Metodika prevencie a pripravenosti organizácie pre systematické zabezpečenie informačnej bezpečnosti

Obsah

[1 Definícia významu kľúčových slov 2](#_Toc492813887)

[2 Účel dokumentu 4](#_Toc492813888)

[3 Spoločné postupy 5](#_Toc492813889)

[3.1 Zber údajov o infraštruktúre organizácie 5](#_Toc492813890)

[3.1.1 Úroveň organizácie 5](#_Toc492813891)

[3.1.2 Úroveň rezortu / sektora 8](#_Toc492813892)

[3.1.3 Národná úroveň 9](#_Toc492813893)

[3.2 Príprava technických spôsobilostí a komunikačných kanálov 9](#_Toc492813894)

[3.2.1 Úroveň organizácie 9](#_Toc492813895)

[3.2.2 Úroveň rezortu/sektora 10](#_Toc492813896)

[3.2.3 Národná úroveň 10](#_Toc492813897)

[3.2.4 Klasifikačná schéma bezpečnostných incidentov 11](#_Toc492813898)

[3.3 Riešenie bezpečnostných incidentov 13](#_Toc492813899)

[3.3.1 Riešenie bezpečnostných incidentov v rámci organizácie 13](#_Toc492813900)

[3.3.2 Koordinácia riešenia bezpečnostných incidentov na úrovni rezortu alebo sektora 14](#_Toc492813901)

[3.3.3 Koordinácie riešenia bezpečnostných incidentov na národnej úrovni. 15](#_Toc492813902)

[4 Bezpečnostné tímy 16](#_Toc492813903)

[Personálne zabezpečenie 17](#_Toc492813904)

[5 Tímy CSIRT 18](#_Toc492813905)

[Personálne zabezpečenie 23](#_Toc492813906)

[6 Bezpečnostné opatrenia 24](#_Toc492813907)

[7 Posúdenie bezpečnosti 26](#_Toc492813908)

[7.1 Analýza rizík 28](#_Toc492813909)

[**Úroveň organizácie** 28](#_Toc492813910)

[7.1.1 Identifikácia a ohodnotenie aktív 28](#_Toc492813911)

[7.1.2 Identifikácia a ohodnotenie hrozieb 28](#_Toc492813912)

[7.1.3 Identifikácia a ohodnotenie zraniteľností 29](#_Toc492813913)

[7.1.4 Výpočet rizika a vyhodnotenie rizík 29](#_Toc492813914)

[7.1.5 Rozhodnutie o správe rizík 29](#_Toc492813915)

[7.1.6 Návrh a implementácia opatrení 30](#_Toc492813916)

[7.1.7 Vyhodnotenie opatrení a preskúmavanie zvyškového rizika 30](#_Toc492813917)

[**Národná úroveň** 31](#_Toc492813918)

[7.2 Audit informačnej bezpečnosti 31](#_Toc492813919)

[**Úroveň organizácie** 31](#_Toc492813920)

[7.2.1 Príprava 31](#_Toc492813921)

[7.2.2 Audit prvého stupňa 32](#_Toc492813922)

[7.2.3 Plán auditu 32](#_Toc492813923)

[7.2.4 Auditný tím 33](#_Toc492813924)

[7.2.5 Audit druhého stupňa 33](#_Toc492813925)

[7.2.6 Správa z auditu 33](#_Toc492813926)

[**Úroveň rezortu** 34](#_Toc492813927)

[**Národná úroveň** 34](#_Toc492813928)

[7.3 Posúdenie zraniteľností 34](#_Toc492813929)

[**Úroveň organizácie** 34](#_Toc492813930)

[7.3.1 Príprava 34](#_Toc492813931)

[7.3.2 Vykonanie posúdenia zraniteľností 35](#_Toc492813932)

[7.3.3 Správa z posúdenia zraniteľností 35](#_Toc492813933)

[7.4 Penetračné testovanie 36](#_Toc492813934)

[**Úroveň organizácie** 36](#_Toc492813935)

[7.4.1 Externé penetračné testovanie 36](#_Toc492813936)

[7.4.2 Interné penetračné testovanie 38](#_Toc492813937)

# Definícia významu kľúčových slov

V tomto dokumente sú použité nasledujúce kľúčové slová podľa uvedeného významu:

„*musí*“ – špecifikuje mandatórnu požiadavku (platí aj pre „je nutné“)

„*nesmie*“ – špecifikuje mandatórny zákaz

„*malo by* [byť]” – špecifikuje požiadavku, ktorá je mandatórna pokiaľ neexistuje pádny dôvod prečo nemôže byť splnená. Ak existuje takýto dôvod, musí byť zdokumentovaný a schválený.

“*nemalo by* [byť]” - špecifikuje zákaz, ktorý je mandatórny pokiaľ neexistuje pádny dôvod prečo nie je možné ho splniť. Ak existuje takýto dôvod, musí byť zdokumentovaný a schválený.

“*odporúča sa*” – špecifikuje odporúčanú požiadavku (platí aj pre “je vhodné”)

Pre úlohy :

„povinná“ – špecifikuje povinnú úlohu

„odporúčaná“ –špecifikuje odporúčanú úlohu

Definície :

Národná autorita pre kybernetickú bezpečnosť – ÚOŠS poverený gesciou kybernetickej bezpečnosti

Rezortná / sektorová autorita – útvar ÚOŠS, ktorý je zodpovedný za kybernetickú bezpečnosť v danom rezorte / sektore kritickej infraštruktúry resp. sektore v zmysle pripravovaného zákona o KB.

Rezortný / sektorový tím CSIRT – útvar ÚOŠS, ktorý vykonáva úlohy CSIRT tímu v rámci rezortu /sektoru. Rezortný / sektorový tím CSIRT môže byť súčasťou rezortnej / sektorovej autority alebo útvar ÚOŠS alebo rozpočtovej organizácie, ktorý je poverený činnosťou rezortného / sektorového CSIRT tímu rezortnou / sektorovou autoritou.

Organizácie s vyššími požiadavkami na bezpečnosť – organizácie, ktoré sú ústrednými orgánmi štátnej správy, spracovávajú citlivé informácie, sú prvkami kritickej infraštruktúry, alebo z povahy svojej činnosti existuje vyššia pravdepodobnosť, že budú cieľom útoku)

Jedná sa minimálne o organizácie[[1]](#footnote-1) :

* ústredné orgány štátnej správy
* prevádzkovatelia prvkov kritickej infraštruktúry
* Kancelária NRSR, Kancelária prezidenta SR
* rozpočtové organizácie MF SR
* súdy, prokuratúra
* PZ SR
* Nases

Do zoznamu organizácií s vyššími požiadavkami na bezpečnosť je možné pridať ďalšie organizácie definované rezortnou / sektorovou autoritou na základe vecnej znalosti činností organizácií v danom rezorte/sektore.

Pre účely tohto dokumentu sa považujú termíny informačná bezpečnosť a kybernetická bezpečnosť za synonymá.

# Účel dokumentu

Cieľom dokumentu je v zmysle úlohy akčného plánu 3.3 Vytvoriť procesy a mechanizmy pri koordinácii zabezpečovania ochrany významných informačných aktív štátu na národnej úrovni je vypracovať metodiku prevencie a pripravenosti pre organizácie verejnej správy pre zabezpečenie z pohľadu informačnej bezpečnosti.

Tento dokument sa sústreďuje na zabezpečenie informačnej bezpečnosti z hľadiska odolnosti pred kybernetickými útokmi a naznačuje minimálne metodické rámce na zabezpečenie informačnej bezpečnosti na úrovni organizácie, úrovni rezortu/sektora a národnej úrovni.

Súčasne tento dokument obsahuje popis časti úloh, ktoré je potrebné splniť na zabezpečenie informačnej bezpečnosti na jednotlivých úrovniach a metodické usmernenia vo vybraných oblastiach.

