šifry a protokoly SSL/TLS by mali byť odolné voči známym typom útokov, ako napríklad: FREAK, BEAST (používanie TLS 1.2, pri TLS 1.0 nepoužívanie šifry s AES), BREACH (Pri SSL/TLS musí byť vypnutá http kompresia), POODLE, LOGJAM, TLS Crime (TLS kompresia by mala byť vypnutá).
  8. Dĺžka kľúča asymetrickej šifry RSA, DSA v X.509 certifikáte musí byť aspoň 2048 bitov, odporúčaná dĺžka je aspoň 4096. Toto neplatí pre ECDSA, kedy na dosiahnutie vysokej bezpečnosti postačujú kratšie kľúče – napríklad 256 bitov, odporúčaná dĺžka je aspoň 512 bitov. Odporúčaná dĺžka pre Diffie Hellman algoritmus je 4096 bitov.
  9. X.509 certifikáty musia byť hashované bezpečnými hashovacími funkciami (napr. kvôli možnosti kolíznych útokov nesmie byť použitý algoritmus MD5), ako napríklad SHA512, SHA2, SHA3, bcrypt
  10. Webový server by mal podporovať iba módy, ktoré majú vlastnosť Perfect Forward Secrecy (PFS).
  11. Webový server nesmie podporovať RC4 a nemal by podporovať DES a 3DES.
  12. Webový server by mal podporovať šifru AES256 v móde GCM, na výmenu kľúčov Diffie Hellman algoritmus alebo eliptický Diffie Hellman algoritmus.
  13. Pre všetky kryptografické operácie musia byť použité kryptograficky silné generátory pseudonáhodných čísel.
  14. Konfiguráciu odporúčame otestovať v SSL/TLS teste[[12]](#footnote-12).
  15. Pri správe SSL/TLS je nutné sledovať a v konfigurácii reflektovať aktuálne odporúčania. V prípade použitia WAF/FW pre SSL/TLS preň platia všetky vyššie uvedené požiadavky.
  16. Kompresia by mala byť vypnutá.

**Konfigurácia webového servera**

Systém

* 1. Systém, nainštalované aplikácie a frameworky musia byť pravidelne aktualizované z pohľadu bezpečnosti.
  2. Používané verzie softvéru musia byť podporované, resp. im nesmie končiť podpora.
  3. Počas doby, kedy prebieha údržba, rozsiahlejšia alebo mimoriadna aktualizácia OS/SW a/alebo nasadzovanie bezpečnostných záplat, by mali byť webové servery oddelené od zvyšku siete orgánu riadenia alebo byť umiestnené v izolovaných sieťach.
  4. Na serveri musia byť deaktivované všetky nepoužívané služby, frameworky, doplnky a funkcionality.
  5. Na serveri musia byť zatvorené všetky nepotrebné porty.
  6. Autentifikácia používateľov na OS servera musí zodpovedať nasledujúcim požiadavkám:
  7. Nepotrebné pôvodné účty musia byť odstránené alebo zneplatnené.
  8. Neaktívne kontá musia byť zneplatnené.
  9. Na serveri by mali byť nakonfigurované používateľské skupiny, kontrola prístupu a udeľovanie privilégií by mali byť pre konkrétnych používateľov riadené ich zaradením do týchto skupín.
  10. Heslo ku kontu musí zodpovedať požiadavkám politiky hesiel, ktorá je uvedená v Prílohe 5 a má byť znemožnený útok hádaním či hrubou silou.
  11. Právo na vykonávanie systémových úkonov musí byť obmedzené na poverených administrátorov. Tí by sa navyše vzdialene mali prihlasovať iba v restricted režime, ak sa používa RDP (RDP restricted admin).
  12. Účet lokálneho administrátora webservera musí byť unikátny pre každý webový server.
  13. Servery s OS Windows by nemali byť v doméne alebo by mali byť spravované RO doménovým radičom (RODC – read-only domain controller).

Webový server

* 1. Pri inštalácií webového servera a bezprostredne po nej by mali byť vykonané nasledovné kontroly a akcie:

1. SW webového servera má byť inštalovaný na dedikovanom hostiteľskom zariadení alebo na dedikovanom virtualizovanom OS.
2. Musia byť aplikované dostupné záplaty a aktualizácie na eliminovanie známych zraniteľností
3. Pre webový obsah by mal byť vytvorený dedikovaný fyzický disk alebo logická partícia (separátne od OS a SW webového servera).
4. Všetky služby inštalované popri webovom serveri, ktoré nie sú potrebné (napr. FTP server alebo služba vzdialenej administrácie) musia byť vypnuté alebo odstránené.
5. Nepotrebné východzie účty vytvorené pri inštalácií by mali byť odstránené alebo vypnuté.
6. Z webového servera majú byť odstránené testovacie a ukážkové súbory vrátane vykonateľných súborov a skriptov a dokumentácia výrobcu.
7. Odporúčame na server aplikovať hardenovací skript alebo bezpečnostnú šablónu, vhodný pre daný OS a webový server.
8. Banner HTTP služby by mal byť rekonfigurovaný, podľa potreby aj s ďalšími bannermi tak, aby nereportovali typ a verziu webového servera a podkladového OS.
   1. Webový server by mal podporovať iba HTTP metódy POST a GET.
   2. Webový server nesmú podporovať (musia byť vypnuté) HTTP metódy OPTIONS, TRACK a TRACE.
   3. Webový server musí byť odolný voči SlowHTTP DoS útokom (limitácia počtu spojení z jednej IP adresy, nastavenie timeoutu na HTTP requesty, implementácia loadbalancerov)
   4. Z webového servera musia byť odstránené všetky nadbytočné a nepotrebné súbory a zložky, obzvlášť konfiguračné súbory a zálohy, ladiace výstupy, dočasné súbory, nepotrebné zdrojové kódy a zálohy súborov.
   5. Ladiace funkcionality (napríklad ASP.NET Application Trace) musia byť vypnuté.
   6. Na serveri musí byť nakonfigurovaný defaultný virtuálny host na obsluhu prístupu na webserver prostredníctvom IP adresy (cez prehliadač). Nesmie byť zobrazovaná defaultná stránka použitého frameworku a pod.
   7. Webový server musí zobrazovať v prípade chyby servera iba všeobecné chybové hlásenia.
   8. Webový server by nemal podporovať funkcionalitu listovania adresára (Directory listing, Microsoft IIS tilde directory enumeration).
   9. Súbor robots.txt nesmie obsahovať odkazy na citlivé zdroje aplikácie (napríklad prihlasovanie administrátora a podobne).
   10. Webový server by mal byť chránený WAF (web aplikačný firewall) minimálne s nasledujúcou funkcionalitou:
9. detekcia a prevencia známych útokov (Code injection – SQL, XSS, Command, XPATH, ...),
10. kontrola používateľských vstupov prostredníctvom whitelistingu a ich prekódovanie do HTML entít alebo podobných bezpečných náhrad.
    1. Na zvýšenie dostupnosti webového servera odporúčame použiť load balancery. Podľa možnosti môžu byť rozšírené o web cache. V prípade podpory web cache nesmú byť cacheované administrátorské stránky, prístupové údaje a podobné citlivé informácie.
    2. Na zvýšenie dostupnosti webového servera môžu byť ako bezpečnostné brány použité reverzné proxy. Podľa možnosti môžu byť rozšírené o funkcie akcelerácie šifrovania, používateľskej autentifikácie alebo filtrovania obsahu.
    3. Webový server nesmie podporovať klientom iniciovanú SSL/TLS renegociáciu šifrovacích kľúčov (kvôli DoS útoku).
    4. Webový server musí dodržiavať negociačný postup negociácie TLS spojenia, popísaný v RFC 5746, kvôli zraniteľnosti Insecure renegociation a riziku útoku typu MitM.
    5. Webový server by mal podporovať bezpečnú renegociáciu (Secure renegotiation)
    6. V prípade viacerých virtuálnych hostov musí byť oddelené úložisko cookies minimálne na úrovni adresárov.
    7. Pre umocnenie účinnosti týchto bezpečnostných opatrení odporúčame riadiť sa odporúčaniami pre zariadenia pre nasadenie a zabezpečenie webového servera uvedených v Prílohe 6.
    8. Na webovom serveri by mal byť zapnutý OCSP Stampling na overenie platnosti SSL certifikátov[[13]](#footnote-13).

Administrácia, logovanie a zálohovanie

* 1. Správcovské rozhrania na všetky služby musia byť dostupné iba z dôveryhodných lokalít (potrebná reštrikcia na lokálne siete).
  2. Z produkčných systémov musia byť odstránené všetky testovacie a pôvodné účty.
  3. Všetky servery a syslog servery musia byť synchronizované s dôveryhodným NTP serverom.
  4. Webové správcovské rozhrania musia byť dostupné iba prostredníctvom SSL/TLS.
  5. Na serveri musí byť aktívne logovanie v nasledovnom rozsahu:

1. Malo by byť použité kombinované logovanie na ukladanie Transfer logov (formát podporujúci prispôsobenie formátu logu). Ak takýto formát nie je dostupný, je potrebné zabezpečiť aby bolo logované aj hlavičky Referer a User-Agent.
2. Pre každý virtuálny host na fyzickom webserveri by mal existovať separátny log.
3. V logoch musia byť uvedené: timestamp, kedy udalosť nastala, vrátane určenia časovej zóny, verejná IP adresa používateľa, dopytovaná stránka/URL, HTTP kód odpovede servera, veľkosť odpovede servera v bytoch, obsahy hlavičiek User-Agent a Referer. V prípade záznamov o udalostiach súvisiacich s autentifikáciou alebo s činnosťou  autentifikovaného používateľa je nutné zaznamenať účet a akciu, aká bola vykonaná.
4. Logy musia byť uchovávané na separátnom zariadení, resp. na separátnej logickej partícii.
5. Na uchovávanie logov musí byť vyhradená dostatočná kapacita.
6. Logy by mali byť archivované po dobu stanovenú pravidlami orgánu riadenia, minimálne však počas 6 mesiacov.
7. Logy musia byť kontrolované minimálne raz týždenne.
   1. Webový server musí byť pravidelne zálohovaný nasledovným spôsobom:
8. Zálohovanie servera má byť upravené internými predpismi orgánu riadenia.
9. Archívna záloha musí byť vytvorená minimálne raz ročne.
10. Diferenciálna alebo zmenová záloha webového servera má byť vytvorená na dennej až týždennej báze.
11. Plný backup webového servera by mal byť vytváraný v týždňových až mesačných intervaloch.
12. Zálohy servera by mali byť periodicky archivované na externé médiá.
13. Mala by byť uchovávaná autoritatívna kópia webovej stránky/stránok.

Kontrola prístupu OS a webového servera

* 1. Proces webového servera aj proces backendovej databázy musí byť konfigurovaný tak, aby bežal pod unikátnym používateľským kontom s limitovanou množinou privilégií.
  2. Webový server by mal byť konfigurovaný tak, aby súbory s webovým obsahom boli procesom prislúchajúcim službe webového servera prístupné na čítanie, no nie na zápis. Procesy webového servera by nemali mať právo zápisu do priečinkov, kde je uchovávaný verejný webový obsah (web content).[[14]](#footnote-14)
  3. OS by mal byť nakonfigurovaný tak, aby proces webového servera mohol vytvárať log záznamy, no nemohol ich čítať.
  4. OS by mal byť podľa možnosti nakonfigurovaný, aby dočasné súbory vytvorené procesmi webového servera boli obmedzené na určený a vhodne zabezpečený priečinok. Ak je to možné, prístup k dočasným súborom by mal byť obmedzený na procesy, ktoré ich vytvorili.
  5. Webový obsah a všetky logy vytvárané webovým serverom by mali byť umiestnené na separátnom pevnom disku alebo na inej logickej partícii, ako OS a webový server.
  6. Odporúča sa webový server izolovať od iných procesov použitím prostriedkov ako napríklad chroot, kontajnery, virtualizácia a pod.
  7. Pre externé skripty a programy, vykonávané ako časť obsahu webového servera by mal byť vytvorený samostatný priečinok (napr. JavaScript knižnice a pod).
  8. Mal by byť stanovený maximálny počet procesov webového servera a/alebo sieťových spojení, ktoré by server mal povoliť.
  9. Spúšťanie skriptov, ktoré nie sú výlučne pod kontrolou administratívneho konta, malo by byť zakázané (napr. vytvorením a kontrolou prístupu k separátnemu priečinku, obsahujúcom autorizované skripty).
  10. Použitie symbolických linkov by malo byť pre procesy webového servera zakázané[[15]](#footnote-15).
  11. Odporúčame vytvoriť kompletnú maticu prístupov k webovému obsahu (access matrix). V nej by malo byť definované, ktoré súbory a priečinky majú byť prístupné a pre koho.
  12. V odôvodnených prípadoch odporúčame zaviesť kontrolu proti botom (napr. CAPTCHA, nofollow, filtrovanie kľúčových slov).

HTTP hlavičky a cookies

* 1. Server by mal pri SSL/TLS používať HSTS - HTTP Strict Transport Security. Nastavené by mali byť direktívy:

1. max-age=<číslo> – počet sekúnd, napr. max-age=63072000, počas ktorých má prehliadač automaticky konvertovať všetky HTTP požiadavky do HTTPS a
2. includeSubDomains – indikuje, že všetky subdomény aplikácie musia používať HTTPS.
   1. V odpovediach webového servera sa nesmú nachádzať hlavičky prezrádzajúce použitú technológiu a / alebo jej verziu (Server, X-Powered-By, X-AspNet-Version a pod.).
   2. V hlavičkách sa nesmú nachádzať informácie o použitých technológiách, backendových serveroch, internej infraštruktúre, ani bezpečnostných prvkoch.
   3. Server by mal používať hlavičky:
3. *X-Frame-Options: SAMEORIGIN* (alebo DENY),
4. X-XSS-Protection: 1,
5. X-Content-Type-Options: nosniff,
6. Strict-Transport-Security.
   1. V odpovediach webového servera by sa nemali nachádzať hlavičky X-Forwarded-For a HTTP\_PROXY.

Aplikácia (webový portál)

* 1. Aplikácia musí ošetrovať všetky chyby a výnimky.
  2. Aplikácia musí zobrazovať v prípade chyby aplikácie iba všeobecné chybové hlásenia.
  3. V generovanom kóde nesmú byť prítomné komentáre, citlivé informácie a odkazy na interné IP adresy.
  4. Aplikácia musí pristupovať k ďalším aplikáciám a serverom prostredníctvom doménového mena (nie IP adresy, obzvlášť internej).
  5. Aplikácia nesmie reflektovať obsahy hlavičiek v odpovedi servera.
  6. Pre posielanie citlivých a autentifikačných údajov musí byť vynucované HTTPS spojenie.
  7. Aplikácia nesmie ukladať citlivé údaje (napríklad identifikátor relácie) v URL adrese. V prípade zakázania cookies v prehliadači musí stránka zobraziť hlásenie o nutnosti použitia cookies (ak sa používajú).
  8. Aplikácia by nemala používať odkazy na externé zdroje (zdroje mimo správy prevádzkovateľa alebo inštitúcie verejnej správy na SR).
  9. Aplikácie nesmie používať odkazy na nedôveryhodné externé zdroje.
  10. Všetky činnosti privilegovaných používateľov a administrátorov by mali byť zaznamenávané do log súborov prostredníctvom vzdialených logovacích serverov (syslog, Windows Event Forward).
  11. Aplikácia nesmie používať funkcie vykonávajúce kód zadaný ako vstupný parameter (ako napr. eval() v PHP alebo Python).
  12. Z aplikácie musia byť odstránené všetky ladiace výstupy, dočasné súbory, nepotrebné zdrojové kódy a zálohy súborov.

Autentifikácia a autorizácia

* 1. Aplikácia musí pre všetky autorizačné mechanizmy implementovať politiku, pri ktorej je zakázané všetko, čo nie je explicitne povolené (default-deny).
  2. Aplikácia musí vyžadovať autentifikáciu pre každú privilegovanú operáciu (napr. meno a heslo na prvotné prihlásenie, token).
  3. Aplikácia musí implementovať autorizáciu a autentifikáciu na strane servera.
  4. Musia byť odstránené všetky testovacie a pôvodné účty z produkčných systémov.
  5. Pre všetky citlivé operácie musia byť implementované anti-CSRF tokeny, ktoré musia byť pri vykonaní operácie overované.
  6. Pre webové aplikácie, ku ktorým je na prístup nutná autentifikácia, je nutné zabezpečiť, aby žiadna webová stránka, ktorá má byť prístupná až po autentifikácii, nebola dostupná bez vykonania kompletného procesu autentifikácie.
  7. Autentifikácia musí prebiehať prostredníctvom protokolu HTTPS.
  8. Aplikácia musí vyžadovať používanie silných hesiel podľa požiadaviek uvedených v Príloha 5.
  9. V prípade použitia iniciálnych náhodne generovaných hesiel pre nového používateľa musí aplikácia pri prvom prihlásení vyžadovať zmenu tohto hesla, v súlade s definovanými pravidlami pre tvorbu hesiel.
  10. Aplikácia musí umožňovať administrátorom i používateľom zmeniť ich heslo.
  11. Aplikácia musí vyžadovať pravidelnú zmenu hesla, musí byť nastavený minimálny a maximálny interval na zmenu hesla.
  12. Aplikácia musí pri zmene hesla vyžadovať zadanie starého hesla.
  13. Aplikácia musí pri zmene hesla vyžadovať opakované zadanie nového hesla (2 krát), pričom nové zadané heslá sa musia zhodovať.
  14. Odporúčame pri zmene hesla používať viacfaktorové potvrdenie, napríklad Out-Of-Band kanálom (mail, SMS, ...)
  15. Aplikácia musí po zmene hesla vydať nový identifikátor relácie, cez ktorú zmena hesla nastala. Ostatné relácie príslušného používateľa musia byť zneplatnené.
  16. Aplikácia by mala pri zmene hesla notifikovať používateľa prostredníctvom Out-Of-Band kanála.
  17. Aplikácia musí uložené heslá hashovať prostredníctvom štandardných kryptografických hashovacích funkcií a musí používať soľ (angl. salt).
  18. Aplikácia musí implementovať funkcionalitu pre odhlásenie (log-out) aj pre automatické odhlásenie po istej dobe nečinnosti. Funkcia odhlásenia má byť jednoducho identifikovateľná a dostupná z každej stránky, prístupnej po autentifikácii.
  19. Odporúča sa, aby sa po odhlásení z aplikácie zneplatnili všetky relácie daného používateľa.
  20. Odporúča sa, aby aplikácia podporovala simultánne paralelné prihlásenie k jednému účtu iba z jednej verejnej IP adresy. Odporúča sa, aby aplikácia pri zmene verejnej IP adresy prihláseného používateľa požadovala reautentifikáciu[[16]](#footnote-16).
  21. Odporúča sa naviazanie relácie na parameter User-Agent.
  22. Aplikácia musí podporovať spustenie mechanizmu zamknutia účtu (lockout) po istom počte neúspešných pokusov (maximálne 5) o prihlásenie.
  23. Zamknutie účtu po stanovenom počte neúspešných pokusov o prihlásenie musí trvať aspoň 10 minút.
  24. Zamknutie účtu po stanovenom počte neúspešných pokusov o prihlásenie do ITVS by malo trvať aspoň hodinu.
  25. Je nutné vytvárať log záznamy všetkých pokusov o autentifikáciu (log-in, log-out, neúspešný log-in, lockout konta, žiadosť o zmenu hesla).
  26. V prípade zamknutia účtu by aplikácia mala notifikovať zodpovednú osobu, resp. administrátora aplikácie.
  27. Pre privilegované účty sa musia používať používateľské mená, ktoré nie je možné jednoducho dedukovať (napr. štandardné loginy ako *admin*, *administrator, user* a pod, názov alebo typ aplikácie, kombinácie uvedených a pod.).
  28. Aplikácia nesmie pre ITVS umožniť funkcionalitu zapamätania si hesla.
  29. Používateľské kontá by mali byť po určitej dobe nečinnosti znefunkčnené.
  30. Používateľské kontá, ktoré neboli použité do 3 mesiacov od ich vytvorenia (používateľ sa počas danej doby nikdy neprihlásil), by mali byť deaktivované.
  31. Každý používateľ a administrátor musia mať jedinečné ID.
  32. Aplikácia nesmie umožniť vytváranie účtov s používateľským menom podobným administrátorským či servisným kontám. Napríklad: *admin,* *administrator, helpdesk, support* a pod.
  33. Aplikácia musí korektne inštruovať prehliadač, aby neukladal citlivé informácie, prenášané prostredníctvom HTTPS, do cache (a aby neboli bez kontroly opäť prístupné z histórie prehliadania) minimálne v rozsahu:

1. Server musí nastavovať vo svojich odpovediach hlavičky.
2. Cache-Control: no-cache, no-store, private, must-re-validate, max-age=0, no-transform.
3. Expires: 0.
4. Pragma: no-cache.

Používateľské vstupy

* 1. Všetky používateľské vstupy musia byť kontrolované na strane servera prostredníctvom whitelistov alebo regulárnych výrazov v kontexte, v ktorom sú použité.
  2. Aplikácia musí brať ako vstupy a primerane ošetrovať všetky používateľom ovplyvniteľné časti dopytu, vrátane HTTP hlavičiek, URL, Cookies a pod. Bez ošetrenia nesmú byť reflektované v odpovedi servera. Napríklad:

1. Aplikácia musí byť odolná voči HTTP Spitting/Smuggling útokom
2. Aplikácia by mala byť odolná voči HTTP Parameter Pollution (HPP) útokom.
3. Aplikácia/webový server musí byť odolný voči Host Header útoku.
   1. Aplikácia by mala používať parametrizované SQL požiadavky (queries), tzv. prepared statements.
   2. Aplikácia nesmie na tvorenie SQL dotazov využívať používateľské vstupy bez ich dôkladnej kontroly a ošetrenia.
   3. Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím aspoň v nasledovnom rozsahu:
4. Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v názvoch súborov a zložiek.
5. Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v akomkoľvek skripte, databázovom dopyte alebo parametri príkazu operačného systému.
6. Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v kontexte HTML.
7. Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v kontexte JavaScript.
8. Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v kontexte REST API.
9. Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v XML dokumentoch.
10. Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v XPath požiadavkách (query).
11. Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v XSL(T) style sheets.
12. Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v SSI (Server-Side Inclusion statements) príkazoch, ak je použitie SSI nutné a povolené.
13. Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v HTTP hlavičkách.
14. Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v HTTP parametroch.
15. Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v LDAP požiadavkách.
16. Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v regulárnych výrazoch.
17. Aplikácia musí ošetrovať vstupy/dátové prúdy prechádzajúce medzi modulmi aplikácie.

Relácie

* 1. Aplikácia by mala používať CSRF tokeny o veľkosti aspoň 128 bitov.
  2. Aplikácia by nemala povoliť požiadavky spôsobujúce zmenu údajov, alebo citlivú operáciu bez platného CSRF tokenu.
  3. Aplikácia nesmie povoliť požiadavky na privilegované operácie bez platného CSRF tokenu.
  4. Na generovanie CSRF tokenov musí aplikácia používať kryptograficky silný generátor pseudonáhodných čísel.
  5. Pri prihlásení musí aplikácia znovu vygenerovať nový identifikátor relácie. Identifikátor predchádzajúcej neautentifikovanej relácie musí byť zneplatnený.
  6. Pri zmene prihlasovacích údajov (používateľské meno, heslo) musí aplikácia znovu vygenerovať identifikátor relácie.
  7. Pri zmene prihlasovacích údajov (používateľské meno, heslo) musí aplikácia zneplatniť ostatné relácie príslušného používateľa.
  8. Pre relačné (session) cookies musí aplikácia nastaviť Secure flag.
  9. Pre relačné (session) cookies musí aplikácia nastaviť HttpOnly flag.
  10. Pre relačné (session) cookies musí aplikácia nastaviť reštriktívnu doménu.
  11. Pre relačné (session) cookies musí aplikácia nastaviť reštriktívnu cestu (path).
  12. Pre generovanie relačných identifikátorov musí aplikácia používať kryptograficky silné generátory pseudonáhodných čísel.
  13. Aplikácia by mala používať relačné identifikátory o veľkosti aspoň 128 bitov.
  14. Aplikácia musí zamietať neznáme relačné identifikátory zo strany klienta.
  15. Relačné identifikátory musí aplikácia prenášať iba cez zabezpečené pripojenia. Aplikácia musí vynucovať periodickú exspiráciu a zneplatnenie relácií.

Nahrávanie súborov

* 1. Aplikácia musí nahrávané súbory ukladať mimo koreňového súboru pre dokumenty (document root) na separátnu partíciu disku (inú, ako je vyhradené na zápis logov), kde súčasne nesmie byť možnosť listovania adresára a nesmie byť možnosť interpretovať nahraté súbory ako napríklad skripty (PHP, ASP, JSP, ...).
  2. Aplikácia nesmie spúšťať a vyhodnocovať (evaluate) nahraté súbory.
  3. Aplikácia musí vynucovať limit pre veľkosť nahratých súborov.
  4. Aplikácia by mala obmedzovať počet súborov nahraných za hodinu.
  5. Aplikácia by mala nahrávané súbory kontrolovať na prítomnosť škodlivého kódu prostredníctvom antimalware riešenia.
  6. Nahrávané súbory by sa nemali ukladať pod pôvodným názvom.

Obsah

* 1. Aplikácia by mala pre všetky poskytované zdroje explicitne definovať typ obsahu.
  2. Aplikácia by mala pre všetky poskytované stránky definovať „character set“.
  3. Zabezpečenie aktívneho obsahu (skripty, spustiteľné súbory):

1. Právo na čítanie a zápis do súborového systému by malo byť limitované alebo zakázané.
2. Mala by byť povolená žiadna alebo len limitovaná interakcia s inými programami.
3. Nemala by byť potrebná žiadna akcia so SUID privilégiami (OS UNIX/Linux).
4. Skripty by pri spúšťaní externých programov mali používať absolútne cesty alebo nepoužívať žiadne cesty a spoliehať sa na premennú PATH, pričom tá musí obsahovať len bezpečné adresáre.
5. Žiadne priečinky nesmú mať súčasne práva na zápis a vykonávanie.
6. Spustiteľné súbory by mali byť umiestnené vo vyhradených priečinkoch.
7. SSI (Server-Side Inclusion) by mali byť zakázané, resp. nie je možné ich spúšťať.
   1. Spracovanie XML:
8. Aplikácia nesmie podporovať XML External entity expansion.
9. Aplikácia nesmie podporovať parsovanie XML External DTD.
10. Aplikácia nesmie podporovať všetky nadbytočné alebo nebezpečné XML rozšírenia.
11. Aplikácia by mala používať XML parser, ktorý neexpanduje entity rekurzívne.

Rôzne

* 1. Aplikácia by nemala podporovať presmerovanie na používateľom poskytnuté externé umiestnenia.
  2. Aplikácia by mala obmedziť (krížový) prístup k (cudzím) doménam prostredníctvom whitelistingu.

1. Ak je na riadenie prístupu medzi doménami používané CORS (Cross Origin Resource Sharing), konfigurácia by mala byť obmedzená na dôveryhodné domény. Napr. nemala by byť použitá direktíva *Access-Control-Allow-Origin:\**
2. Ak aplikácia používa na kontrolu prístupu k zdrojom na externých doménach súbory crossdomain.xml a/alebo clientaccesspolicy.xml, obsah by mal mať obmedzený na nutné domény, porty a protokoly. Nemali by byť používané nadmerne voľné pravidlá s „\*“. Crossdomain.xml a clientaccesspolicy.xml nesmú byť prístupné koncovému používateľovi.
   1. Aplikácia by mala pre všetky emailové funkcionality implementovať rate limiting.
   2. Aplikácia by mala pre všetky funkcionality vyžadujúce veľa zdrojov (napríklad CPU čas) implementovať rate limiting.
   3. Pri implementácii rate limitingu sa musí brať ohľad na predchádzanie neúmyselnému odopretiu služby.

Mechanizmus kontroly

* 1. Bezpečnosť webových aplikácií je nutné pravidelne preverovať externým skenom zraniteľností.
  2. Externým penetračným testom by mal prejsť každý projekt ešte pred nasadením do ostrej prevádzky.
  3. Komplexný kontrolný externý penetračný test odporúčame vykonať raz ročne.
  4. V prípade, že webový server sa nachádza v infraštruktúre orgánu riadenia, bezpečnosť podkladového OS má byť preverovaná tak, ako je uvedené v kapitole o zabezpečení internej infraštruktúry orgánu riadenia.
  5. Bezpečnostný audit servera a aplikácie by mal byť vykonaný minimálne raz ročne.