Na systematické zvýšenie bezpečnosti organizácie je potrebné:

1. Organizačne, materiálne a personálne zabezpečiť riešenie informačnej bezpečnosti v organizácií vrátane zabezpečenia spôsobilostí riešenia bezpečnostných incidentov v rámci organizácie.
2. Implementovať štruktúry riadenia informačnej bezpečnosti na rezortnej, sektorovej a národnej úrovni .
3. Implementovať systému riadenia informačnej bezpečnosti v organizácií (vrátane analýzy bezpečnostných rizík) a implementáciu bezpečnostných opatrení za účelom vytvorenia bezpečnostného baseline v organizácií.
4. Pravidelné vykonávať kontrolné činnosti (audity bezpečnosti vrátane penetračných testov)

Vzhľadom na štruktúru Internetu, typy a rozsahy hrozieb a potrebné odborné spôsobilosti na ich zvládanie je potom na národnej / vládnej úrovni ďalej potrebné:

1. Vytvoriť spôsobilostí poslednej inštancie na národnej a vládnej úrovni
2. Vytvoriť spôsobilostí na analytické a proaktívne činnosti
3. Vydávať štandardy v oblasti informačnej bezpečnosti pre organizácie VS a pravidelne ich aktualizovať.
4. Vydávať postupy na bezpečnú konfiguráciu jednotlivých technológií (tzv. hardening guidov)
5. Školiť zamestnancov – špecialistov v oblasti informačnej bezpečnosti
6. Zvyšovať povedomie všetkých zamestnancov organizácií

V tomto dokumente sú ďalej podrobnejšie rozobraté ako nutná súčasť riešenia informačnej bezpečnosti v SR:

* Predpoklady pre riešenie bezpečnostných incidentov
* Riešenie a koordinácia riešenia bezpečnostných incidentov na úrovni organizácie / rezortu /sektora a národnej úrovni
* Tvorba bezpečnostných[[2]](#footnote-2) a CSIRT[[3]](#footnote-3) tímov, požiadavky na bezpečnostné a CSIRT tímy na úrovni organizácie, rezortu/sektora a národnej úrovni
* Požiadavky na zabezpečenie infraštruktúry organizácie ako nutný predpoklad pre zabezpečenie organizácie pred kybernetickými útokmi.
* Základná úroveň overovania úrovne informačnej bezpečnosti v organizáciách ako nutný predpoklad pre zabezpečenie a udržanie úrovne informačnej bezpečnosti v organizácií.

Rozpracované časti sú minimálnou množinou[[4]](#footnote-4) oblastí potrebných na zabezpečenie organizácie / rezortu / sektora a národného kybernetického priestoru z pohľadu informačnej bezpečnosti pred kybernetickými útokmi.

# Spoločné postupy

V rámci riešenia incidentov na národnej úrovni je potrebné rozdeliť riešenie incidentov na tieto časti:

* Príprava na riešenie bezpečnostných incidentov
* Riešenie bezpečnostných incidentov v rámci organizácie
* Koordinácia riešenia bezpečnostných incidentov na úrovni rezortu alebo sektora
* Koordinácie riešenia bezpečnostných incidentov na národnej úrovni.

Príprava na riešenie bezpečnostných incidentov z hľadiska organizácie obsahuje minimálne nasledujúce kroky :

* zber údajov o infraštruktúre
* príprava technických spôsobilostí a komunikačných kanálov
* implementácia detekčných mechanizmov v rámci organizácie
* návrh a implementácia procesu riešenia bezpečnostných incidentov

## Zber údajov o infraštruktúre organizácie

Aby bolo, možné riešiť bezpečnostné incidenty v rámci organizácie, sektora / rezortu, alebo národnej úrovni je potrebné získať komplexné informácie o poskytovaných elektronických službách v zmysle zákona o E-Governmente, ale aj o poskytovaných službách v zmysle technicky dostupných sieťových služieb z externých sietí ako napríklad Internet, FINET, Govnet. Tieto informácie potom môžu byť použité na zaistenie bezpečnosti organizácie prostredníctvom identifikácie zraniteľných verzií a ich následnej oprave (úprava konfigurácie, aktualizovanie na aktuálnu podporovanú verziu prípadne aplikáciu hotfixu).

Na národnej sektorovej/ rezortnej úrovni je možne tieto podklady využiť pri riadení rizík, detekcií zraniteľných služieb a koordináciu riešenia bezpečnostných incidentov.

V strednodobom horizonte je potom predpoklad vytvorenia komplexných konfiguračných databáz na úrovni organizácií, úrovni rezortu/sektora a na národnej úrovni.

### Úroveň organizácie

Organizácia musí mať k dispozícií aktuálne (a pravidelne aktualizované) údaje o verejne dostupných službách, použitých technológiách, pridelených verejných IP adresách ako aj spravovaných resp. vlastnených domén. Tieto informácie sú potrebné na riešenie bezpečnostných incidentov ako aj pre overenie, či sa bezpečnostný incident stal v infraštruktúre organizácie alebo sa jedná o bezpečnostný incident v inej organizácií alebo infraštruktúre. Rovnako tieto informácie je potrebné, zbierať, vyhodnocovať sa ukladať na úrovni organizácie, rezortu a národnej úrovni. Tieto informácie môžu byť použité na proaktívnu detekciu zraniteľností v používaných technológiách a je možné zaslať dotknutým subjektom varovanie o zraniteľnostiach v ich používaných technológiách.

Pre riešenie bezpečnostných incidentov je potrebné zozbierať minimálne nasledujúce typy dát :

* IP adresné rozsahy (verejné IP adresy)
* Zoznam verejne dostupných služieb
  + IP adresy / domény
  + URL
  + sieťové porty
  + popis dostupných služieb
  + dôležitosť dostupných služieb na stupnici od 0-3 z hľadiska dôvernosti
    - 0 - nedôležitá služba
    - 3 - kritická služba pre funkčnosť inštitúcie alebo vykonávané činnosti
  + dôležitosť dostupných služieb na stupnici od 0-3 z hľadiska integrity
    - 0 - nedôležitá služba
    - 3 - kritická služba pre funkčnosť inštitúcie alebo vykonávané činnosti
  + dôležitosť dostupných služieb na stupnici od 0-3 z hľadiska dostupnosti
    - 0 - nedôležitá služba
    - 3 - kritická služba pre funkčnosť inštitúcie alebo vykonávané činnosti
  + dôležitosť dostupných služieb na stupnici od 0-3 z hľadiska legislatívy (osobné údaje)
    - 0 - nedôležitá služba
    - 3 - kritická služba pre funkčnosť inštitúcie alebo vykonávané činnosti
* Zoznam používaných technológií[[5]](#footnote-5)
  + OS
  + Aplikačné vybavenie
  + Používané platformy
* Kontaktné osoby pre riešenie bezpečnostných incidentov
  + Primárny kontakt pre nahlasovanie bezpečnostných incidentov
  + Sekundárny kontakt pre prípad nedostupnosti primárneho kontaktu
  + Kontakt na osobu s riadiacimi právomocami pre eskaláciu bezpečnostného incidentu resp. koordináciu riešenia rozsiahleho bezpečnostného incidentu.
* Kontaktné osoby pre zasielanie varovaní, informácií o stave kybernetickej bezpečnosti v sektore a ďalšie informácie v oblasti kybernetickej bezpečnosti

Kontaktné osoby musia byť zvolené nasledovne :

* Primárny kontakt
  + musí mať IT znalosti minimálne v rozsahu znalostného štandardu vypracovaného pre vedúcich pracovníkov v oblasti informačnej bezpečnosti[[6]](#footnote-6)
  + musí byť interným zamestnancom organizácie
  + odporúča sa, aby sa jednalo o správcu IKT v organizácií alebo zamestnanca IT oddelenia
* Sekundárny kontakt
  + odporúča sa aby mal IT znalosti minimálne v rozsahu znalostného štandardu vypracovaného pre vedúcich pracovníkov v oblasti informačnej bezpečnosti[[7]](#footnote-7)
  + mal by byť interným zamestnancom organizácie
  + odporúča sa, aby sa jednalo o správcu IKT v organizácií alebo zamestnanca IT oddelenia
* Osoba s riadiacimi právomocami pre eskaláciu bezpečnostného incidentu resp. koordináciu riešenia rozsiahleho bezpečnostného incidentu.
  + odporúča sa aby mal IT znalosti minimálne v rozsahu znalostného štandardu vypracovaného pre vedúcich pracovníkov v oblasti informačnej bezpečnosti[[8]](#footnote-8)
  + musí byť interným zamestnancom organizácie
  + musí mať právomoc v prípade potreby vypnúť / zablokovať / vykonať zmenu / obmedziť prevádzku služieb poskytovaných prostredníctvom externých sietí.
  + mal by mať právomoc poskytnúť kompletný prístup k dotknutej časti IKT organizácie rezortnému / sektorovému CSIRT tímu

V rámci kontaktných údajov pre každú kontaktnú osobu musí byť uvedené :

* Meno, Priezvisko a funkcia kontaktnej osoby
* Rola kontaktnej osoby (primárny, sekundárny kontakt alebo koordinačný kontakt)
* Email kontaktnej osoby
* Telefónne číslo kontaktnej osoby
* Telefónne číslo na mobilný telefón kontaktnej osoby

Všetky uvedené informácie musia byť pravidelne aktualizované. V rámci organizácie je nutné identifikovať funkciu a zodpovednú osobu, ktorá bude zodpovedať za aktualizáciu týchto údajov a ich nahlasovanie. Údaje musia byť aktualizované vždy pri ich zmene, **minimálne** však **raz ročne**.