1. **Minimálne požiadavky na zabezpečenie infraštruktúry**

V tejto kapitole sú uvedené požiadavky na zabezpečenie infraštruktúry, ktoré sú spoločné pre internú infraštruktúru aj pre externú infraštruktúru.

Výnimkou k požiadavkám uvedeným v tomto dokumente je tzv. labová sieť – t.j. testovacia sieť určená na testovanie nových technológií. Takáto sieť – ak sa používa – by mala byť fyzicky oddelená od siete orgánu riadenia a mala by využívať vlastné pripojenie do externých sietí. Nesmú existovať prepojenia medzi koncovými stanicami internej siete orgánu riadenia a labovou sieťou.

Všeobecné požiadavky

* 1. Prístup k službe musí byť filtrovaný aspoň na centrálnom FW, na lokálnom FW systému a v konfigurácii danej služby.
  2. Všetok softvér a firmvér musí byť pravidelne aktualizovaný. Musia byť dodržané tieto princípy:

1. Aktualizácia ITVS musí prebiehať prostredníctvom kanála zabezpečujúceho integritu a autentickosť.
2. Odporúča sa vopred otestovať vplyv aktualizácii na ITVS na testovacom zariadení.
3. V prípade infraštruktúry Windows a použitia lokálneho aktualizačného servera (WSUS) je nutné implementovať šifrovanie aj metadát a implementovať používanie certifikátov podpísaných dôveryhodnou certifikačnou autoritou.
   1. Na zariadeniach musí byť zapnuté minimálna množina služieb potrebná pre správne fungovanie. Všetka nepotrebná funkcionalita by mala byť neimplementovaná/neinštalovaná - musí byť aspoň vypnutá.
   2. Konfiguračné súbory musia byť zabezpečené minimálne takto:
4. Konfiguračné súbory by mali byť modifikovateľné len správcom.
5. Súbory obsahujúce heslá, kryptografické kľúče a iné tajomstvá musia byť modifikovateľné a čitateľné len oprávnenými používateľmi.
   1. Správcovské a monitorovacie rozhrania sieťových prvkov a serverov nesmú byť prístupné priamo z externej siete. Správcovské a monitorovacie rozhrania musia byť prístupné len zo špecifikovaných sietí (napr. administrátorská sieť).
   2. Správcovské rozhrania služieb by nemali byť priamo prístupné z externej siete. V prípade potreby dostupnosti takýchto rozhraní sa odporúča využiť správcovská VPN. V prípade nutnosti sprístupnenia priamo z externej siete je nutné sprístupniť to len dočasne pre špecifikované zdrojové IP adresy a odporúča sa využiť dodatočnú formu autentifikácie ako je napríklad použitie klientskych certifikátov.
   3. Správcovské rozhrania zariadení a služieb by nemali byť prístupné cez nešifrované kanály. Pre prístup na správcovské rozhrania sa odporúča využívať autentifikáciu pomocou asymetrickej kryptografie (napr. RSA kľúče, alebo klientske certifikáty). Mal by byť nakonfigurovaný maximálny timeout pre platnosť neaktívneho spojenia. Musia byť logované všetky pokusy o prihlásenie na správcovské rozhrania.
   4. Všetky autentifikačné mechanizmy musia používať silnú autentifikáciu. V prípade hesiel a zdieľaných tajomstiev platia požiadavky na komplexnosť a dĺžku hesla, v prípade certifikátov a kryptografických kľúčov platia požiadavky na minimálnu dĺžku a použitý hashovací algoritmus (požiadavky sú uvedené v Prílohe 5).
   5. Pre ITVS kategórie I3 by mala byť zaistená implementácia kontrolného súčtu (hash funkcií) na kontrolu integrity databáz.
   6. Ak sa nepoužíva IPv6, musí byť vypnutá podpora IPv6 v celej infraštruktúre. To znamená, že koncové stanice musia mať vypnutý IPv6 stack, switche a smerovače nesmú spracovávať a preposielať IPv6, na sieťových firewalloch musia byť nastavené pravidlá zahadzujúce IPv6 komunikáciu vrátane IPv6 komunikácie tunelovanej cez IPv4.
   7. Ak sa používa IPv6, všetky bezpečnostné prvky (napr. FW, IPS, ACL) filtrujúce komunikáciu musia rozoznávať a kontrolovať aj IPv6.
   8. Všetky koncové zariadenia by mali byť nakonfigurované tak, aby nespracovávali ICMP Redirect a ICMPv6 Redirect správy.
   9. Fyzická bezpečnosť zariadení musí byť zabezpečená aspoň v tomto rozsahu:
6. Prístup k zariadeniu musí mať len autorizovaný personál (aspoň na úrovni prístupu do miestnosti, v prípade zdieľaných miestností aj na úrovni stojanového rozvádzača).
7. Musia byť zabezpečené vhodné prevádzkové podmienky zabezpečujúce stabilitu systému určené na základe odporúčaní výrobcu. Minimálne musí byť kontrolovaná teplota, vlhkosť, prašnosť a bezpečný prívod elektrickej energie.

Konfigurácia sieťovej infraštruktúry

* 1. Nepoužívaný verejný IP rozsah orgánu riadenia by mal byť null-routed (t.j. nesmerovaný).
  2. Servery poskytujúce služby či už do externej alebo internej siete musia mať smerom do externej siete povolenú len potrebnú komunikáciu na základe whitelistingu.
  3. Správcovské rozhrania sieťových prvkov by mali byť dostupné len cez dedikované manažmentové rozhranie a z fyzicky oddelenej správcovskej siete.
  4. Sieťové prvky musia byť prístupné prostredníctvom šifrovaného protokolu. Pre prístup by nemal byť použitý telnet ani HTTP, odporúča sa využívať SSHv2 alebo HTTPS. Pre zálohovanie by nemalo byť použité TFTP, odporúča sa SCP alebo SFTP.
  5. Pre autentifikáciu prístupov sa odporúča implementovať autentifikačný server (napríklad TACACS+ alebo Radius). Lokálne heslo nakonfigurované pre offline prístup by malo byť unikátne pre každé zariadenie a prístupné len v prípade potreby a nedostupnosti služby autentifikačného servera. V rámci infraštruktúry by nemali byť používané zdieľané administrátorské heslá. Kedykoľvek je to možné, musia byť heslá v konfigurácii zariadenia uložené v šifrovanej / hashovanej forme. Pričom hash nesmie byť reverzibilný (ako je napr. Cisco password type 7).
  6. Aktívne sieťové prvky musia byť pred nasadením do prevádzky hardenované a to aspoň v rozsahu:

1. Vypnutie nepotrebných služieb (napríklad bootp, CDP, DHCP klient, HTTP server, SNMP a iné).
2. Nastavenie manažment rozhrania, prístupových metód a prístupového ACL.
3. Vypnutie password-recovery precedúry.
4. Nastavenie žiadanej úrovne logovania bezpečnostných udalostí.
5. Odporúča sa hardenovať podľa odporúčaní výrobcu.
   1. Kontrolné správy vymieňané sieťovými prvkami zapojenými v móde "high availability" (napr. hraničné smerovače vo failover móde) musia mať zabezpečenú autentickosť (napríklad využitím silného kľúča) a mali by mať zabezpečenú aj dôvernosť. Taktiež by mali na komunikáciu používať separátny na to určený kanál.
   2. Komunikácia v rámci použitých smerovacích protokolov musí byť autentifikovaná.
   3. Pri každej zmene v sieťovej infraštruktúre je nutné aktualizovať ACL a FW pravidlá.
   4. Odporúča sa dokumentovať účel a potrebu FW pravidiel a ACL pravidiel v komentároch daných pravidiel.
   5. Ak sa používa IPv6, musia byť aplikované IPv6 ACL a FW pravidlá v celej infraštruktúre a musia brať ohľad na špecifiká IPv6. IPv6 infraštruktúra musí byť hardenovaná minimálne v rozsahu:
6. princípy architektúry siete a filtrovania komunikácie na základe „least priviledge“ sú obdobné ako pre IPv4 a mali by byť dodržané základné pravidlá uvedené v tomto dokumente
7. Hraničné routre musia byť nakonfigurované podľa pravidiel uvedených pre IPv4 routre s týmto rozdielom: musia byť schopné odosielať a prepúšťať ICMPv6 Packet Too Big správu.
8. Mal by byť implementovaný anti-bogon filtering na vstupoch z externých sietí.
9. V sieti by nemali byť používané ani povolené „deprecated“ IPv6 funkcionality. Nesmie sa používať Extension Header Routing type 0 a musí byť zahadzovaný na sieťových firewalloch.
10. Nemali by byť používané ani preposielané žiadne IPv6 Extension Headers s výnimkou ESP a AH ak je používaný IPSec.
11. Klientské stanice nesmú byť prístupné priamo z Externých sietí.
12. Klientské stanice by mali pristupovať do Externých sietí cez proxy
13. Sieťové firewally musia byť schopné mapovať k povoleným spojeniam prípadné vracajúce sa ICMPv6 Error správy. Sieťové firewally na rozhraniach interných a externých sietí musia rozoznávať a filtrovať IPv6 extension headers.
14. Pri prideľovaní IPv6 adries serverom by mal byť dodržaný princíp riedkej alokácie adries. Ak sa používa DHCPv6 pre klientské počítače, odporúča sa využiť princíp riedkej alokácie adries.
15. Pakety s multicastovou zdrojovou IPv6 adresou musia byť zahadzované.
16. Smerovače musia rešpektovať IPv6 unicast aj multicast scope (napr. paket s Link Local zdrojovou IP adresou nesmie byť smerovaný ďalej)
17. Zariadenia v sieti by nemali odpovedať na ICMPv6 echo request s multicastovou cieľovou IPv6 adresou
18. Ak sa nepoužíva QoS, odporúča sa normalizácia polí Flow Label a ToS v IPv6 hlavičkách spojení s Externými sieťami.

Zabezpečenie servera

* 1. Odporúča sa aby každá služba bežala na samostatnom serveri. Ak je potrebné využiť jeden server pre viacej služieb, musia na ňom bežať služby s podobným určením a požiadavkami na hardvérovú a softvérovú konfiguráciu.
  2. Všetky servery dostupné z externých sietí musia byť hardenované podľa odporúčaní výrobcu. Všetky servery by mali byť hardenované podľa odporúčaní výrobcu.
  3. Každá sieťovo prístupná služba by mala byť spúšťaná pod dedikovaným používateľom a tento používateľ by mal mať obmedzené práva v rámci systému na nutné minimum. Všetky ostatné služby a aplikácie bežiace na danom serveri by mali bežať s právami obmedzenými na nutné minimum.
  4. Všetky používateľom kontrolované vstupy by mali byť ukladané na diskovú partíciu inú od systémovej partície (na ktorej sú súbory OS a aplikácií).
  5. Pri inštalovaní nového servera sa odporúča začínať od minimálnej inštalácie a doinštalovať programy a služby podľa potreby.
  6. Pri inštalovaní nového servera alebo nasadzovaní novej služby je nutné vykonať to v separátnej sieti (VLAN) na to určenej. Do tejto siete a z tejto siete musí byť povolená len minimálna nutná komunikácia na správcovský prístup, inštaláciu aktualizácii a testovanie služby.
  7. Servery s OS Windows v DMZ (so službami dostupnými z externých sietí) musia byť spravované RO doménovým radičom (RODC – read-only domain controller), alebo ak to nie je možné, tak nesmú byť zaradené v doméne.
  8. Na kritických serveroch s OS Windows ako sú doménové kontrolery, DNS servery apod. musí byť implementovaný whitelisting spúšťateľných súborov (napr. Applocker od Microsoft) tak, aby bolo možné spúšťať iba dôveryhodné povolené aplikácie.
  9. Na kritických serveroch s OS Windows ako sú doménové kontrolery, DNS servery apod. musí byť nainštalovaný a nakonfigurovaný nástroj EMET (od Microsoft) so zapnutými všetkými ochranami, ktoré je možné zapnúť. Ak pre niektorý používaný program nie je možné zapnúť všetky ochrany, odporúča sa prehodnotiť potrebu jeho používania.
  10. Na kritických serveroch ako sú servery s externe dostupnými službami, doménové kontrolery, DNS servery apod, by mali byť aktualizácie a mitigácie pre kritické zraniteľnosti (s vysokým dopadom) aplikované do 72 hodín od ich zverejnenia.

Monitorovanie a logovanie

* 1. V prípade neobvyklej udalosti by mal byť notifikovaný systémový administrátor a to minimálne v týchto prípadoch:

1. blížiace sa zaplnenie kapacity úložného priestoru,
2. neštandardne vysoká záťaž systému (load) alebo
3. detegovaná neobvyklá bezpečnostná udalosť.
   1. Logy by mali byť posielané zabezpečeným kanálom a/alebo dedikovanou správcovskou linkou.
   2. Odporúča sa implementovať unifikovaný centrálny monitorovací systém s nastavenými metrikami pre každé monitorované zariadenie/systém. Príklady nastavenia metrík: upozornenie e-mailom pri 80% zaplnenia diskovej partície, SMS alert pri 95% zaplnení diskovej partície, upozornenie pri 50% využití CPU počas 5 minút, SMS alert pri nedostupnosti kritickej služby viac ako 5 minút.
   3. Musia byť monitorované všetky centrálne sieťové prvky a servery a služby prístupné do externých sietí ako aj kritické interné servery a služby. Mali by byť monitorované všetky sieťové prvky a servery a služby.
   4. Musí byť určený personál zodpovedný za monitorovanie logov a upozornení a vykonanie potrebnej akcie v prípade incidentu. Odporúča sa vytvoriť prvú líniu operátorov, ktorý budú obsluhovať monitorovací systém a korigovať nápravné opatrenia.
   5. Odporúča sa nastaviť monitorovací systém tak aby v prípade vážnych udalostí produkoval aj upozornenie "out-of-band" kanál (napríklad e-mail a SMS).
   6. Logy musia obsahovať korektné informácie o dátume, čase a použitej časovej zóne. Pre korektné nastavenie času sa odporúča nastaviť synchornizáciu s dôveryhodným NTP serverom. Odporúča sa využiť autentifikovanú NTP synchronizáciu.
   7. Granularita logovania musí zodpovedať požiadavkám danej služby alebo zariadenia a jeho kritickosti.
   8. Logovanie musí byť nastavené tak, aby prípadné zaplnenie logovacieho miesta neovplyvnilo stabilitu OS. Možné opatrenia: samostatná disková partícia, rotovanie logov a maximálna veľkosť logov.
   9. Logy z kritických služieb a serverov musia byť synchronizované na samostatné logovacie zariadenie.
   10. Logovacie súbory by mali byť zabezpečené aspoň takýmto spôsobom:
4. Mali by byť čitateľné len administrátorom.
5. Nemali by byť prepisovateľné a vymazateľné (mal by byť možný len zápis na koniec súboru)[[17]](#footnote-17).
6. Odporúča sa komprimovať a šifrovať archivované logovacie súbory. Pri ručnej archivácii sa odporúča aj podpisovať logovacie súbory.
   1. Bezpečnostný monitoring by mal zbierať aspoň tieto informácie z pracovných staníc a serverov (v zátvorkách uvádzame príklady Event ID pre OS Windows 6.0+)
7. Vytvorenie nového používateľa (Windows Security event ID 4720, 4724, 4738)
8. Pridanie používateľa do privilegovanej skupiny (Windows Security Event ID 4728, 4732)
9. informácie o zmazaní logov (Windows Security Event ID 1102)
10. Nainštalovanie novej služby (Windows System Event ID 7045, 7030)
11. Vypnutie lokálneho firewallu (Windows Event ID 2003)
12. Nepovolenie spustenia vykonateľného súboru, kvôli whitelisting pravidlu (Windows Applocker: Event ID 8004)
13. Detekcia a zabránenie vykonania potenciálne škodlivého kódu, alebo vypnutie programu anti-exploit komponentom (Microsoft EMET: Windows Application Log Provider EMET ID 2)
14. Detekcia škodlivého kódu antimalware riešením
15. informácie o všetkých spustených procesoch aj s plným príkazovým riadkom
16. odporúča sa implementovať logovanie prístupu k citlivým aktívam (napríklad súbory, riadky databázovej tabuľky apod.)
    1. Odporúča sa aby bezpečnostný monitoring zbieral aspoň tieto informácie zo sieťového monitoringu:
17. skenovanie sietí a portov, pokus o prístup do nevyužitého IP rozsahu orgánu riadenia, pokus o prístup na honeypot,
18. história dotazov na DNS mená a vyhodnocovanie podozrivých DNS mien (napríklad na základe entropie, reputačných databáz, alebo štatistiky využitia).
    1. Odporúča sa do citlivých interných sietí (napríklad VLAN interných serverov) umiestniť honeypot (t.j. nepoužívaný počítač, ktorého účelom je detegovať prítomnosť útočníka v sieti) a pravidelne alebo automaticky vyhodnocovať, či nebol detegovaný pokus o prístup.
    2. Informácie získané bezpečnostným monitoringom by mali byť vyhodnocované operátorom a v prípade detegovanej zmeny, ktorá nie je zaznamenaná Zmenovým riadením (CM – Change management) by mal byť okamžite spustený proces riešenia bezpečnostného incidentu.
19. **Minimálne požiadavky na zabezpečenie externej infraštruktúry**

Všeobecné požiadavky

* 1. ­Pre servery s verejne prístupnými službami je nutné aplikovať bezpečnostné aktualizácie prioritne a to hneď ako je to možné (minimálne raz za mesiac).
  2. Verejne prístupné zdroje (web, bannery, DNS apod.) nesmú obsahovať informácie o použitých technológiách, interných IP adresách a použitých TCP/UDP portoch.
  3. Verejne dostupné služby by mali byť dostupné takým spôsobom, ktorý umožňuje používateľovi overiť identitu služby a autentickosť údajov (napr. web, VPN). Odporúča sa verejne prístupné služby sprístupňovať len takýmto spôsobom.

Konfigurácia sieťovej infraštruktúry

* 1. Služby dostupné verejnosti (napríklad webové servery) by mali používať iné pripojenie do Internetu ako to, ktoré používa orgán riadenia na prístup k Internetu alebo iným externým sieťam.
  2. ACL na hraničných sieťových prvkoch aplikované na všetku komunikáciu prichádzajúcu z externých sietí musí obsahovať aspoň nasledovné pravidlá:

1. Zahadzovať komunikáciu so zdrojovými IP adresami z rozsahu RFC 1918 (privátne IP adresy).
2. Filtrovať komunikáciu z rozsahu RFC 6890 (IP adresy rezervované pre špeciálne použitie).
3. Zahadzovať komunikáciu so zdrojovými IP adresami z rozsahu používaného v sieti orgánu riadenia.
4. Zahadzovať ICMP protokol s výnimkou ICMP echo request. Echo request musí byť povolený len ak je to potrebné a len do DMZ sietí. Taktiež preň musí byť implementovaný rate-limiting.
5. Odporúča sa implementovať anti-bogon filtering (\*oficiálna databáza je udržiavaná na https://www.team-cymru.org/bogon-reference.html).
   1. Hraničné sieťové prvky by nemali nijak odpovedať na pokusy o pripojenie na neexistujúci TCP/UDP port. Nesmú odosielať správy "ICMP unreachable".
   2. Z externých sietí nesmie byť povolený ICMP protokol. Výnimkou môže byť povolenie "ICMP echo request" na konkrétne servery v DMZ, pričom musí byť limitovaný počet požiadaviek za daný čas.
   3. Mal by byť implementovaný Reverse Path Filtering.
   4. Všetky servery so službami priamo prístupnými z externých sietí musia byť v samostatných sieťových segmentoch (DMZ). V rovnakom segmente by mali byť iba servery s rovnakými bezpečnostnými požiadavkami a podobným účelom.

Firewall

* 1. Všetky prepojenia medzi segmentmi a externými sieťami musia byť chránené firewallom a všetky spojenia (IN aj OUT) musia byť povoľované iba na princípe least privilege.
  2. Smerom do vnútra musia byť povolené len špecifikované služby umiestnené v DMZ (politika "default deny")
  3. Smerom do externých sieti by mala byť povolená len špecifikovaná komunikácia (pre klientské siete by to malo byť len HTTP a HTTPS).
  4. Všetky spojenia do externých sietí musia byť smerované cez dedikovaný sieťový firewall. Všetky spojenia do externých sietí by mali byť smerované aj cez IDS/IPS (ak je IDS/IPS použité) - výnimkou sú komunikácie s veľkým tokom dát alebo počtom paketov (ako napr. VoIP alebo videokonferencie), pre ktoré sa toto odporúča, ak to výkon a funkcionalita IDS/IPS dovoľuje.
  5. Musí byť obmedzená táto komunikácia:

1. DNS požiadavky smerom do externých sietí (dport UDP/TCP 53) môžu iniciovať len autorizované rekurzívne DNS servery.
2. SMTP správy smerom do externých sietí (dport TCP 25) môžu iniciovať len autorizované (t.j. na to určené) SMTP servery.
3. Odporúča sa nepovoľovať smerom do externých sietí komunikáciu na TCP/445 (SMB), TCP/6697 (IRC).

Ochrana proti DoS útokom

* 1. Pre ITVS kategórie A3 je nutné zabezpečiť anti-DoS službu na strane poskytovateľa pripojenia do externej siete, ktorá zablokuje objemové DoS a DDoS útoky ešte pred vstupom do siete orgánu riadenia. Pre ostatné ITVS je takáto služba odporúčaná.
  2. On-site by mala byť implementovaná anti-DoS ochrana chrániaca verejne dostupné služby aj proti ostatným typom DoS útokov ako sú zahltenie aplikácie, pomalé útoky ("low & slow") a SSL/TLS útoky. Takéto riešenie musí byť zabezpečené pre ITVS a základné služby s vysokými nárokmi na dostupnosť (napr. právne záväzné elektronické služby občanom).
  3. Anti-DoS riešenie musí notifikovať dedikovaný personál o výskyte prebiehajúceho útoku, alebo inej anomálie v sieťovej prevádzke. Anti-DoS riešenie musí logovať informácie o zablokovaných pokusoch o útok.
  4. Odporúča sa implementovať vhodný rate-limiting na lokálnych a centrálnych FW.

Zabezpečenie DNS infraštruktúry

* 1. Autoritatívny DNS server by nemal byť zároveň rekurzívnym DNS serverom.
  2. Autoritatívny DNS server musí povoľovať príjem požiadaviek na DNS Zone transfer len zo špecifikovaných IP adries a na Zóny, pre ktoré je autoritatívny. Musí povoľovať vykonať DNS transakciu "Zone transfer" len na špecifikované IP adresy.
  3. Pre požiadavky aj odpovede na "Zone transfer" sa odporúča zabezpečiť autentifikáciu a integritu. Pre požiadavky aj odpovede na "Update" request by mala byť zabezpečená autentifikácia a integrita. Je možné podpisovať dopyty a odpovede zdieľaným kľúčom (využiť napr. HMAC a RR TSIG). Pre každého klienta autoritatívneho servera by mal byť nakonfigurovaný iný kľúč.
  4. Odporúča sa aby boli nakonfigurované ACL pre všetky typy DNS transakcií, ktoré povoľujú len požiadavky od špecifikovaných klientov.
  5. DNS dopyty na name servery sa odporúča limitovať počtom z jednej IP adresy za špecifikovaný čas.
  6. DNS dopyty by mali odchádzať z náhodného TCP/UDP portu.
  7. Odporúča sa aby autoritatívny a sekundárne DNS servery boli logicky a geograficky oddelené.
  8. DNS záznamy o interných zariadeniach nesmú byť prístupné z externých sietí (je možné využiť napríklad SPLIT DNS architektúru, alebo dve rôzne zóny).
  9. Rekurzívny (cache) DNS server nesmie prijímať požiadavky z externých sietí. Nemal by byť z externých sietí vôbec prístupný.
  10. Veľmi citlivé informácie nesmú byť uložené v rámci DNS (napr. špecifické HINFO alebo TXT záznamy).
  11. DNS server by nemal zverejňovať informácie o použitom softvéri - minimálne nesmie odpovedať na špecifické dotazy typu "Version Query".
  12. Musí byť rezervované doménové meno wpad.{doména}, kde {doména} je doménové meno používané orgánom riadenia a je publikované v odpovediach DHCP serverov. Rovnako pre všetky používané subdomény – t.j. wpad.{subdoména}.{doména}.

Zabezpečenie mailovej infraštruktúry

* 1. SMTP banner by nemal obsahovať informácie o použitom softvéri ani iné citlivé informácie. Nesmie byť možné zistiť verziu použitého softvéru prostredníctvom help príkazov.
  2. Mailové správy odchádzajúce z orgánu riadenia by nemali obsahovať informácie o infraštruktúre orgánu riadenia (napríklad privátne IP adresy v hlavičke Received-From).
  3. Odpoveď na príkaz VRFY by nemala obsahovať informáciu o existencií adresy alebo používateľského mena. Odporúča sa odpovedať kódom 252 s generickou hláškou.
  4. Nemala by byť povolená metóda EXPN.
  5. SMTP server by nemal preposlať e-mail, ktorý neobsahuje zdrojovú hlavičkovú e-mailovú adresu.
  6. SMTP server musí prijímať správy na doručenie z externých sietí len pre spravované domény.
  7. SMTP server musí prijímať správy na preposlanie len od autentifikovaných používateľov alebo z určených SMTP serverov.
  8. Server by mal detegovať a blokovať pokusy o rozoslanie veľkého množstva e-mailov.
  9. SMTP server musí kontrolovať správy pomocou anti-spam filtra.
  10. SMTP server musí kontrolovať správy na prítomnosť škodlivého kódu
  11. SMTP server musí logovať všetky detegované anomálie.
  12. SMTP server musí logovať informácie o spracovávaných e-mailoch a tieto informácie by mali byť uchovávané aspoň 6 mesiacov. Musia byť uchovávané aspoň 3 mesiace.
  13. Prístup k e-mailovým účtom musí byť možný len prostredníctvom šifrovaného kanála.
  14. Odporúča sa na prístup k e-mailovej schránke nepoužívať proprietárne protokoly.
  15. Z externých sietí by sa malo pristupovať na e-mail len prostredníctvom HTTPS alebo použitím štandardných protokolov POP3S alebo IMAPS. Odporúča sa autentifikovať klienta aj na základe certifikátu alebo vyžadovať použitie VPN. V prípade použitia iných protokolov by sa malo pristupovať prostredníctvom VPN pripojenia.

Zabezpečenie VPN infraštruktúry

* 1. Všetky VPN spojenia musia byť šifrované. Odporúča sa implementovať a vyžadovať šifrovanie spojenia s využitím Forward Secrecy.
  2. Ak je potrebný vzdialený prístup k správcovským rozhraniam alebo do správcovskej siete, mala by byť využitá autentifikácia s využitím klientskych certifikátov. Aj pre bežných používateľov sa odporúča využiť autentifikáciu na základe klientskych certifikátov. Použité certifikáty musia používať aspoň RSA-2048, odporúča sa RSA-4096.
  3. Ak sa používa PSK, musí byť použitý silný pre-shared key s entropiou aspoň 128 bitov. Odporúča sa náhodne generovaný reťazec.
  4. VPN spojenia musia byť ukončované v samostatnom segmente.
  5. Musia byť špecifikované FW pravidlá oddeľujúce sieť používateľov VPN a zvyšok internej siete a to metódou whitelistingu in aj out na princípe „least privilege“.
  6. Ak sa používa SSL/TLS, mal by byť používaný len protokol TLS1.2. Nesmie byť použitý protokol SSL.
  7. Nesmie byť možné vynegociovať použitie slabých šifier (ako sú napríklad sady šifier využívajúce RC4, DES a 3DES).
  8. Na šifrovanie komunikácie by mal byť použitý protokol AES a to minimálne AES-128 (odporúča sa použiť AES-256). Pre prístup k citlivým ITVS alebo pre správcovskú VPN by mal byť na šifrovanie komunikácie použitý aspoň AES-256.
  9. Mal by byť použitý hashovací algoritmus minimálne SHA-256
  10. Ako algoritmus na výmenu kľúča by mal byť použitý DH (Diffie-Hellman) s dĺžkou aspoň 2048b.
  11. Ďalšie požiadavky na zabezpečenie IPSec VPN:

1. VPN server nesmie umožniť využiť Aggresive mód nadviazania spojenia
2. Mal by sa používať len IKEv2
3. Platnosť šifrovacieho kľúča by mala byť nastavená na maximálne jeden deň
4. Odporúča sa skontrolovať politiky, ktoré sú k dispozícii pre IKE fázu 1 a odstrániť politiky, ktoré umožňujú nastavenie málo bezpečných parametrov
   1. Ďalšie požiadavky na zabezpečenie SSL VPN alebo OpenVPN:
5. Klient musí overovať certifikát VPN servera
6. VPN server musí overovať platnosť klientskych certifikátov a mal by ju overovať aj voči CRL.
7. V klientskej konfigurácii OpenVPN sa odporúča používať perzistentné TUN/TAP rozhrania.