Údaje vo formáte (viď príloha UDAJE1) musia byť nahlásené prostredníctvom šifrovaného emailu na kontaktné miesta na úrovni sektora a národnej úrovni.

**Úlohy** (všetky organizácie verejnej správy a prvky kritickej infraštruktúry)

* Názov úlohy : Zozbierať údaje v rozsahu prílohy UDAJE 1 a zaslať ich rezortnému / sektorovému kontaktnému bodu do 31.1. roku alebo do 30 dní po významnej zmene prostredníctvom listu alebo zašifrovaným emailom
  + Periodicita plnenia : ročne do 31.1. alebo do 30 dní po významnej zmene
  + Typ úlohy : povinná
* Názov úlohy : Skenovať verejné IP rozsahy organizácie prostredníctvom nástroja typu port scanner[[9]](#footnote-9) s detekciou verzií sieťových služieb, vyhodnotiť informácie o otvorených sieťových portoch a vypnúť služby, ktoré sú nepotrebné pre chod organizácie. Informáciu o dostupných službách zaslať rezortnému / sektorovému kontaktnému bodu do 31.1. roku prostredníctvom listu alebo zašifrovaným emailom
  + Periodicita plnenia : ročne do 31.1.
  + Typ úlohy : povinná
* Názov úlohy : Vytvoriť komplexnú konfiguračnú databázu pre informačné aktíva
  + Periodicita plnenia : jednorázovo
  + Typ úlohy : povinná
* Názov úlohy : Udržiavať konfiguračnú databázu aktuálnu
  + Periodicita plnenia : priebežne
  + Typ úlohy : povinná

### Úroveň rezortu / sektora

Rezortný / sektorový útvar musí mať k dispozícií informácie o používaných technológiách a kontaktné údaje zo všetkých organizácií vo svojej pôsobnosti a musí pravidelne (minimálne však raz ročne ) overiť platnosť všetkých kontaktných údajov.

Rezortná / sektorová autorita musí v zodpovedajúcom rezorte / sektore vytvoriť kontaktné miesto a identifikovať kontakty na ktoré je možné nahlasovať bezpečnostné incidenty a koordinovať riešenie rozsiahlych bezpečnostných incidentov. Toto kontaktné miesto je určené pre všetky organizácie v danom sektore/ rezorte. Kontaktné miesto je potrebné organizáciám nahlásiť listom a publikovať na webovej stránke organizácie, ktorá plní úlohu rezortnej / sektorovej autority.

Kontaktné miesto (KM) musí minimálne obsahovať :

* Emailovú adresu v generickom tvare (napríklad [incident@csirt.gov.sk](mailto:incident@csirt.gov.sk))
* Telefónne číslo na kontaktovanie v pracovných hodinách
* Telefónne číslo na kontaktovanie v mimo pracovných hodinách pre prípad núdze.
* URL na ktorej je webový portál rezortnej/sektorovej autority a CSIRT tímu

Kontaktné miesto by malo ďalej obsahovať :

* Verejný PGP kľúč, ktorým je možné šifrovať správy pre rezortnú / sektorovú autoritu

Kontakty by musia viesť na osoby s dostatočnými technickými znalosťami aby bolo možné riešiť bezpečnostné incidenty. Kontakty by mali byť presmerované na rezortný / sektorový CSIRT tím.

**Úlohy** (rezortné / sektorové autority)

* Názov úlohy : Vytvoriť kontaktné miesto na nahlasovanie bezpečnostných incidentov, zabezpečiť dostupnosť kontaktov , publikovať informácie o kontaktoch na webovej stránke organizácie.
  + Periodicita : neodkladne
  + Typ úlohy : povinná
* Názov úlohy : Nahlásiť národnej autorite kontaktné údaje kontaktného miesta
  + Periodicita : neodkladne
  + Typ úlohy : povinná
* Názov úlohy : Viesť evidenciu kontaktov na úrovni rezortu / sektora v rozsahu poskytovaných k údajov organizáciami.
  + Periodicita plnenia : priebežne
  + Typ úlohy : povinná
* Názov úlohy : Overiť a vyhodnotiť získané informácie od organizácií v rezorte / sektore, identifikovať na základe zozbieraných informácií zraniteľné verzie a informovať dotknuté organizácie o zistených zraniteľnostiach.
  + Periodicita plnenia : neodkladne po získaní dát od organizácií, najneskôr však do 30 dní
  + Typ úlohy : povinná
* Názov úlohy : Zozbierané kontaktné údaje zaslať národnej autorite najneskôr do 30 dní od ich získania.
  + Periodicita plnenia: priebežne
  + Typ úlohy : povinná

### Národná úroveň

Na národnej úrovni musia byť k dispozícii kontaktné údaje všetkých organizácií na území SR. Národná autorita musí pravidelne (minimálne však raz ročne) overiť platnosť všetkých kontaktných údajov rezortných / sektorových autorít.

Národná autorita musí na národnej úrovni vytvoriť kontaktné miesto a identifikovať kontakty na ktoré je možné nahlasovať bezpečnostné incidenty a koordinovať riešenie rozsiahlych bezpečnostných incidentov. Toto kontaktné miesto je určené pre všetky rezortné/sektorové autority. Kontaktné miesto je potrebné rezortným/sektorovým autoritám nahlásiť listom a publikovať na webovej stránke organizácie, ktorá plní úlohu národnej autority.

Kontaktné miesto musí minimálne obsahovať :

* Emailovú adresu v generickom tvare (napríklad [incident@csirt.gov.sk](mailto:incident@csirt.gov.sk))
* Telefónne číslo na kontaktovanie v pracovných hodinách
* Telefónne číslo na kontaktovanie v mimo pracovných hodinách pre prípad núdze.

Kontaktné miesto by malo ďalej obsahovať :

* Verejný PGP kľúč, ktorým je možné šifrovať správy pre rezortnú / sektorovú autoritu
* Kontakty musia viesť na osoby s dostatočnými technickými znalosťami aby bolo možné riešiť bezpečnostné incidenty. Kontakty by mali byť presmerované na vládny CSIRT tím.

## Príprava technických spôsobilostí a komunikačných kanálov

### Úroveň organizácie

Efektívne riešenie bezpečnostných incidentov v organizácií vyžaduje vybudovanie technických spôsobilostí v organizácií (viď budovanie bezpečnostného tímu resp. tímu CSIRT). Okrem vybudovania technických spôsobilostí by mala organizácia zabezpečiť :

* Schopnosť odosielať a prijímať šifrované maily
* Komunikačné kanály na komunikáciu s organizáciou.
* Eskalačné a koordinačné postupy v prípade rozsiahleho bezpečnostného incidentu.

Organizácia by mala byť spôsobilá prijímať a posielať zašifrované emaily. Rezortná/sektorová autorita musí byť spôsobilá prijímať a posielať zašifrované emaily. Toto je potrebné pre nahlasovanie incidentov, riešenie bezpečnostných incidentov ako aj koordináciu riešenia bezpečnostných incidentov. Odporúča sa používať šifrovanie emailov prostredníctvom technológie PGP resp. GPG.

Organizácia musí podporovať minimálne nasledujúce komunikačné kanály pre nahlasovanie bezpečnostných incidentov, riešenie bezpečnostných incidentov a koordináciu riešenia bezpečnostných incidentov:

* Email
* Telefón (so spôsobilosťou prijímať SMS správy)

Organizácia by ďalej mala podporovať nasledujúce komunikačné kanály pre nahlasovanie bezpečnostných incidentov, riešenie bezpečnostných incidentov a koordináciu riešenia bezpečnostných incidentov:

* Šifrovaný email
* Kanály definované systémom včasného varovania v zmysle úlohy 3.4 Akčného plánu ku koncepcií KB

### Úroveň rezortu/sektora

Rezortné / sektorové autority musia mať technické spôsobilosti potrebné na riešenie bezpečnostných incidentov vo svojej pôsobnosti, základnú úroveň reaktívnych činnosti, a spôsobilosti na posudzovanie bezpečnostných zraniteľností, poskytovať služby poslednej inštancie pre rezort / sektor ,vydávanie technických odporúčaní a posudzovanie a úpravu technických štandardov pre rezort/sektor.

Rezortné / sektorové autority a organizácie so zvýšenými požiadavkami na bezpečnosť musia mať prostredníctvom bezpečnostných tímov spôsobilosti na proaktívne zabezpečenie prevádzkovanej infraštruktúry minimálne v rozsahu :

* Vytvorenie a udržiavanie konfiguračnej databázy spravovanej infraštruktúry
* Hardening systémov na základe odporúčaní rezortnej/sektorovej alebo národnej autority
* Monitoring infraštruktúry
* Automatizované ohodnotenie zraniteľností na základe verzie a konfigurácie software.