Zabezpečenie VOIP infraštruktúry a služieb videoconference

* 1. VOIP komunikácia z a do externých sietí by mala byť šifrovaná. Odporúča sa šifrovať aj internú VOIP komunikáciu (napr. SIP over TLS a SRTP a SRTCP).
  2. VOIP zariadenia by mali byť z externých sietí do siete orgánu riadenia pripájané len cez VPN .
  3. Všetky VOIP a telepresence zariadenia musia byť pred pripojením do siete hardenované (napr. podľa odporúčaní výrobcu).
  4. Riadiaca komunikácia musí byť autentifikovaná (t.j. call signalling a web services signalling) a mala by byť aj šifrovaná.
  5. Správcovské heslá telefónov musia byť komplexné a rôzne pre každé zariadenie.
  6. Centrálny firewall by mal vedieť filtrovať VoIP komunikáciu. Odporúča sa nasadiť riešenie na filtrovanie VoIP spamu (SPIT - Spam over IP Telephony)
  7. Pre konfiguračné súbory sťahované do telefónov by mala byť zabezpečená integrita a koncové zariadenia by mali overovať integritu týchto súborov.
  8. Videoconferencing meeting by mal byť povinne šifrovaný (t.j. ak to zariadenie účastníka nepodporuje, nemôže sa zúčastniť).
  9. Mal by byť použitý VOIP-aware firewall, ktorý umožňuje inšpekciu SIP protokolu.
  10. SIP server musí byť na portoch TCP/UDP 5060/5061 dostupný len z potrebných zariadení.
  11. Mal by byť použitý SBC (session border controller) a mal by ukončovať všetky prichádzajúce telefonáty a preposielať dáta cieľu (B2BUA)
  12. Pohyblivá kamera na zariadení ako aj zapnutie mikrofónu nesmie byť ovládateľné na diaľku prostredníctvom siete.
  13. Zariadenia pre videoconference by mali byť do siete pripájané len vtedy keď je to potrebné pre potreby videokonferencie alebo servisných zásahov.
  14. Používané kamery, alebo zariadenia s kamerami, musia viditeľne indikovať, že sú zapnuté a snímajú.

Zabezpečenie iných služieb

* 1. Pre prístup k neštandardným službám, ktoré nie je možné hardenovať a zabezpečiť štandardným spôsobom (napr. TLS) sa odporúča využiť prístup cez VPN.

Mechanizmus kontroly

* 1. Otvorené porty do Internetu by mali byť revidované aspoň raz za pol rok. Súčasťou revízie je sken otvorených portov do externých sietí a ohodnotenie, či sú naďalej potrebné.
  2. Penetračné testy externej infraštruktúry by mali byť vykonané aspoň raz za rok.
  3. Aspoň raz za rok by mali byť kontrolované verejne prístupné zdroje s cieľom skontrolovať, či nie sú zverejnené dôverné alebo citlivé informácie.

1. **Minimálne požiadavky na zabezpečenie internej infraštruktúry**

Implementácia architektúry riešenia

* 1. Sieť musí byť **segmentovaná na základe účelu** zariadení v jednotlivých segmentoch a rovnakých bezpečnostných požiadaviek. Minimálne takto:

1. Samostatné subsiete/VLAN pre oddelenia
2. Samostatné subsiete/VLAN pre manažment infraštruktúry a zálohovanie
3. Samostatné subsiete/VLAN pre manažment serverov a ich zálohovanie
4. Samostatné subsiete/VLAN pre servery s rovnakými bezpečnostnými požiadavkami
5. Samostatné subsiete/VLAN pre doménové radiče (okrem RODC)
6. Samostatné subsiete/VLAN pre manažment bezpečnostných prvkov
7. Samostatné subsiete/VLAN pre manažment virtualizačných serverov
8. Samostatné subsiete pre DMZ
9. Samostatné subsiete pre ICS/SCADA systémy
10. Samostatné subsiete pre VOIP
11. Samostatné subsiete pre wireless AP
    1. Prepojenia medzi jednotlivými segmentmi sú chránené prostredníctvom ACL, ktoré sú nakonfigurované na princípe „Least Privilege“.
    2. Pre pripojenia pracovných staníc a všetky dostupné sieťové porty mimo zabezpečených priestorov by malo byť implementované Port Security, Dynamic ARP inspection a DHCP snooping. Ak sa používa IPv6, mali by byť implementované: NDP inspection a snooping, DHCPv6 snooping, RA Guard (Router Advertisement Guard).
    3. Servery prístupné z externých sietí musia byť v iných segmentoch ako servery internej infraštruktúry. Medzi týmito segmentami musí byť implementovaný firewall a ACL na princípe  „Least Privilege“
    4. V sieti by mal byť implementovaný OOBM (Out of band manažment).
    5. Servery prístupné z externých sietí by mali byť na iných virtualizačných serveroch ako servery internej infraštruktúry
    6. Ak je implementovaný SSO (Single Sign-On) pre ITVS kategórie C3 a I3 by mala byť navyše vyžadovaná samostatná doplnková autentifikácia.
    7. Pre prihlásenie do siete (do pracovnej stanice a na služby v doméne) odporúčame využívať dvojfaktorovú autentifikáciu.
    8. V rámci implementácie architektúry by orgán riadenia mal dodržiavať:
12. multi-vendor princíp pre bezpečnostné prvky
13. musí byť dodržané oddelenie DMZ, Perimetra (prvky, ktoré majú priamy prístup do Internetu) a interných častí siete.
14. VPN pripojenia musia byť ukončované v separátnych segmentoch a prístupy k ďalším častiam siete je možné iba prostredníctvom ACL na princípe „Least Privilege“.
15. Interné servery ani pracovné stanice by nemali mať priamy prístup do Internetu ani externých sietí. Všetky pripojenia by mali prechádzať prostredníctvom perimetrových zariadení (Web a email proxy servery Proxy, aplikačné port forwardery pre potrebné iné služby)
    1. V sieti by mali byť implementované lokálne NTP servery.
    2. V sieti by mali byť implementované lokálne DNS servery.
    3. V sieti by mali byť implementované lokálne Syslog servery.
    4. V sieti by mali byť implementované lokálne update servery pre OS Windows aj Linux.
    5. V sieti musia byť implementované:
16. Firewally na všetkých pripojeniach medzi sieťou orgánu riadenia a externými sieťami
17. Firewally na všetkých pripojeniach do kritických segmentov siete
    1. V sieti by mali byť implementované:
18. IPS na všetkých pripojeniach medzi sieťou orgánu riadenia a externými sieťami
19. IPS/IDS na všetkých pripojeniach do kritických segmentov siete
20. Centralizované Anti malware riešenie na všetkých serveroch a pracovných staniciach.
21. Odporúčame ďalej implementovať sieťovú behaviorálnu analýzu na všetkých významných uzloch siete najmä však na známych perimetroch, prepojeniach medzi DMZ, perimetrovými sieťami a internou sieťou.
    1. V infraštruktúre musia byť pravidelne aktualizované OS a všetky aplikácie a aspoň:
22. Raz za mesiac pre OS na platforme Windows
23. Raz za mesiac pre OS na platforme Linux a Unix
24. Raz denne pre antivírové riešenia na klientskych pracovných staniciach
25. Raz za týždeň pre antivírové riešenia na serveroch
26. Raz za 6 mesiacov pre OS bezpečnostných prvkov, sieťových prvkov a iných zariadení pripojených do infraštruktúry
27. Raz za mesiac všetky aplikácie na klientskych zariadeniach
28. Raz za rok všetky aplikácie a služby na serveroch
    1. V infraštruktúre sa musia používať iba podporované verzie OS a aplikácií. Všetky výnimky musia byť schválené a implementované bezpečnostné opatrenia tak, aby nebolo možné tieto verzie zneužiť na kompromitáciu infraštruktúry.
    2. Všetky účty, ktoré majú administrátorské oprávnenia musia spĺňať politiku hesiel pre účty s administrátorským prístupom.
    3. Všetky účty, ktoré neboli použité do troch mesiacov (a zmenené heslo) od ich vytvorenia musia byť zablokované.

Hardening serverov, sieťových a bezpečnostných prvkov

* 1. Všetky nepoužívané a nepotrebné služby musia byť vypnuté.
  2. Všetky firmware musia byť pravidelne aktualizované a hardenované podľa odporúčaní výrobcu.
  3. Administračné rozhrania typu ILO resp. iDRAC musia byť aktualizované a prístupné iba z administrátorskej siete a musia byť v samostatných segmentoch.
  4. Prístup k administrátorským rozhraniam musí byť iba zo siete administrátorov, ktorá je rozdielna od siete používateľov.
  5. Servery nesmú umožniť prihlásenie anonymného používateľa (Guest prístup)
  6. Servery musia mať nakonfigurovaný a udržiavaný host-based firewall (napríklad iptables v Linux alebo Windows firewall vo Windows) na princípe „least privilege“ pre spojenia dnu aj von.
  7. Servery by mali mať partície na diskoch v RAID 1,5, 6, 10 alebo 50.
  8. Všetky zariadenia by mali používať lokálne DNS servery.
  9. Všetky zariadenia musia byť synchronizované s NTP serverom.
  10. Všetky zariadenia by na synchronizáciu mali používať lokálny NTP server.
  11. Všetky zariadenia by mali posielať logy na vzdialený logovací server:

1. Pre zariadenia ktoré podporujú syslog na vzdialený syslog server
2. Pre zariadenia Windows na vzdialený Windows Log server prostredníctvom funkcionality Windows Event Forwarding
   1. Všetky servery by mali mať nainštalované antimalware riešenie s centrálnym manažmentom a zberom logov .
   2. Syslog servery:
3. Musia mať dostupnú dostatočnú diskovú kapacitu na uloženie dát aspoň na 6 mesiacov
4. Musia byť synchronizované s NTP serverom
5. Logy musia byť pravidelne zálohované (minimálne raz za mesiac)
6. Logy musia byť pre všetkých používateľov syslog serveru nastavené iba na čítanie
   1. Administračné rozhrania by mali byť prístupné iba prostredníctvom šifrovaných sieťových kanálov.
7. Šifrované kanály sa musia prezentovať dôveryhodným verejným kľúčom alebo certifikátom
8. V prípade, že nie je možné používať šifrované kanály by malo byť implementované ACL na princípe "Least privilege" a vyčlenené tieto rozhrania do samostatných segmentov
   1. Logovanie musí zaznamenávať[[18]](#footnote-18):
9. (Úspešné aj neúspešné) Prihlásenie a odhlásenie
10. (Úspešné aj neúspešné) Spustenie procesu alebo služby
11. (Úspešné aj neúspešné) Vytvorenie, modifikáciu alebo zmazanie používateľa alebo skupiny
12. (Úspešné aj neúspešné) Pokusy pristúpiť k citlivým údajom
13. (Úspešné aj neúspešné) Spustenie a ukončenie procesu
14. (Úspešné aj neúspešné) Prihlásenie sa zo systému na iný systém alebo službu

Sieťové prvky

* 1. Všetky nepotrebné služby musia byť vypnuté alebo odinštalované.
  2. OS/firmvéry by mali byť pravidelne aktualizované.
  3. Používateľské heslá by nemali byť uložené v reverzibilnom formáte.
  4. Pre pripojenie pracovných staníc by mal orgán riadenia využívať NAC (napríklad NAP alebo 802.1x).
  5. Vo všetkých používateľských segmentoch by mala byť implementovaná PVLAN.
  6. V sieti by nemalo byť používané SNMPv2 (SNMPv2c) a malo by byť používané SNMPv3, ak sa SNMP používa.

1. V prípade použitia SNMPv2 (SNMPv2c) musia community reťazce spĺňať politiku hesiel pre účty s administrátorským prístupom.
2. Community reťazce musia byť unikátne pre sieťový segment a účel použitia.
   1. V Pre všetky dátové toky a služby v rámci monitoringu musia byť implementované ACL na princípe "Least privilege".

Monitoring

* 1. V sieti by mal byť implementovaný dohľad nad funkčnosťou zariadení a služieb.
  2. V rámci siete by mal byť implementovaný bezpečnostný monitoring ktorý bude monitorovať aspoň:

1. bezpečnostné prvky,
2. sieťové prvky orgánu riadenia a
3. doménu Windows.

Tlačiarne

* 1. Tlačiarne by mali byť umiestnené v samostatnom segmente.
  2. Správcovské rozhrania by mali byť prístupné iba z administrátorskej siete a musí byť na správcovskom rozhraní implementovaná autentifikácia a účty musia spĺňať politiku hesiel pre používateľov.
  3. Tlačiarne by mali byť prístupné klientom iba prostredníctvom tlačových serverov.