### Národná úroveň

Národná autorita musí mať technické spôsobilosti potrebné na riešenie bezpečnostných incidentov na národnej úrovni, obranu voči pokročilým kybernetickým útokom, poskytovať služby poslednej inštancie na národnej úrovni, spôsobilosti na posudzovanie a analýzu bezpečnostných hrozieb a tvorbu bezpečnostných štandardov pre infraštruktúry verejnej správy.

Jedná sa najmä o :

* Počítačovú forenznú analýzu
* Analýzu malware
* Penetračné testy
* Koreláciu a vyhodnocovanie údajov z rôznych organizácií
* Technologický dozor (Identifikácia zraniteľností v používaných technológiách)
* analýza incidentov,
* analýza bezpečnostných rizík a zraniteľností
* služby detekcie prienikov
* monitorovanie stavu hrozieb v oblasti IKT
* konzultačná činnosť v oblasti informačnej bezpečnosti

### Klasifikačná schéma bezpečnostných incidentov

Národná autorita musí definovať klasifikačnú schému bezpečnostných incidentov, ktorá sa bude používať na klasifikáciu detegovaných bezpečnostných incidentov. Táto klasifikačná schéma by mala byť kompatibilná s klasifikačnou schémou navrhnutou agentúrou ENISA pre zabezpečenie kompatibility klasifikačnej schémy na medzinárodnej úrovni. Príkladom takejto klasifikácie je klasifikačná schéma CSIRT.SK uvedená na webovom portáli : <http://www.csirt.gov.sk/napoveda-pre-typ-incidentu-7eb.html>.

Rezortné / sektorové autority by mali prebrať klasifikačnú schému pre klasifikáciu bezpečnostných incidentov a rozšíriť ju o špecifické bezpečnostné incidenty v sektore / rezorte a publikovať ju na svojej webovej stránke. Rezortné / sektorové autority musia definovať podmienky (na základe špecifikácie od národnej autority), pre nahlasovanie bezpečnostných incidentov organizácií rezortnej /sektorovej autorite.

Organizácie musia prebrať klasifikačnú schému pre klasifikáciu bezpečnostných incidentov od svojej rezortnej/sektorovej autority. Organizácie musia nahlasovať bezpečnostné incidenty svojej rezortnej / sektorovej autorite prostredníctvom definovaného kontaktného miesta. Rozsah a typ nahlasovaných bezpečnostných incidentov musí spĺňať požiadavky definované rezortnou / sektorovou autoritou.

**Úlohy** (všetky organizácie verejnej správy a prvky kritickej infraštruktúry, rezortné/sektorové autority, národná autorita)

* Názov úlohy : Implementovať systém šifrovania emailov prostredníctvom PGP resp. GPG a zaslanie verejných kľúčov sektorovému / rezortnému útvaru
  + Periodicita plnenia : jednorázovo
  + Typ úlohy : odporúčaná (pre sektorové/ rezortné autority povinná)
* Názov úlohy : Definovať jednotné kontaktné miesto v rámci organizácie, na ktoré budú nahlasované bezpečnostné incidenty z vnútra organizácie aj mimo organizácie. Zverejnenie kontaktných údajov tohto kontaktného miesta pre zamestnancov organizácie a zaslanie kontaktných údajov rezortnému / sektorovému útvaru
  + Periodicita plnenia : jednorázovo
  + Typ úlohy : povinná
* Názov úlohy : Prebrať klasifikačnú schému od rezortnej/ sektorovej autority a implementovať proces riešenia bezpečnostných incidentov zahŕňajúci túto klasifikačnú schému
  + Periodicita plnenia : jednorázovo
  + Typ úlohy : povinná

**Úlohy** (rezortné/sektorové autority)

* Názov úlohy : Vytvoriť rezortný/ sektorový CSIRT tím s nasledujúcimi spôsobilosťami:
  + - Riešenie a analýza bezpečnostných incidentov v rezorte/sektore
    - Základná úroveň reaktívnych činností (analýza incidentov, analýza škodlivého kódu, zaistenie digitálnych stôp, )
    - Poskytovanie služieb CSIRTu poslednej inštancie pre rezort / sektor
    - Základná analýza bezpečnostných zraniteľností a návrh bezpečnostných opatrení
    - Vydávanie a úprava technických štandardov vydaných národnou autoritou
  + Periodicita plnenia : jednorázovo
  + Typ úlohy : povinná (pre sektorové / rezortné autority)
* Názov úlohy : Vytvoriť klasifikačnú schému na rezortnej / sektorovej úrovni a publikovať ho na webovej stránke. (Mal by byť založený na systéme publikovanom rezortnou autoritou)
  + Periodicita plnenia : jednorázovo
  + Typ úlohy : povinná
* Názov úlohy : Definovať rozsah, typ a spôsob nahlasovania bezpečnostných incidentov sektorovému / rezortnému CSIRT tímu.
  + Periodicita plnenie : jednorázovo
  + Typ úlohy : povinná

**Úlohy** (rezortné/sektorové autority, organizácie so zvýšenými požiadavkami na bezpečnosť)

* Názov úlohy : Vytvoriť a udržiavať konfiguračnú databázu spravovanej infraštruktúry
  + Periodicita plnenie : priebežne
  + Typ úlohy : povinná
* Názov úlohy : Vytvoriť bezpečnostný tím s nasledujúcimi spôsobilosťami :
  + - Hardening technológií používaných v rezorte/ sektore/ organizácií
    - Bezpečnostný monitoring infraštruktúry
    - Udržiavanie a konfigurácia bezpečnostných technológií
    - Ohodnotenie zraniteľností na základe verzie a konfigurácie
  + Periodicita plnenie : jednorázovo
  + Typ úlohy : povinná
* Názov úlohy : Vykonať hardening celej infraštruktúry na základe definovanej úrovne národnou/rezortnou/sektorovou autoritou, viesť evidenciu implementovaných opatrení
  + Periodicita plnenie : priebežne
  + Typ úlohy : povinná

**Úlohy** (národná autorita)

* Názov úlohy : Vytvoriť vládny CSIRT tím s nasledujúcimi technickými spôsobilosťami
  + - Riešenie bezpečnostných incidentov
    - Počítačovú forenznú analýzu
    - Analýzu malware
    - Penetračné testy
    - Koreláciu a vyhodnocovanie údajov z rôznych organizácií
    - Technologický dozor (Identifikácia zraniteľností v používaných technológiách)
    - analýza incidentov,
    - analýza bezpečnostných rizík a zraniteľností
    - služby detekcie prienikov
    - monitorovanie stavu hrozieb v oblasti IKT
    - konzultačná činnosť v oblasti informačnej bezpečnosti
  + Periodicita plnenie : jednorázovo
  + Typ úlohy : povinná
* Názov úlohy : Vytvoriť klasifikačnú schému pre ohodnotenie bezpečnostných incidentov. (Odporúča sa, aby bola kompatibilná s klasifikačnou schémou ENISA)
  + Periodicita plnenie : jednorázovo
  + Typ úlohy : povinná
* Názov úlohy : Definovať rozsah, typ a spôsob nahlasovania bezpečnostných incidentov vládnemu CSIRT tímu.
  + Periodicita plnenie : jednorázovo
  + Typ úlohy : povinná
* Názov úlohy : Definovať základné požiadavky na hardening technológií
  + Periodicita plnenie : jednorázovo
  + Typ úlohy : povinná

## Riešenie bezpečnostných incidentov

### Riešenie bezpečnostných incidentov v rámci organizácie

V rámci organizácie prebieha riešenie bezpečnostných incidentov na základe povinností vyplývajúcich z legislatívnych povinností , nariadení rezortného/ sektorového útvaru a usmernení publikovaných národnou autoritou pre kybernetickú bezpečnosť.

Odporúča sa, aby každá organizácia by mala mať implementovaný proces riešenia bezpečnostných incidentov. Organizácie s vyššími požiadavkami na bezpečnosť, rezortné/sektorové autority a národná autorita musia mať implementovaný proces riešenia bezpečnostných incidentov.