Windows infraštruktúra

* 1. Na všetkých serveroch musí byť zakázaný prístup na čítanie prostredníctvom neautentifikovaného používateľa (napríklad ošetrená tzv. CIFS null zraniteľnosť)
  2. Na doménových radičoch nesmú byť ukladané heslá prostredníctvom Group Policy Preferences v aplikovaných doménových politikách.
  3. Všetky interné servery by mali byť v doméne.
  4. Autentifikácia na servery by mala byť iba prostredníctvom Kerberosu
  5. Autentifikácia prostredníctvom NTLM by mala byť zakázaná
  6. SMB podpisovanie musí byť vyžadované
  7. Na všetkých serveroch musia byť implementované dôveryhodné certifikáty na prístup ku všetkým službám (RDP, HTTPS,LDAPS,..)
  8. Doménoví administrátori a enterprise administrátori musia mať zakázaný prístup a autentifikáciu na všetky pracovné stanice.
  9. Servery prístupné z externých sietí nie sú v doméne alebo sa autentifikujú voči RODC, ktorý je v samostatnom segmente (DMZ) a je prístupný iba z ostatných DMZ.
  10. Administrátorské a používateľské účty administrátorov musia byť oddelené a mať rozdielne heslá
  11. Doménoví administrátori by mali využívať dvojfaktorovú autentifikáciu
  12. Počítače musia byť do domény pridávané pod samostatným účtom, ktorý ma oprávnenie iba pridávať počítače do domény. Žiadni iní používatelia nesmú mať právo pridať počítač do domény.
  13. V sieti by malo byť vypnuté prostredníctvom GPO automatické vyhľadávanie proxy servera WPAD. Konfigurácia proxy servera by mala byť nakonfigurovaná prostredníctvom GPO.
  14. Implementácia nového softvéru na servery by mala prebiehať prostredníctvom balíčkovacích nástrojov (Deployment services resp. System center)
  15. Remote powershell execution by malo byť povolené len z administrátorskej siete.
  16. V prípade používania RDP musí byť možné prihlasovanie iba v restricted režime (RDP restricted admin).
  17. GPO preferences musia byť vypnuté

Mechanizmus kontroly

* 1. Mal by byť interný penetračný test aspoň raz za 2 roky. Aplikovanie odporúčaní výsledkov penetračného testu.
  2. Odporúča sa vykonať interný technický audit splnenia požiadaviek plynúcich z tohto dokumentu.

1. **Minimálne požiadavky na zabezpečenie pracovných staníc pristupujúcich k implementovanému riešeniu**

Všeobecné požiadavky

* 1. Na pracovných staniciach musí byť nainštalované anti-malware riešenie

1. Riešenie musí byť pravidelne aktualizované (aspoň jeden krát za deň)
2. Riešenie musí byť pravidelne využité na skenovanie pracovnej stanice (aspoň raz za týždeň)
3. Riešenie musí podporovať rezidentnú ochranu[[19]](#footnote-19) a táto musí byť aktívna
4. Riešenie by malo byť centrálne spravované a  malo by mať centrálne vyhodnocované výsledky skenov a detekcie hrozieb
5. Logy z anti-malware riešenia musia byť archivované minimálne 6 mesiacov
   1. OS, všetky jeho súčasti a nainštalované aplikácie musia byť vo verziách podporovaných výrobcom a pravidelne aktualizované (najviac s oneskorením jeden mesiac).
   2. Aktualizácie, záplaty a opatrenia pre kritické zraniteľnosti (s vysokým dopadom) by mali byť aplikované do 72 hodín od ich zverejnenia na pracovných staniciach, z ktorých je možný prístup ITVS a dátam. Mal by byť vedený zoznam takýchto staníc.
   3. Na pracovných staniciach by malo byť zapnuté automatické sťahovanie a inštalácia aktualizácií.
   4. Na pracovných staniciach musí byť implementovaný lokálny firewall:
6. Všetky prichádzajúce aj odchádzajúce spojenia musia byť zakázané okrem spojení, ktoré sú potrebné na štandardnú činnosť aplikácie.
7. Pravidlá vo firewalli by mali byť centrálne spravované a implementované na princípe „least privilege“
8. Všetky zakázané spojenia musia byť archivované minimálne na dobu 6 mesiacov.
9. Informácie o zakázaných spojenia by mali byť archivované na centrálnom úložisku

Logovanie

* 1. Bezpečnostné Logy z pracovných staníc by mali byť odosielané na centrálny server a ukladané minimálne po dobu 6 mesiacov.
  2. Na pracovných staniciach by malo byť logovanie nastavené minimálne v rozsahu:

1. (Úspešné aj neúspešné) Prihlásenie a odhlásenie
2. (Úspešné aj neúspešné) Spustenie procesu alebo služby
3. (Úspešné aj neúspešné) Vytvorenie, modifikáciu alebo zmazanie používateľa alebo skupiny
4. (Úspešné aj neúspešné) Pokusy o prihlásenie prostredníctvom RDP, SSH

Hardening

* 1. Pracovná stanica musí byť hardenovaná minimálne v rozsahu

1. Všetky Windows pracovné stanice musia byť pripojené do domény
2. Všetky služby, ktoré nie sú potrebné sú odinštalované alebo aspoň zakázané alebo vypnuté.
3. Všetky programy a súčasti OS, ktoré nie sú potrebné sú odinštalované
4. Všetky programy boli povolené a otestované bezpečnostným útvarom orgánu riadenia
5. Používatelia nemajú administrátorské oprávnenia
6. Lokálne administrátorské účty sú neaktívne. Ak musia byť z nejakého dôvodu aktívne heslá k týmto účtom spĺňajú požiadavky na heslá pre účty s administrátorským prístupom[[20]](#footnote-20)
7. Pracovné stanice musia na prihlásenie vyžadovať heslo
8. Po dobe nečinnosti (najviac 30 minút) musí byť spustený šetrič obrazovky a uzamknutá pracovná plocha
   1. V prípade pracovných staníc s OS Windows musí byť pracovná stanica hardenovaná minimálne v rozsahu:
9. Používatelia nemajú právo inštalácie softvéru
10. Používatelia ani administrátori nemajú Debug privilégium.
11. Na pracovnej stanici je počet uložených hashov prihlasovacích účtov nastavený na maximálne dva[[21]](#footnote-21).
12. Na pracovnej stanici by mal byť implementovaný whitelisting spustiteľných súborov (napr. Applocker alebo Software Restriction Policies [SRP]) tak, aby bolo možné spúšťať iba dôveryhodné povolené aplikácie.
13. Na pracovnej stanici musí byť zapnutý UAC (User Access Control) a mal by byť nastavený na najvyššiu hodnotu.
14. Na pracovnej stanici by mal byť nainštalovaný a nakonfigurovaný nástroj EMET (od Microsoft) so zapnutými všetkými ochranami, ktoré je možné zapnúť. Ak pre niektorý používaný program nie je možné zapnúť všetky ochrany, odporúča sa prehodnotiť potrebu jeho používania.
15. Doménoví administrátori a ostatní privilegovaní používatelia nemajú oprávnenie na prihlásenie sa na pracovné stanice.
16. Na pracovnej stanici je vypnuté automatické spúšťanie programov po vložení vymeniteľného média (Autoplay)
17. IPv6 by malo byť vypnuté, pokiaľ nie je používané
18. NetBios nad IPv4 by mal byť vypnutý
19. Makrá v MS Office by mali byť vypnuté a nemalo by byť možné ich povoliť. Ak sú makrá používané, malo by byť ich vykonávanie povolené len pre konkrétneho používateľa a len z dôveryhodných špecifikovaných lokalít (nie z Internetu), prípadne implementovať podpisovanie makier pomocou PKI.
20. Lokálne účty nesmú byť zlinkované s MICROSOFT ID
21. Dáta na pracovnej stanici nesmú byť synchronizované prostredníctvom verejných služieb (OneDrive, DROPBox, Google Drive, MEga a podobne)
    1. Prenosné pracovné stanice musia byť hardenované minimálne v rozsahu:
22. Disk musí byť šifrovaný (Full disk encryption)
23. Záložný kľúč k šifrovanému disku by mal mať orgán riadenia k dispozícií (Implementovaný key escrow mechanizmus)
24. BIOS/UEFI by mal byť chránený heslom pri prenosných zariadeniach.
    1. Webové prehliadače by mali mať implementovanú funkcionalitu alebo rozšírenia:
25. Rozšírenie na blokovanie spúšťania skriptov (napr. NoScript)
26. Rozšírenie na blokovanie reklamy (napr. Adblock, UBlock Origin)
27. Rozšírenie na blokovanie trackerov (napr. Privacy Badger)

Mechanizmus kontroly

Rovnaký ako pre internú infraštruktúru.

1. **Administratívne opatrenia**

Všeobecné požiadavky

* 1. Orgán riadenia musí vytvoriť, schváliť, implementovať, dokumentovať a dodržiavať Bezpečnostnú politiku, ktorá spĺňa aspoň nasledovné požiadavky:

1. Je adekvátna veľkosti, typu, zameraniu a činnostiam orgánu riadenia.
2. Definuje bezpečnostné ciele, spôsob ich schvaľovania, dosahovania a merania účinnosti ich dosahovania.
3. Vyjadruje záväzok vedenia orgánu riadenia dosahovať stanovené bezpečnostné ciele a spĺňať požiadavky všetkých zainteresovaných strán.
4. Definuje rozsah a pravidelnosť školení zamestnancov a iných aktivít zameraných na zvyšovanie povedomia o informačnej bezpečnosti, súvisiacich hrozbách a možnostiach ochrany pred týmito hrozbami.
5. Je publikovaná na mieste prístupnom všetkým zamestnancom a je propagovaná v rámci orgánu riadenia a v rámci školení – a to aspoň každých 12 mesiacov – je adekvátne komunikovaná všetkým zamestnancom.
6. Definuje roly a zodpovednosti za informačnú bezpečnosť. Musia byť definované zodpovednosti aspoň pre tieto roly: vrcholný predstaviteľ orgánu riadenia, manažér pre bezpečnosť, vedúci pracovník, administrátor, audítor, používateľ.
7. Definuje spôsob riadenia informačných aktív a spôsob vedenia inventáru/zoznamu týchto aktív.
8. Definuje spôsob vykonávania manažmentu rizík informačnej bezpečnosti.
9. Definuje spôsob nahlasovania a reakcie na bezpečnostné incidenty.
10. Definuje spôsob vykonávania a frekvenciu preskúmavania bezpečnostnej politiky.
11. Definuje spôsob vykonávania a frekvenciu vykonávania interných auditov informačnej bezpečnosti.
    1. Orgán riadenia musí vytvoriť, schváliť, implementovať, dokumentovať a dodržiavať Smernicu pre manažment rizík informačnej bezpečnosti, ktorá spĺňa aspoň nasledovné požiadavky:
12. Definuje spôsob identifikácie a ohodnotenia informačných aktív.
13. Definuje spôsob identifikácie a ohodnotenia hrozieb, ktoré vplývajú na informačné aktíva.
14. Definuje spôsob identifikácie a ohodnotenia zraniteľností, ktoré informačné aktíva obsahujú.
15. Definuje spôsob ohodnotenia rizík na základe identifikovaných hrozieb a zraniteľností.
16. Definuje postup pre výber spôsobu ošetrenia identifikovaných rizík, ktorými sú najmä redukcia rizika, akceptácia rizika, vyhnutie sa riziku, resp. prenos rizika na inú stranu.
17. Definuje spôsob pre vytvorenie Plánu pre ošetrenie rizík, ktorý stanovuje konkrétne opatrenia, zodpovednosti za implementáciu týchto opatrení, termíny a potrebné zdroje na ošetrenie rizík.
18. Definuje spôsob vyhodnotenia efektívnosti implementovaných opatrení.
    1. Orgán riadenia musí vytvoriť, schváliť, implementovať, dokumentovať a dodržiavať Smernicu pre bezpečné používanie aktív, ktorá spĺňa aspoň nasledovné požiadavky:
19. Definuje pravidlá pre bezpečné používanie e-mailu, služieb v Internete a iných komunikačných prostriedkov.
20. Definuje pravidlá pre bezpečnú prácu s heslami.
21. Definuje pravidlá pre inštaláciu hardvéru a softvéru.
22. Stanovuje zákaz inštalácie alebo používania neautorizovaného alebo nelegálneho softvéru.
23. Definuje pravidlá pre ochranu pred škodlivým softvérom a základnými útokmi na používateľa.
24. Definuje pravidlá pre bezpečné používanie aktív mimo priestorov orgánu riadenia.
25. Je publikovaná na mieste prístupnom všetkým zamestnancom a je propagovaná v rámci orgánu riadenia a v rámci školení – a to aspoň každých 12 mesiacov – je adekvátne komunikovaná všetkým zamestnancom.
26. Je pravidelne preskúmavaná aspoň každých 12 mesiacov a v prípade zmien v rámci orgánu riadenia alebo zmien v jeho ITVS alebo v prípade výskytu bezpečnostných incidentov je aktualizovaná a jej zmena je komunikovaná všetkým zamestnancom orgánu riadenia.
    1. Orgán riadenia musí vytvoriť, schváliť, implementovať, dokumentovať a dodržiavať Smernicu pre riadenie prístupu, ktorá spĺňa aspoň nasledovné požiadavky:
27. Definuje spôsob žiadania o prístup, schvaľovania a prideľovania prístupu k jednotlivým ITVS a fyzickým priestorom na základe objektívnej potreby a zamýšľaného používania ITVS či potreby prístupu do fyzických priestorov.
28. Definuje zodpovednosti za prideľovanie, monitorovanie, pravidelné preskúmavanie prístupových práv do ITVS a odstraňovanie neplatných účtov.
29. Definuje spôsob monitorovania prístupov do ITVS, monitorovania používania ITVS a vyhodnocovania auditných log záznamov.
30. Definuje spôsob riadenia jednotlivých typov prístupových účtov a manažment privilégií.
31. Definuje spôsob implementácie oddelenia povinností (tzv. Separation of Duties) s cieľom predchádzať škodlivej aktivite a chybám.
32. Definuje spôsob implementácie minimálnych privilégií (tzv. Least Privilege) s cieľom zaistiť prístup len k tým aktívam a aplikáciám, ktoré sú potrebné na vykonávanie pracovných úloh.
33. Definuje spôsob časového obmedzenia používania aktív, ITVS a aplikácií a spôsob uzamknutia relácie pri definovanom čase nečinnosti používateľa.
34. Definuje spôsob vzdialeného prístupu k aktívam, ITVS a aplikáciám, monitorovanie vzdialeného prístupu a bezpečnostné požiadavky pre vzdialený prístup.
35. Definuje spôsob riadenia prístupu k bezdrôtovým sieťam.
36. Definuje spôsob riadenia prístupu mobilných zariadení.
37. Definuje spôsob riadenia prístupu k ITVS s verejne dostupným obsahom (napr. webové sídlo, účet na sociálnych sieťach a pod.).
    1. Orgán riadenia musí vytvoriť, schváliť, implementovať, dokumentovať a dodržiavať Smernicu pre riešenie kybernetických bezpečnostných incidentov, ktorá spĺňa aspoň nasledovné požiadavky:
38. Definuje spôsob klasifikácie incidentov, ktorý obsahuje aspoň nasledovné typy incidentov: nežiaduci obsah, škodlivý kód, získavanie informácií, pokus o prienik, prienik, nedostupnosť, ohrozenie bezpečnosti informácií, podvod, sprenevera.
39. Definuje spôsob komunikácie, komunikačné kanály a postupy nahlasovania incidentov.
40. Definuje roly a zodpovednosti pri riešení incidentov.
41. Definuje spôsob riešenia incidentov.
42. Definuje spôsob zaistenia dôkazov.
43. Definuje spôsob vedenia dokumentácie o bezpečnostných incidentoch.
44. Definuje spôsob vyšetrovania bezpečnostných incidentov,  spôsob vyvodzovania zodpovednosti a ukladaní sankcií za spôsobený incident.
    1. Orgán riadenia musí vytvoriť, schváliť, implementovať, dokumentovať a dodržiavať Smernicu pre riadenie kontinuity činností, ktorá spĺňa aspoň nasledovné požiadavky:
45. Definuje roly a zodpovednosti za jednotlivé činnosti pri riadení kontinuity činností.
46. Definuje ciele riadenia kontinuity činností.
47. Definuje požiadavky na vykonanie analýzy dopadov a analýzy rizík.
48. Definuje spôsob určenia cieľovej doby obnovy (RTO – recovery time objective) a cieľového bodu obnovy (RPO – recovery point objective) pre jednotlivé procesy, ITVS a aplikácie.
49. Definuje spôsob tvorenia stratégie kontinuity činností.
50. Definuje spôsob vytvorenia havarijných plánov a plánov obnovy.
51. Definuje komunikačné plány v prípade mimoriadnej udalosti (prerušenia činností).
52. Definuje frekvenciu vykonávania cvičení a testovania plánov kontinuity činností a školení.
53. Definuje frekvenciu preskúmavania a aktualizácie plánov kontinuity činností.
    1. Zmluvy s dodávateľmi musia ustanoviť právo orgánu riadenia vykonať u dodávateľa audit bezpečnosti informačných systémov a kontrolu dodržiavania bezpečnostných požiadaviek. Taktiež musia zaväzovať dodávateľa opraviť prípadné nájdené nedostatky.
    2. Orgán riadenia musí, pri dodávaní služieb súvisiacich s IKT, s dodávateľom uzavrieť dohodu o úrovni poskytovania služieb (SLA), ktorá musí obsahovať aspoň[[22]](#footnote-22):
54. Bezpečnostné opatrenia, ktoré je dodávateľ povinný dodržiavať.
55. Požiadavky na monitorovanie súladu s SLA a aktívne hlásenie nedodržania bezpečnostných požiadaviek a bezpečnostných incidentov súvisiacich s poskytovaním služieb.
56. Dohodu, že aktivity vykonávané dodávateľom sú ním dokumentované a podliehajú kontrole a auditu zo strany orgánu riadenia.
57. Finančné pokuty za nedodržanie dohody.
58. Právo na odstúpenie od dohody v prípade, že nie sú naplnené jej podmienky.
    1. Orgán riadenia musí zaviesť nasledovné predpisy:
59. Bezpečnostná politika pre prácu tretích strán a ich účasť v procesoch orgánu riadenia.
60. Smernica pre vzdialený prístup do ITVS.
61. Smernica pre klasifikáciu informácií v súlade s touto vyhláškou.
    1. Orgán riadenia by mal zaviesť nasledovné predpisy:
62. Smernica pre výkon interného auditu.
63. Smernica pre BYOD a prácu na diaľku.
64. Smernica pre ničenie informácií a ich nosičov.
65. Smernica pre riadenie zraniteľností a implementáciu záplat.
    1. Orgán riadenia by mal viesť aspoň nasledovné záznamy:
66. Záznamy o školeniach, kvalifikácii a skúsenostiach zamestnancov.
67. Výsledky monitorovania a merania informačnej bezpečnosti.
68. Program interných auditov a výsledky (správy) z vykonania interných auditov.
69. Log záznamy, záznamy o bezpečnostných udalostiach a bezpečnostných incidentoch.