Proces riešenia bezpečnostného incidentu v rámci organizácie sa skladá zo 4 fáz:

* Detekcia bezpečnostného incidentu
* Ohodnotenie a klasifikácia bezpečnostného incidentu
* Vyriešenie bezpečnostného incidentu
* Vykonanie systémových opatrení na zabránenie opakovania bezpečnostného incidentu

Proces riešenia bezpečnostných incidentov v organizácií musí zahŕňať :

* Spôsob detekcie bezpečnostných incidentov, pričom jeden z podporovaných spôsobov musí byť nahlásenie bezpečnostných incidentov na primárny alebo sekundárny kontakt.
* Klasifikáciu bezpečnostných incidentov na základe klasifikačnej schémy definovanej a publikovanej sektorovou / rezortnou autoritou.
* Štandardné postupy riešenia jednotlivých typov incidentov. Tieto postupy môžu byť definované rezortnou/sektorovou autoritou, alebo v prípade, že nie sú sa jedná o postupy definované organizáciou.
* Eskalačné postupy uvedené nižšie.
* Zaistenie a uchovanie digitálnych stôp. Digitálne stopy musia byť zaistené na základe postupov definovaných sektorovou / rezortnou autoritou a stopy musia byť zaistené tak, aby nedošlo k ich zmene resp. bolo možné takúto zmenu detegovať.
* Vedenie evidencie o bezpečnostných incidentoch podľa špecifikácie rezortnej/sektorovej autority.

V prípade, že organizácia nemá dostatočné spôsobilosti na vyriešenie prebiehajúceho bezpečnostného incidentu, požiada o pomoc rezortný/sektorový útvar. Sektorový/rezortný útvar následne zabezpečí pomoc organizácií prostredníctvom rezortného/sektorového tímu CSIRT. Rezortný/ sektorový CSIRT je povinný spustiť riešenie bezpečnostného incidentu bezodkladne najneskôr však do 24 hodín. Organizácia kontaktuje rezortný / sektorový tím CSIRT prostredníctvom kontaktu publikovaného na webovej stránke

Rezortný /sektorový tím by mal byť kontaktovaný prostredníctvom definovaných kontaktných úda

V prípade, že sektorový/rezortný CSIRT tím nie je schopný vyriešiť prebiehajúci bezpečnostný incident požiada o pomoc vládny a CSIRT tím. Vládny CSIRT je povinný riešenie bezpečnostného incidentu bezodkladne najneskôr však do 24 hodín.

**Úlohy** (organizácie verejnej správy)

* Názov úlohy : Implementovať proces riešenia bezpečnostných incidentov podľa definovaných požiadaviek
  + Periodicita plnenie : jednorázovo
  + Typ úlohy : odporúčaná
* Názov úlohy : Nahlasovať bezpečnostné incidenty sektorovej / rezortnej autorite v definovanom rozsahu definovaným spôsobom
  + Periodicita plnenia : neodkladne po detekcií / nahlásení bezpečnostného incidentu
  + Typ úlohy : povinná

**Úlohy** (rezortné/sektorové autority, organizácie so zvýšenými požiadavkami na bezpečnosť)

* Názov úlohy : Implementovať proces riešenia bezpečnostných incidentov podľa definovaných požiadaviek
  + Periodicita plnenie : jednorázovo
  + Typ úlohy : povinná

**Úlohy** (rezortné/sektorové autority)

* Názov úlohy: Špecifikovať štandardné postupy riešenia bezpečnostných incidentov
  + Periodicita plnenie : jednorázovo
  + Typ úlohy : odporúčaná
* Názov úlohy : Nahlasovať bezpečnostné incidenty národnej autorite v definovanom rozsahu definovaným spôsobom
  + Periodicita plnenia : neodkladne po detekcií / nahlásení bezpečnostného incidentu
  + Typ úlohy : povinná

### Koordinácia riešenia bezpečnostných incidentov na úrovni rezortu alebo sektora

Rezortný / sektorový CSIRT tím koordinuje bezpečnostné incidenty na úrovni rezortu / alebo sektoru. V prípade, že rezortný / sektorový CSIRT identifikuje bezpečnostný incident (alebo hrozbu) a vyhodnotí, že sa jedná o závažný bezpečnostný incident, ktorý ohrozuje viacero organizácií rezortu alebo sektora, zabezpečí koordináciu riešenia bezpečnostného incidentu. V rámci koordinácie rezortný / sektorový CSIRT zabezpečuje

* Eskalačné procesy s vládnym CSIRT tímom
* Bezpečnú výmenu informácií medzi všetkými účastníkmi, ktorí sú zapojení do riešenia bezpečnostného incidentu
* Technickú podporu pri riešení bezpečnostných incidentov
* Analytické činnosti v súvislosti s riešeným bezpečnostným incidentov
* Udržuje aktuálnu situačnú mapu v zmysle aktuálneho stavu bezpečnostného incidentu
* V spolupráci s bezpečnostnými tímami organizácií identifikuje a realizuje potrebné preventívne alebo reaktívne bezpečnostné opatrenia

Riešenie bezpečnostných incidentov na rezortnej / sektorovej úrovni zabezpečuje z technického pohľadu rezortný / sektorový tím CSIRT.

Dotknuté organizácie rezortu/sektora musia zabezpečiť :

* Požadovanú súčinnosť pri riešení bezpečnostného incidentu alebo jeho predchádzaní v rozsahu adekvátnom pre danú organizáciu.
* Implementáciu požadovaných bezpečnostných opatrení schválených príslušnou rezortnou / sektorovou autoritou.

### Koordinácie riešenia bezpečnostných incidentov na národnej úrovni.

Koordinácia riešenie bezpečnostných incidentov národnej úrovni je znázornená na obrázku č. 1. V prípade, že niektorý sektorový / rezortný alebo vládny CSIRT tím (reprezentovaný národným kontaktným miestom) vyhodnotia, že sa jedná o bezpečnostný incident, ktorý zahŕňa viacero sektorov / rezortov, alebo sa jedná o mimoriadne závažný bezpečnostný incident, koordináciu riešenia tohto bezpečnostného incidentu preberie vládny tím CSIRT. V rámci koordinácie vládny CSIRT zabezpečuje :

* Eskalačné procesy s národnou autoritou pre kybernetickú bezpečnosť
* Bezpečnú výmenu informácií medzi všetkými účastníkmi, ktorí sú zapojení do riešenia bezpečnostného incidentu
* Technickú podporu pri riešení bezpečnostných incidentov
* Analytické činnosti v súvislosti s riešeným bezpečnostným incidentov
* Udržuje aktuálnu situačnú mapu v zmysle aktuálneho stavu bezpečnostného incidentu
* V spolupráci s rezortnými / sektorovými CSIRT tímami identifikuje a realizuje potrebné preventívne alebo reaktívne bezpečnostné opatrenia
* V prípade, že sa jedná o bezpečnostný incident, ktorý ohrozuje bezpečnosť SR informuje určený orgán pre bezpečnosť sietí a informačných systémov (resp. garanta kybernetickej bezpečnosti), ktorý spustí procesy pre krízové riadenie rozsiahlych bezpečnostných udalostí.

Riešenie bezpečnostných incidentov na národnej úrovni zabezpečuje z technického pohľadu vládny tím CSIRT.

Rezortné / sektorové CSIRT tímy (autority) a dotknuté organizácie musia zabezpečiť :

* Požadovanú súčinnosť pri riešení bezpečnostného incidentu alebo jeho predchádzaní v rozsahu adekvátnom pre danú organizáciu.
* Implementáciu požadovaných bezpečnostných opatrení schválených príslušnou rezortnou / sektorovou autoritou.



Obrázok 1Koordinácia riešenie bezpečnostných incidentov národnej úrovni

# Bezpečnostné tímy

V rámci prípravy technických spôsobilostí (viď Príprava technických spôsobilostí a komunikačných kanálov) musí každý rezortný /sektorový útvar, národná autorita, organizácia so zvýšenými požiadavkami na bezpečnosť disponovať Bezpečnostným tímom, ktorý zabezpečí základnú úroveň bezpečnosti informačných systémov v danej inštitúcii. Je odporúčané, aby túto základnú úroveň zabezpečili priamo interní zamestnanci Bezpečnostného tímu. Časť nižšie uvedených úloh (pri ktorých je to explicitne uvedené) je možné delegovať na dodávateľské subjekty, avšak v tomto prípade musia interní zamestnanci Bezpečnostného tímu robiť dohľad nad akciami vykonanými dodávateľom a následne skontrolovať výsledok akcií.

**Úlohy**

* Vytvorenie a udržiavanie konfiguračnej databázy spravovanej infraštruktúry s uvedením, či sú jednotlivé prvky spravované internými , externými zamestnancami alebo dodávateľmi
  + je potrebné zabezpečiť, aby ku každému prvku vo vlastníctve inštitúcie disponoval administrátorským prístupom aspoň jeden interný zamestnanec bezpečnostného tímu (môže byť použitý pre účely dohľadu nad akciami dodávateľov)
  + Periodicita plnenia: priebežne pri každej zmene v infraštruktúre
  + Typ úlohy: povinná
* Implementovať dohľadový systém nad spravovanou infraštruktúrou
  + Za dohľadový systém pre účely splnenia tejto úlohy je možné považovať aj centrálny logovací systém za predpokladu, že sú doň preposielané logy z dôležitých častí infraštruktúry a tieto logy je možné kontrolovať
  + úlohou môžu byť poverení dodávatelia, avšak je potrebné vykonať kontrolu jej splnenia
  + Periodicita plnenia: Jednorazovo
  + Typ úlohy: povinná
* Monitorovať infraštruktúru prostredníctvom dohľadového systému
  + musia byť zaznamenávané anomálie a na základe bezpečnostných politík danej inštitúcie musí byť vyhodnocované, či sa jedná o bezpečnostný incident
  + v prípade detekcie bezpečnostného incidentu je potrebné začať incident riešiť (viď časť o riešení bezpečnostných incidentov)
  + Periodicita plnenia: pravidelne
  + Typ úlohy: povinná
* Hardening systémov na základe odporúčaní rezortnej/sektorového útvaru alebo národnej autority
  + úlohou môžu byť poverení dodávatelia, avšak je potrebné vykonať kontrolu jej splnenia
  + Periodicita plnenia: priebežne
  + Typ úlohy: povinná
* Ohodnotenie zraniteľností na základe verzie a konfigurácie software
  + V prípade prijatia varovania o zraniteľnostiach musí byť na základe konfiguračnej databázy zistené, či sa zraniteľnosť týka danej inštitúcie a ohodnotené riziko prípadného zneužitia takejto zraniteľnosti
  + Periodicita plnenia: priebežne
  + Typ úlohy: povinná

### Personálne zabezpečenie

V rámci personálneho zabezpečenia Bezpečnostného tímu musí inštitúcia zabezpečiť aspoň dvoch interných zamestnancov, z toho

* aspoň jedného s IT znalosťami minimálne v rozsahu znalostného štandardu vypracovaného pre vedúcich pracovníkov v oblasti informačnej bezpečnosti[[10]](#footnote-10) ,
* aspoň jedného s IT znalosťami minimálne v rozsahu znalostného štandardu vypracovaného pre nešpecialistov v oblasti informačnej bezpečnosti[[11]](#footnote-11).

Bezpečnostné tímy rezortných a sektorových útvarov by mali mať aspoň troch interných zamestnancov, z toho

* aspoň jedného s IT znalosťami minimálne v rozsahu znalostného štandardu vypracovaného pre vedúcich pracovníkov v oblasti informačnej bezpečnosti[[12]](#footnote-12) ,
* aspoň dvoch s IT znalosťami minimálne v rozsahu znalostného štandardu vypracovaného pre nešpecialistov v oblasti informačnej bezpečnosti[[13]](#footnote-13).

Členom bezpečnostného tímu musí byť interný zamestnanec s právomocou v prípade potreby vypnúť / zablokovať / vykonať zmenu / obmedziť prevádzku služieb poskytovaných prostredníctvom externých sietí. Je odporúčané, aby bol tento zamestnanec jeden z vyššie uvedených zamestnancov.

Platové ohodnotenie člena bezpečnostného tímu musí byť minimálne na úrovni 80 percent výšky platového ohodnotenia na rovnakej pozícií v súkromnom sektore.

# Tímy CSIRT

V rámci prípravy technických spôsobilostí (viď Príprava technických spôsobilostí a komunikačných kanálov) musí každý rezortný /sektorový útvar a národná autorita disponovať CSIRT tímom, ktorý zabezpečí na riešenie bezpečnostných incidentov v danom rezorte/sektore a v organizáciách so zvýšenými požiadavkami na bezpečnosť. Bezpečnostné incidenty by mali riešiť priamo interní zamestnanci rezortných/sektorových CSIRT tímov, v prípade nedostatočných kapacít musí rezortný/sektorový CSIRT tím eskalovať riešenie bezpečnostného incidentu na národnú autoritu (vládny CSIRT tím).

Rezortné/sektorové CSIRT tímy musia mať technické spôsobilosti potrebné na riešenie bezpečnostných incidentov na rezortnej/sektorovej úrovni, obranu voči kybernetickým útokom, spôsobilosti na posudzovanie a analýzu bezpečnostných hrozieb, tvorbu bezpečnostných štandardov pre infraštruktúry daného rezortu/sektora s ohľadom na špecifické hrozby pre daný rezort/sektor.

**Úlohy (rezortný/sektorový CSIRT tím)**

Rezortný/sektorový CSIRT tím by mal pre svoju konštituenciu (rezort/sektor) zabezpečiť nasledovné služby:

* Základná počítačová forenzná analýza
  + Disponovať technickými spôsobilosťami na prevedenie základných úkonov súvisiacich s forenznou analýzou:
    - Zaisťovanie obrazu operačnej pamäte a pevných diskov[[14]](#footnote-14)
    - Kontrola prebiehajúcej sieťovej komunikácie a spustených procesov a služieb[[15]](#footnote-15)
    - Identifikácia programov spúšťaných po štarte operačného systému a/alebo po prihlásení používateľa[[16]](#footnote-16)
  + Periodicita plnenia: priebežne
  + Typ úlohy: povinná
* Základná analýza malware
  + Disponovať technickými spôsobilosťami na prevedenie základných úkonov súvisiacich s analýzou škodlivého kódu:
    - Mať pripravené fyzicky izolované prostredie od zvyšku siete, ktoré je určené na takúto analýzu
    - Vyhľadávanie analýz daného súboru[[17]](#footnote-17)
    - Kontrolu základných informácií o vzorke a určenie, či môže byť škodlivá[[18]](#footnote-18)
    - Analýza správania sa vzorky za normálnych okolností[[19]](#footnote-19)
  + Periodicita plnenia: priebežne
  + Typ úlohy: odporúčaná
* Penetračné testy
  + Vykonať externé penetračné testy verejne poskytovaných služieb organizácií .
  + Periodicita plnenia: priebežne. Každá organizácia aspoň raz za 3 roky.
  + Typ úlohy: odporúčaná
* Korelácia a vyhodnocovanie údajov z rôznych podriadených organizácií v rámci sektora/rezortu
  + Viesť evidenciu o zaznamenaných incidentoch v rámci konštituencie a hľadať medzi nimi vzájomné súvislosti
  + Periodicita plnenia: priebežne
  + Typ úlohy: povinná
* Analýza a riešenie incidentov
  + Disponovať spôsobilosťami na analýzu a riešenie incidentov:
    - Identifikácia incidentov, vyhľadávanie relevantných informácií súvisiacich s incidentom[[20]](#footnote-20)
    - Kooperovať a poskytnúť vzdialenú podporu Bezpečnostného tímu počas riešenia incidentu
    - Kooperácia s ďalšími CSIRT tímami a relevantnými organizáciami[[21]](#footnote-21)
    - Vykonať základnú forenznú analýzu na mieste incidentu
    - Určiť pravdepodobné príčiny vzniku incidentu a navrhnúť opatrenia
  + Periodicita plnenia: priebežne
  + Typ úlohy: povinná
* Analýza bezpečnostných rizík
  + Na základe informácií o zraniteľnostiach vykonať analýzu rizík s ohľadom na informačné systémy v konštituencii a informovanie konštituencie
  + Periodicita plnenia: priebežne
  + Typ úlohy: povinná
* Služby detekcie prienikov
  + V súčinnosti s Bezpečnostným tímom pri riešení incidentu na mieste detegovať prienik útočníka do infraštruktúry na základe:
    - Sieťovej komunikácie pracovných staníc a serverov
    - Spustených procesov a služieb
    - Programov spúšťaných po štarte operačného systému a/alebo po prihlásení používateľa
    - Odhalenia použitia podsunutých dát a/alebo informácií útočníkom[[22]](#footnote-22)
  + Periodicita plnenia: priebežne
  + Typ úlohy: povinná
* Monitorovanie stavu hrozieb v oblasti IKT s ohľadom na špecifické hrozby pre daný rezort/sektor
  + Kontrolovať a vyhodnocovať informačné zdroje minimálne v rozsahu
    - Varovania a oznámenia od národnej autority
    - Webové portály výrobcov hardvéru a softvéru používaného v informačných systémoch konštituencie
  + Periodicita plnenia: priebežne
  + Typ úlohy: povinná
* Konzultačná činnosť v oblasti informačnej bezpečnosti a zvyšovanie povedomia o informačnej bezpečnosti v rámci rezortu/sektora
  + Periodicita plnenia: priebežne
  + Typ úlohy: povinná

Národná autorita musí zabezpečiť vládny CSIRT tím, ktorý musí mať technické spôsobilosti potrebné na riešenie bezpečnostných incidentov na národnej úrovni, obranu voči pokročilým kybernetickým útokom, spôsobilosti na posudzovanie a analýzu bezpečnostných hrozieb a tvorbu bezpečnostných štandardov pre infraštruktúry verejnej správy.