Mechanizmus kontroly

* 1. Bezpečnostná politika a bezpečnostné smernice musia byť pravidelne preskúmavané manažérom bezpečnosti aspoň raz za každých 12 mesiacov a vždy v prípade zmien v rámci orgánu riadenia alebo v jeho ITVS, alebo v prípade výskytu bezpečnostných incidentov.
  2. Dodržiavanie bezpečnostnej politiky a bezpečnostných smerníc musí byť pravidelne kontrolované prostredníctvom pravidelných interných auditov informačnej bezpečnosti.

**Príloha č. 4**

**k vyhláške č. xx/2019 Z. z.**

**Zoznam atribútov SAML Assertion**

1.1 Zoznam atribútov SAML Assertion v štruktúre AttributeStatement je uvedený v tejto  
tabuľke:

|  |  |
| --- | --- |
| **Atribút** | **Význam** |
| ActorIDSector | Typ použitého identifikátora v kontexte informačného systému, ktorý je zdrojom a správcom identity použitej v atribúte ActorID pre rolu aktér. Hodnotou je textový reťazec. Pre identity federované z ústredného portálu verejnej správy je hodnotou „SECTOR\_UPVS“. |
| ActorID | Samotný identifikátor identity v roli aktér - používateľ, ktorý akciu vykonal. Hodnotou je identifikátor právnickej osoby alebo identifikátor fyzickej osoby. |
| SubjectIDSector | Typ použitého identifikátora v kontexte informačného systému, ktorý je zdrojom a správcom identity použitej v atribúte SubjectID pre rolu subjekt. Hodnotou je textový reťazec. Pre identity federované z ústredného portálu verejnej správy je hodnotou„SECTOR\_UPVS“. |
| SubjectID | Samotný identifikátor identity v roli subjekt. Subjektom je konkrétna osoba, v mene ktorej sa vykonáva proces. Hodnotou je identifikátor právnickej osoby alebo identifikátor fyzickej osoby. V prípade, že používateľ koná vo svojom mene, hodnota je totožná s ActorID. |
| DelegationType | Typ zastupovania: v akom vzťahu je identita SubjectID k identite ActorID. Hodnotou je 0 – generálne zastupovanie podľa všeobecne záväzného právneho predpisu, napríklad konateľ právnickej osoby, alebo súdom určený zástupca nesvojprávnej osoby, 1 až n – delegované zastupovanie. |
| QAAlevel | Úroveň autentifikácie podľa prílohy č. 6 tabuľky č. 8[[23]](#footnote-23), ktorú použil používateľ pri prihlásení sa do systému. Hodnotou je číslo úrovne autentifikácie elektronických služieb verejnej správy. |

1.2 Atribúty podľa bodu 1.1 môžu byť rozšírené o ďalšie atribúty, potrebné pre špecifickú  
implementáciu.

**Príloha č. 5**

**k vyhláške č. xx/2019 Z. z.**

**Politika hesiel**

**Heslá pre účty s administrátorskými oprávneniami**

1. Dĺžka hesla musí byť aspoň 14 znakov
2. Heslá musia obsahovať
3. aspoň jedno veľké písmeno
4. aspoň jedno malé písmeno
5. aspoň jednu číslicu
6. aspoň jeden špeciálny znak
7. Odporúčame aby heslo obsahovalo aspoň jeden znak s diakritikou (ak je heslo používané v rámci homogénneho prostredia)
8. Zmena hesla
9. Heslá by mali byť zmenené aspoň raz za rok
10. Odporúča sa aby zmenené heslá mali od pôvodného hesla editačnú vzdialenosť aspoň 7 (t.j. počet operácií vymazania, vloženia alebo prepísania znaku, ktorými sa z pôvodného hesla dá získať nové)
11. Zmenené heslo by nemalo byť jedným z posledných 15 hesiel v histórii hesiel pre daný účet
12. Heslo je možné zmeniť najviac raz za 1 deň.

**Heslá pre účty s privilegovaným prístupom**

1. Dĺžka hesla musí byť aspoň 12 znakov (20 znakov pre systémové a technické účty)
2. Heslá musia obsahovať
3. aspoň jedno veľké písmeno
4. aspoň jedno malé písmeno
5. aspoň jednu číslicu
6. aspoň jeden špeciálny znak
7. Zmena hesla
8. Heslá musia byť zmenené aspoň raz za 2 roky
9. Zmenené heslá musia mať zmenené viac ako polovicu znakov oproti pôvodnému heslu
10. Zmenené heslo nesmie byť jedným z posledných 10 hesiel v histórii hesiel pre daný účet

**Heslá pre neprivilegované účty**

1. Dĺžka hesla musí byť aspoň 12 znakov
2. Heslá musia obsahovať
3. aspoň jedno veľké písmeno
4. aspoň jedno malé písmeno
5. aspoň jednu číslicu
6. aspoň jeden špeciálny znak
7. Zmena hesla
8. Heslá by mali byť menené aspoň raz za 6 mesiacov
9. Heslá musia byť zmenené aspoň raz za rok
10. Zmenené heslo nesmie byť jedným z posledných 5 hesiel v histórii hesiel pre daný účet
11. Heslo je možné zmeniť najviac raz za 1 deň.

**Príloha č. 6**

**k vyhláške č. xx/2019 Z. z.**

**Zariadenia pre nasadenie a zabezpečenie webového servera**

1. Je dostupných mnoho typov bezpečnostných zariadení, určených na zabezpečenie webových serverov. Vyššie uvedené bezpečnostné odporúčania možno do istej miery implementovať pomocou nich. Tieto zariadenia umocňujú účinok opatrení. Môžu zabrániť v prístupe útočníka k webovému serveru, čo je výhodné najmä počas doby odstraňovania novozisteného bezpečnostného nedostatku.
2. Medzi najznámejšie funkcie zariadení určených na zabezpečenie webového servera patria
   1. SSL akcelerátory – preberajú náročné výpočty potrebné na nadviazanie SSL/TLS spojení
   2. Bezpečnostné brány – monitorujú HTTP prevádzku v smere do a od webového servera, v prípade podozrenia na útok vykonajú opatrenia podľa potreby
   3. Content filtre – monitorujú prevádzku webového servera v oboch smeroch, po stránke obsahovej: v prípade zaznamenania citlivých či nevhodných dát podľa potreby vykonajú opatrenia
   4. Autentifikačné brány – rôznymi mechanizmami autentifikujú používateľov, riadia prístup k URL na webovom serveri
3. V mnohých prípadoch sú vyššie uvedené funkcie kombinované v jedinom zariadení, často označovanom ako reverzné proxy.
4. Na zjednodušenie a zvýšenie bezpečnosti už pri prvotnej inštalácií webového servera možno použiť niektoré spomedzi balíčkov, kombinujúcich hardenovaný operačný systém a webový server. Spravidla ide o zabezpečený univerzálny OS (Linux, Windows, ... ) prispôsobený na podporu bezpečne konfigurovaného webového servera (Apache, IIS, ... ). Podobné riešenia sa opierajú o
   1. Bezpečnú defaultnú konfiguráciu
   2. Hardenovaný OS/TOS
   3. Hardenovaný software webového servera
   4. Rozšírené možnosti auditu
   5. Aplikačné wrappery
   6. Sieťové wrappery a/alebo funkcia host-based firewallu
   7. Host-based IDS
   8. Zjednodušená administrácia bezpečnosti (napr. GUI či menu)
5. Webaplikačné firewally (WAF) sú špeciálnym typom firewallu, prispôsobeným na zabezpečenie webového servera. Ide o filter, plugin či zariadenie ktorý aplikuje set pravidiel na HTTP prevádzku. Všeobecne tieto pravidlá pokrývajú útoky ako XSS a SQL Injection. Prispôsobením potrebám aplikácie môže byť pomocou WAF množstvo útokov eliminovaných. WAF sa pôvodne zameriavali na monitorovanie prevádzky na aplikačnej vrstve, teda na úrovni HTTP protokolu. V súčasnosti sa funkcie tradičného WAF kombinujú s inými robustnými sieťovými technológiami, ako sú load balancing, sieťové firewally či aplikačné servery.
6. K bezpečnosti webových služieb môžu výrazne prispieť prvky použité na zabezpečenie externej infraštruktúry, ako firewally či IDS/IPS riešenia. Venuje sa im nasledujúca kapitola tohto dokumentu.
7. Nasadenie HW a SW zariadení na zvýšenie ochrany webového servera možno odporúčať. Konfigurácia zariadenia však musí zodpovedať požiadavkám na zabezpečenie konkrétneho servera a musí byť v súlade s opatreniami, uvedenými vyššie v tejto kapitole. Pri použití predpripravených balíčkov OS s webovým serverom je potrebné preveriť súlad východiskovej konfigurácie s popísanými požiadavkami a podľa potreby nastavenia upraviť. Kontrola továrenských nastavení a konfigurácia podľa definovaných požiadaviek je potrebná pri akomkoľvek spomínanom bezpečnostnom riešení.

Pozn. V tomto dokumente sa nevenujeme problematike tzv. web appliances, teda zariadení špeciálne určených iba na beh webového servera. Ide o zariadenia so zjednodušeným operačným systémom a s množinou služieb nutnou na beh webového servera. Optimalizovaný OS a minimum nadbytočných servisov, konfiguračných možností a jednoduchá správa z týchto zariadení robí riešenie vhodné pre malé až stredné aplikácie. Cieľom dokumentu je však poskytnúť komplexné odporúčania, vhodné i pre zložité, viacvrstvové modely webových aplikácií, pre ktorých funkciu jednoduché jednoúčelové zariadenie nepostačuje.