**Úlohy (vládny CSIRT tím)**

Rezortný/sektorový CSIRT tím by mal pre svoju konštituenciu (organizácie so zvýšenými požiadavkami na bezpečnosť, pomoc rezortným/sektorovým CSIRTom v prípade eskalácie bezpečnostného incidentu) zabezpečiť nasledovné služby:

* Pokročilá počítačová forenzná analýza
  + Disponovať technickými spôsobilosťami na prevedenie základných aj pokročilých úkonov súvisiacich s forenznou analýzou:
    - Zaisťovanie obrazu operačnej pamäte a pevných diskov[[23]](#footnote-23)
    - Kontrola prebiehajúcej sieťovej komunikácie a spustených procesov a služieb[[24]](#footnote-24)
    - Identifikácia programov spúšťaných po štarte operačného systému a/alebo po prihlásení používateľa[[25]](#footnote-25)
    - Offline analýza zaistených obrazov operačnej pamäte a pevného disku, vyhľadávanie škodlivých artefaktov a digitálnych stôp relevantných pre overovanie forenznej hypotézy[[26]](#footnote-26)
    - Offline aj online analýza sieťovej komunikácie[[27]](#footnote-27)
  + Periodicita plnenia: priebežne
  + Typ úlohy: povinná
* Pokročilá analýza malware
  + Disponovať technickými spôsobilosťami na prevedenie základných aj pokročilých úkonov súvisiacich s analýzou škodlivého kódu:
    - Mať pripravené fyzicky izolované prostredie od zvyšku siete, ktoré je určené na takúto analýzu
    - Vyhľadávanie analýz daného súboru[[28]](#footnote-28)
    - Kontrolu základných informácií o vzorke a určenie, či môže byť škodlivá[[29]](#footnote-29)
    - Analýza správania sa vzorky za normálnych okolností[[30]](#footnote-30)
    - Dynamická analýza vzorky (debuggovanie)
    - Reverzné inžinierstvo, zistenie kompletných schopností vzorky vrátanie odhalenia skrytej funkcionality
  + Periodicita plnenia: priebežne
  + Typ úlohy: povinná
* Penetračné testy
  + Vykonávať externé penetračné testy nasadzovaných informačných systémov v konštituencii s kontrolou zraniteľností minimálne v rozsahu OWASP Top Ten[[31]](#footnote-31)
  + Periodicita plnenia: priebežne
  + Typ úlohy: povinná
* Korelácia a vyhodnocovanie údajov z rôznych podriadených organizácií v rámci celej konštituencie (vrátane jednotlivých rezortov/sektorov aj organizácii so zvýšenými požiadavkami na bezpečnosť)
  + Viesť evidenciu o zaznamenaných incidentoch v rámci konštituencie a hľadať medzi nimi vzájomné súvislosti
  + Periodicita plnenia: priebežne
  + Typ úlohy: povinná
* Analýza a riešenie incidentov
  + Disponovať spôsobilosťami na analýzu a riešenie rozsiahlych incidentov na národnej a medzinárodnej úrovni:
    - Identifikácia incidentov, vyhľadávanie relevantných informácií súvisiacich s incidentom[[32]](#footnote-32)
    - Kooperovať a poskytnúť vzdialenú podporu Bezpečnostného tímu a rezortným/sektorovým CSIRT tímom počas riešenia incidentu
    - Kooperácia s ďalšími CSIRT tímami na národnej aj medzinárodnej úrovni a relevantnými organizáciami[[33]](#footnote-33)
    - Vykonať základnú forenznú analýzu na mieste incidentu, vykonať pokročilú forenznú analýzu a v prípade potreby analýzu malware
    - Určiť pravdepodobné príčiny vzniku incidentu a navrhnúť opatrenia
  + Disponovať kapacitami na súčasné riešenie minimálne troch rozsiahlych incidentov
  + Periodicita plnenia: priebežne
  + Typ úlohy: povinná
* Analýza bezpečnostných rizík a zraniteľností
  + Na základe informácií o objavených zraniteľnostiach analyzovať tieto zraniteľnosti, možnosti ich zneužitia a dôsledky
  + Na základe informácii o zraniteľnostiach a analýzy zraniteľností Vykonať analýzu rizík s ohľadom na informačné systémy v konštituencii a informovanie konštituencie
  + Periodicita plnenia: priebežne
  + Typ úlohy: povinná
* Služby detekcie prienikov
  + V súčinnosti s Bezpečnostným tímom, príp. rezortným/sektorovým CSIRTom pri riešení incidentu na mieste detegovať prienik útočníka do infraštruktúry na základe:
    - Sieťovej komunikácie pracovných staníc, serverov a sieťových prvkov prostredníctvom nástrojov dostupných na daných systémoch aj skryto prostredníctvom zariadení typu network tap
    - Spustených procesov a služieb
    - Programov spúšťaných spúšťaných po štarte operačného systému a/alebo po prihlásení používateľa
    - Odhalenia použitia podsunutých dát a/alebo informácií útočníkom[[34]](#footnote-34)
  + Periodicita plnenia: priebežne
  + Typ úlohy: povinná
* Monitorovanie stavu hrozieb v oblasti IKT s ohľadom na špecifické hrozby infraštruktúry verejnej správy
  + Kontrolovať a vyhodnocovať informačné zdroje minimálne v rozsahu
    - Varovania a oznámenia od zahraničných partnerov
    - Neverejné príspevky na konferenciách určených pre akreditované CSIRT tímy[[35]](#footnote-35)
    - Webové portály výrobcov hardvéru a softvéru používaného v informačných systémoch konštituencie
    - Databázy verejne známych exploitov
    - Verejné mailinglisty a diskusné skupiny zamerané na kybernetickú bezpečnosť
    - Neverejné časti Internetu (Dark web)
  + Periodicita plnenia: priebežne
  + Typ úlohy: povinná
* Konzultačná činnosť v oblasti informačnej bezpečnosti a zvyšovanie povedomia o informačnej bezpečnosti zamestnancov verejnej správy
  + Pravidelne školiť vedúcich pracovníkov a technických zamestnancov rezortných/sektorových CSIRT tímov a bezpečnostných tímov vo verejnej správe
  + Pravidelne školiť bežných zamestnancov verejnej správy, resp. vyškoliť špecialistov v rezortných/sektorových CSIRT tímoch, ktorí budú školiť zamestnancov v príslušných rezortoch/sektoroch
  + Periodicita plnenia: priebežne
  + Typ úlohy: povinná

### Personálne zabezpečenie

V rámci personálneho zabezpečenia **rezortných/sektorových CSIRT tímov** by mala rezortná/sektorová autorita zabezpečiť aspoň štyroch interných zamestnancov, z toho

* aspoň jedného s IT znalosťami minimálne v rozsahu znalostného štandardu vypracovaného pre vedúcich pracovníkov v oblasti informačnej bezpečnosti[[36]](#footnote-36) ,
* aspoň dvoch s IT znalosťami minimálne v rozsahu znalostného štandardu vypracovaného pre špecialistov v oblasti informačnej bezpečnosti[[37]](#footnote-37) ,
* aspoň jedného s IT znalosťami minimálne v rozsahu znalostného štandardu vypracovaného pre nešpecialistov v oblasti informačnej bezpečnosti[[38]](#footnote-38).

Rezortné/sektorové tímy musia mať aspoň dvoch zamestnancov, ktorí ovládajú anglický jazyk minimálne na úrovni B1.

V prípade, že rezortná/sektorová autorita nevie splniť uvedené personálne požiadavky, musí zabezpečiť iný CSIRT tím, ktorý bude vykonávať úlohy príslušného CSIRT tímu. Takto poverený CSIRT tímu však musí mať minimálne štyroch zamestnancov, ktorí sú interní zamestnanci niektorej organizácie verejnej správy a spĺňajú vyššieuvedené kvalifikačné predpoklady na zamestnancov rezortných/sektorových CSIRT tímov. Odporúčané je v tomto prípade uzavrieť dohodu o spolupráci a poveriť rezortný/sektorový CSIRT tím iného rezortu/sektora. Alternatívne je možné uzavrieť dohodu o spolupráci priamo s vládnym CSIRT tímom.

V rámci personálneho zabezpečenia **vládneho CSIRT tímu** by mala národná autorita zabezpečiť aspoň trinástich interných zamestnancov, z toho

* aspoň troch s IT znalosťami minimálne v rozsahu znalostného štandardu vypracovaného pre vedúcich pracovníkov v oblasti informačnej bezpečnosti[[39]](#footnote-39) ,
* aspoň desiatich s IT znalosťami minimálne v rozsahu znalostného štandardu vypracovaného pre špecialistov v oblasti informačnej bezpečnosti[[40]](#footnote-40) .