**Príloha č. 7**

**k vyhláške č. xx/2019 Z. z.**

**Špecifikácia rozsahu školenia na zvýšenie povedomia o informačnej bezpečnosti**

1. Školenia zamerané na zvýšenie bezpečnostného povedomia o rizikách, kybernetických útokoch a možnostiach ochrany pred nimi sú často krát jedinou formou obrany v prípadoch, kedy sú informačné systémy orgánu riadenia z technického hľadiska zabezpečené a prípadnému útočníkovi sa viac oplatí pokúsiť sa zneužiť zraniteľnosť v podobe neuvedomelého používateľa. Absolvovanie školení na zvýšenie povedomia o informačnej bezpečnosti má umožniť zamestnancom pri ich zorientovaní sa v oblasti informačnej bezpečnosti, naučiť ich odhaľovať potenciálny škodlivý kód, zvýšiť ich obozretnosť pri práci s Internetom a elektronickou poštou a zoznámiť ich s najzaujímavejšími kybernetickými incidentmi a ich príčinami.
2. Pre zamestnancov orgánu riadenia sú v rámci školenia účastníkom ozrejmené tieto oblasti:
3. dôvernosť, integrita a dostupnosť,
4. útoky sociálnym inžinierstvom,
5. bežné formy škodlivého softvéru,
6. časté chyby pri práci s informačnými a komunikačnými technológiami,
7. spôsoby zabezpečenia webových prehliadačov,
8. bezpečné používanie emailu,
9. bezpečné používanie sociálnych sietí,
10. používanie šifrovania,
11. riziká vzdialeného prístupu k IS,
12. zabezpečenie WiFi spolu s praktickou ukážkou,
13. bezpečné používanie mobilných zariadení,
14. bezpečné používanie Internet of Things,
15. organizačné aspekty bezpečnosti orgánu riadenia,
16. čo robiť v prípade vzniku bezpečnostného incidentu,
17. najzaujímavejšie incidenty v nedávnom období,
18. odporúčania na záver.
19. Pre zamestnancov orgánu riadenia podľa §5 ods. (3) a ods. (4) sú v rámci školenia vykonané aj tieto aktivity:
20. ukážka útoku pomocou RAT a ako sa voči nemu brániť,
21. vykonanie workshopu na odhaľovanie útokov sociálnym inžinierstvom a ochrany voči nim.
22. Pre zamestnancov orgánu riadenia podľa §5 ods. (4) sú v rámci školenia vykonané aj tieto aktivity:
23. ukážka ovládnutia firemnej siete pomocou škodlivého e-mailu a možnosti ochrany,
24. Pre zamestnancov orgánu riadenia v roli administrátora sú raz za tri roky v rámci školenia vykonané aj tieto aktivity:
25. ukážka praktického útoku na zraniteľnú webovú aplikáciu a možnosti ochrany,
26. proces riešenia kybernetického bezpečnostného incidentu.
27. Pre zamestnancov orgánu riadenia podľa §5 ods. (3) a ods. (4) v roli administrátora sú raz za tri roky v rámci školenia vykonané aj tieto aktivity:
28. zaisťovanie digitálnych stôp.
29. Pre zamestnancov orgánu riadenia podľa §5 ods. (4) sú raz za tri roky v rámci školenia vykonané aj tieto aktivity:
30. úvod do forenznej analýzy a threat huntingu,
31. bezpečná architektúra a defense in depth,
32. úvod do penetračného testovania,
33. statická analýza škodlivého softvéru.

**Príloha č. 8**

**k vyhláške č. xx/2019 Z. z.**

**Zoznam dokumentácie bezpečnosti ITVS**

Orgán vedenia pre potreby implementácie požiadaviek tejto vyhlášky vydá súbor materiálov, ktorý bude obsahovať šablóny a vzory dokumentácie bezpečnosti ITVS, návody, školiace materiály a ukážky. Materiály sú dostupné na webovom sídle Vládnej jednotky CSIRT obsahujú:

**Šablóny**

Bezpečnostná politika

- zoznam dokumentov na zaistenie informačnej bezpečnosti

- postupu pri revízii bezpečnostnej politiky

- určenie vlastníkov aktív

- určenie privilegovaných používateľských rolí v ITVS,

- určenie bezpečnostných požiadaviek na jednotlivé privilegované používateľské roly a

- určenie, ktoré používateľské roly nie je možné navzájom zlúčiť

Smernica pre bezpečné používanie ITVS

Smernica pre zálohovanie

Smernica pre personálnu bezpečnosť

- roly a zodpovednosti

- poučenie o právach, povinnostiach a riadiacich aktoch orgánu riadenia

- postup pre disciplinárne konanie

- postup pri ukončení pracovného pomeru

- program vzdelávania o informačnej bezpečnosti

- záznamy o absolvovaných školeniach na zvýšenie povedomia

Analýza rizík kritických procesov

Metodika analýzy rizík

Plány obnovy

Smernica o internej kontrole a audite informačnej bezpečnosti

Evidencia o všetkých miestach prepojenia sietí

- Interný akt riadenia prístupu medzi týmito sieťami

- Dokumentácia o sieti vrátane topológie siete

Pravidlá pre prácu v zabezpečenom priestore

Pravidlá pre:

1. údržbu, uchovávanie a evidenciu technických komponentov ITVS a zariadení ITVS,

2. používanie zariadení ITVS na iné účely, na aké boli pôvodne určené,

3. používanie zariadení ITVS mimo určených priestorov,

4. vymazávanie, vyraďovanie a likvidovanie zariadení ITVS a všetkých typov relevantných záloh,

5. prenos technických komponentov ITVS alebo zariadení ITVS mimo priestorov orgánu riadenia,

6. narábanie s elektronickými dokumentmi, dokumentáciou systému, pamäťovými médiami, vstupnými a výstupnými údajmi ITVS tak, aby sa zabránilo ich neoprávnenému zverejneniu, odstráneniu, poškodeniu alebo modifikácii,

Smernica na riešenie incidentov

- záznam o incidente

Smernica na riadenia prístupu

Zásady pre mobilné pripojenie do ITVS a pre prácu na diaľku

Smernica pre manažment zmien, riadenie zraniteľností, manažment záplat a riadenie kapacít

Záznamy o testovaní

Bezpečnostné požiadavky do zmluvy

Dokumentácia o ITVS:

- používateľská dokumentácia,

- administrátorská dokumentácia,

- prevádzková dokumentácia.

Zmluva na SW

Zmluva na prevádzku ITVS

SLA s dodávateľom

Smernica o šifrovaní

Smernica o riadení kontinuity činností

Program kontroly, auditu a testovania bezpečnosti ITVS

Záznamy z kontrol a preskúmania

Správa z auditu informačnej bezpečnosti

Správa z penetračného testovania

Správa z hodnotenia zraniteľností

Správa z testovania sociálnym inžinierstvom

Žiadosť o udelenie výnimky z opatrenia

**Návody a školenia**

Návod pre hardening

Návod pre antimalware riešenie

Návod pre host FW

Hodnotenie zraniteľností

Video školenia

- Školenia na zvýšenie povedomia - HOTOVO

- Ukážka útoku - HOTOVO

- Workshop social a Phishing

- šifrovanie

- keepass

**Príloha č. 9**

**k vyhláške č. xx/2019 Z. z.**

**Rozsah inventáru aktív zasielaného orgánu vedenia**

1. Zoznam IPv4 a IPv6 adries (rozsahov) dostupných zo siete Internet alebo Govnet využívaných orgánom riadenia a ich využitie.
2. Zoznam doménových mien registrovaných orgánom riadenia a ich využitie.
3. Zoznam služieb dostupných z verejných sietí a ich technický popis.
4. Zoznam používaných operačných systémov
5. Zoznam používaných aplikácií
6. Zoznam kontaktných osôb pre technické riešenie bezpečnostného incidentu a na komunikáciu s orgánom riadenia ohľadom bezpečnostného incidentu.

**Príloha č. 10**

**k vyhláške č. xx/2019 Z. z.**

**Obsah a štruktúra bezpečnostného projektu**

1. Orgán riadenia podľa §5 ods. (2), okrem prevádzkovateľa základnej služby podľa osobitného predpisu[[24]](#footnote-24), nie je povinný vypracovať bezpečnostný projekt.
2. Orgán riadenia podľa §5 ods. (3), okrem prevádzkovateľa základnej služby podľa osobitného predpisu24 vypracuje a udržiava v aktuálnom stave bezpečnostný projekt, ktorý obsahuje aspoň:
   1. inventár aktív podľa ustanovení Z1-A písm. c),
   2. popis implementovaných bezpečnostných opatrení,
   3. bezpečnostnú politiku a súvisiace interné predpisy vyplývajúce z ustanovení Z1,
   4. evidencia o všetkých miestach prepojenia sietí Z1-F písm. b).
3. Orgán riadenia podľa §5 ods. (4), okrem prevádzkovateľa základnej služby podľa osobitného predpisu24 vypracuje udržiava v aktuálnom stave bezpečnostný projekt, ktorý obsahuje aspoň:
   1. inventár aktív podľa ustanovení Z1-A písm. c),
   2. dokumentácia súvisiaca s manažmentom rizík podľa ustanovení Z2-C,
   3. popis implementovaných bezpečnostných opatrení,
   4. bezpečnostnú politiku a súvisiace interné predpisy vyplývajúce z ustanovení Z1 a Z2,
   5. evidencia o všetkých miestach prepojenia sietí Z1-F písm. b).
4. Orgán riadenia podľa §5 ods. (5) a prevádzkovateľ základnej služby podľa osobitného predpisu24 vypracuje bezpečnostný projekt, ktorý obsahuje aspoň:
   1. inventár aktív podľa ustanovení Z1-A písm. c),
   2. dokumentácia súvisiaca s manažmentom rizík podľa ustanovení Z2-C,
   3. popis implementovaných bezpečnostných opatrení,
   4. bezpečnostnú politiku a súvisiace interné predpisy vyplývajúce z ustanovení Z1, Z2 a Z3,
   5. havarijne plány,
   6. plány obnovy,
   7. evidencia o všetkých miestach prepojenia sietí Z1-F písm. b).
5. Orgán riadenia podľa §5 ods. (5) a prevádzkovateľ základnej služby podľa osobitného predpisu 24 pre tie ITVS, ktoré sú kategorizované ako C3, I3 alebo A3 vypracuje bezpečnostný projekt, ktorý okrem požiadaviek podľa ods. (4), obsahuje aj:
   1. dokumentácia súvisiaca s inventárom aktív podľa ustanovení špecifických opatrení č. 1.2,
   2. dokumentácia súvisiaca s manažmentom rizík podľa ustanovení špecifických opatrení č. 1.3,
   3. bezpečnostnú politiku, súvisiace interné predpisy a záznamy vyplývajúce z ustanovení špecifických opatrení č. 1.4 – 1.11 a č. 8.

**Príloha č. 11**

**k vyhláške č. xx/2019 Z. z.**

**Mapovanie klasifikačných stupňov**

Klasifikačné stupne v zmysle tejto vyhlášky sa na klasifikačné stupne v zmysle osobitného predpisu[[25]](#footnote-25) mapujú takto:

|  |  |
| --- | --- |
| **Táto vyhláška** | **Osobitný predpis25** |
| *Klasifikačné stupne z hľadiska dôvernosti:* | |
| C0 (verejné) | verejné |
| C1 (interné) | interné |
| C2 (chránené) | chránené |
| C3 (vysoko chránené) | prísne chránené |
| *Klasifikačné stupne z hľadiska integrity:* | |
| I0 (nepodstatná) | nízka |
| I1 (nízka) | nízka |
| I2 (stredná) | stredná |
| I3 (vysoká) | vysoká |
| *Klasifikačné stupne z hľadiska dostupnosti:* | |
| A0 (nepodstatná) | nízka |
| A1 (nízka) | nízka |
| A2 (stredná) | stredná |
| A3 (vysoká) | vysoká |

1. Vyhláška Národného bezpečnostného úradu č. 362/2018 Z. z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení [↑](#footnote-ref-1)
2. Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov. [↑](#footnote-ref-2)
3. informácia o aktuálnej minimálnej verzií je dostupná na stránke Vládnej jednotky CSIRT [↑](#footnote-ref-3)
4. Sú publikované na webovej stránke Vládnej jednotky CSIRT [↑](#footnote-ref-4)
5. V prípade, že je zdieľanie hesiel nutné (napr. administrátorské a servisné účty), musia byť bezpečne skladované prostredníctvom šifrovaných zdieľaných úložísk. Zdieľanie hesiel musí byť odôvodnené, dokumentované a musia byť stanovené osoby, ktoré majú k zdieľaným heslám prístup. [↑](#footnote-ref-5)
6. Funkcia audítora musí byť organizačne nezávislá od oblasti alebo činnosti, ktorá je predmetom auditu tak, aby umožnila jeho objektívne vykonanie a zamedzila takým vplyvom na audítora, ktoré by mohli ohroziť jeho integritu, objektivitu, profesionálny skepticizmus a úsudok. [↑](#footnote-ref-6)
7. Napr. knižnice a komponenty dodané tretími stranami; systémy, na ktorých bude riešenie postavené alebo ktoré bude využívať pri svojej prevádzke [↑](#footnote-ref-7)
8. Angl. „Version control system“, napr. git [↑](#footnote-ref-8)
9. Napr. stack protection, DEP, PIE, nonexecutable stack [↑](#footnote-ref-9)
10. Je možné použiť aj niektoré „Format-Preserving Encryption“ algoritmy [↑](#footnote-ref-10)
11. Napr. prihlasovacie údaje k databázam. [↑](#footnote-ref-11)
12. Je možné využiť napríklad bezplatný test od Qualys: https://www.ssllabs.com/ssltest/index.html [↑](#footnote-ref-12)
13. Konfiguráciu je možné získať napr. na https://cipherli.st/. [↑](#footnote-ref-13)
14. Iba procesy určené na správu webservera (nie procesy bežiacej webovej služby) by mali mať právo zapisovať do súborov s webovým obsahom. [↑](#footnote-ref-14)
15. Príklad pre konfiguráciu Apache: odstrániť Options FollowSymLinks [↑](#footnote-ref-15)
16. Funkcionalita zviazania zdrojovej IP adresy s reláciou je problematická ak k aplikácii pristupujú klienti, ktorých ISP dynamicky mení zdrojovú verejnú IP adresu. Taktiež môže byť problematická ak sa používa IPv6. [↑](#footnote-ref-16)
17. Pri používaní logrotate je potrebná dodatočná konfigurácia. [↑](#footnote-ref-17)
18. Ak to uvedená technológia umožňuje. [↑](#footnote-ref-18)
19. T.j. detekciu škodlivého kódu pri otváraní súborov a spúšťaní programov [↑](#footnote-ref-19)
20. Viď Príloha 5. [↑](#footnote-ref-20)
21. Kľúč registra HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\_NT\ CurrentVersion\Winlogon\CachedLogonsCount [↑](#footnote-ref-21)
22. Template SLA (časť informačná bezpečnosť) je dostupný na webstránkach https://www.csirt.sk. [↑](#footnote-ref-22)
23. Výnos Ministerstva financií Slovenskej republiky č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy. [↑](#footnote-ref-23)
24. Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov. [↑](#footnote-ref-24)
25. Vyhláška Národného bezpečnostného úradu č. 362/2018 Z. z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení [↑](#footnote-ref-25)