Aspoň ôsmi zamestnanci vládneho tímu musia ovládať anglický jazyk minimálne na úrovni B1. Zároveň aspoň piati špecialisti a aspoň dvaja vedúci pracovníci musia byť držiteľmi niektorého z medzinárodne uznávaných certifikátov dokladajúcich ich odbornosť. Pre špecialistov sú odporúčané certifikáty CEH, CHFI, GCIH, CISSP, GCIH,GCFA, CASP, SSCP. Pre vedúcich zamestnanec sú odporúčané: CISSP, CISM, CISA, CGEIT.

Platové ohodnotenie člena tímu CSIRT musí byť minimálne na úrovni 80 percent výšky platového ohodnotenia na rovnakej pozícií v súkromnom sektore.

Národná autorita nemôže delegovať riešenie a analýzu incidentov na zamestnancov, ktorí nie sú zamestnancami v štátnej alebo vo verejnej službe. V prípade rozsiahleho bezpečnostného incidentu alebo incidentu, ktorý svojou náročnosťou presahuje technické spôsobilosti uvedené v tomto dokumente, môže vládny CSIRT požiadať o spoluprácu vo forme konzultácie niektoré súkromné spoločnosti. Národná autorita však musí zabezpečiť ochranu citlivých údajov súvisiacich s riešeným incidentom.

# Bezpečnostné opatrenia

Bezpečnostné opatrenia v rámci organizácie boli navrhnuté v rámci metodiky : Metodika pre zabezpečenie organizácií v oblasti informačnej bezpečnosti, ktorá bola vypracovaná špecializovaným útvarom CSIRT.SK v spolupráci s Úradom podpredsedu vlády SR pre investície a informatizáciu

Metodika bola napísaná na zvýšenie odolnosti organizácií voči štandardným a niektorým typom pokročilých kybernetických útokov.

Táto metodika obsahuje požiadavky na organizáciu rozdelenú do oblastí:

* 1. Administratívna a organizačná bezpečnosť,
  2. Vývoj a nasadenie informačného systému,
  3. Zabezpečenie externe dostupných služieb,
  4. Zabezpečenie externe dostupných služieb – webové služby,
  5. Zabezpečenie internej infraštruktúry,
  6. Zabezpečenie pracovných staníc.

Metodika je dostupná na webovom sídle CSIRT.SK[[41]](#footnote-41).

# Posúdenie bezpečnosti

Nutným predpokladom vytvorenia a udržania požadovanej úrovne informačnej bezpečnosti z hľadiska odolnosti voči kybernetickým útokom sú kontrolné mechanizmy resp. mechanizmy na posúdenie bezpečnosti[[42]](#footnote-42) .

Mechanizmy posúdenia bezpečnosti sú špecifikované v tabuľke č. 1. Pre každý mechanizmus sú uvedené:

* Názov mechanizmu posúdenia informačnej bezpečnosti z hľadiska odolnosti voči kybernetickým útokom
* Popis mechanizmu posúdenia informačnej bezpečnosti z hľadiska odolnosti voči kybernetickým útokom
* Cieľ mechanizmu (dôvod vykonávania)
* Frekvencia opakovania : potrebná periodicita vykonania posúdenia informačnej bezpečnosti
* Predpoklady vykonania daného posúdenia informačnej bezpečnosti
* Súvisiace aktivity

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Názov** | **Popis** | **Cieľ** | **Frekvencia opakovania** | **Predpoklady** | **Súvisiaca aktivita** |
| Analýza rizík | Identifikácia a posúdenie rizík informačnej bezpečnosti na základe identifikácie a ohodnotenia aktív, bezpečnostných zraniteľností a bezpečnostných hrozieb a ohodnotenie pravdepodobnosti a možných dopadov zneužitia zraniteľnosti aktíva hrozbou. | Získanie prehľadu o rizikách informačnej bezpečnosti, prioritizácia ich zmierňovania, identifikácia opatrení na ich zmiernenie, určenie miery akceptovateľného rizika. | Vždy pred nasadením IS do produkčného prostredia. Aspoň raz ročne aktualizácia a prehodnotenie zvyškových rizík. | Stredná úroveň vyspelosti bezpečnostných opatrení. | Audit informačnej bezpečnosti |
| Audit informačnej bezpečnosti | Technické, procesné alebo dokumentačné posúdenie informačnej bezpečnosti | Posúdenie zhody informačnej bezpečnosti so štandardom alebo súlad s legislatívnymi, normatívnymi, regulačnými alebo zmluvnými požiadavkami. | Raz za tri roky musia byť auditované všetky IS a procesy, odporúča sa vykonávať čiastkové audity raz ročne | Stredná úroveň vyspelosti bezpečnostných opatrení, nezávislosť audítora na predmete auditu. | Analýza rizík, Posúdenie zraniteľností |
| Posúdenie zraniteľností | Identifikácia a technické posúdenie bezpečnostných zraniteľností | Identifikácia čo možno najväčšieho množstva zraniteľností a ich závažnosti a prioritizácia ich odstraňovania. | Vždy pred nasadením IS do produkčného prostredia. Aspoň raz ročne. | Nízka alebo stredná úroveň vyspelosti bezpečnostných opatrení, počiatočné fázy implementácie bezpečnostného programu. | Penetračné testovanie |
| Penetračné testovanie | Technické posúdenie informačnej bezpečnosti za použitia techník a nástrojov útočníkov, ide napr. o prienik do IS a následnú exfiltráciu údajov, získanie doménového administrátora alebo modifikáciu informácií. | Overenie úrovne zabezpečenia informačných systémov pred počítačovými útokmi, identifikovanie zraniteľností a navrhnutie bezpečnostných opatrení | Po implementácii všetkých opatrení vyplývajúcich z posúdenia zraniteľností. Aspoň raz za dva roky. | Vysoká úroveň vyspelosti bezpečnostných opatrení, predchádzajúce vykonanie viacerých posúdení zraniteľností a implementácia všetkých opatrení. | Posúdenie zraniteľností, Red Teaming |

Uvedené mechanizmy sú minimálnou množinou kontrolných mechanizmov na úrovni organizácie, rezortu/sektora a národnej úrovni na komplexné posudzovanie informačnej bezpečnosti, ktoré je potrebné implementovať na získanie prehľadu o stave informačnej bezpečnosti v organizácií resp. rezorte/sektore resp. národnej úrovni.

## Analýza rizík

V súčasnosti je známych veľké množstvo postupov na analýzu rizík, ktoré sú vhodné pre jednotlivé účely použitia na ktoré boli vytvorené ako aj množstvo všeobecných metodík na analýzu rizík.

Aby bolo možné porovnávať výsledky z analýz rizík v jednotlivých organizáciách, na úrovni rezortov/ sektorov a na národnej úrovni je potrebné aby analýza rizík bola kompatibilná z hľadiska výstupov a ich odbornej úrovne.

Nižšie je uvedená základná kvalitatívna metodika pre analýzu rizík, ktorá bola vybraná z dôvodu nízkej náročnosti na realizáciu a relatívne vysokej prehľadnosti výstupov.

Alternatívne je na národnej úrovni uvedená úloha na vytvorenie prípadne komplexnej národnej metodiky na analýzu rizík v spolupráci s akademickou obcou a odbornou verejnosťou.

**Úroveň organizácie**

### Identifikácia a ohodnotenie aktív

* Organizácia musí identifikovať všetky významné aktíva, ktoré sa podieľajú na kľúčových procesoch, alebo tvoria súčasť informačného systému.
* Pri ohodnotení aktív by sa mali využiť rozhovory so zamestnancami, mali by sa načrtnúť realistické scenáre prípadov ohrozenia týchto aktív, ktoré by mohli nastať (napr. ich poškodenie, zničenie, narušenie ich dostupnosti, dôvernosti a integrity).
* Pri ohodnocovaní aktív organizácia musí použiť vopred definovanú stupnicu. Odporúča sa použiť stupnicu aspoň v nasledovnom rozsahu:
  + 1 (málo významné) – aktívum, ktorého poškodenie, zničenie alebo strata dôvernosti, dostupnosti alebo integrity nenaruší kľúčové procesy a prípadné škody je možné rýchlo a ľahko kompenzovať.
  + 2 (stredne významné) – aktívum, ktorého poškodenie, zničenie alebo strata dôvernosti, dostupnosti alebo integrity môže čiastočne narušiť procesy a prípadné škody budú mať vplyv na rozpočet organizácie.
  + 3 (veľmi významné) – aktívum, ktorého poškodenie, zničenie alebo strata dôvernosti, dostupnosti alebo integrity môže významne ohroziť kľúčové procesy, prípadne samotnú existenciu organizácie a spôsobiť vysokú škodu alebo ohroziť zdravie a životy osôb.

### Identifikácia a ohodnotenie hrozieb

* Pre každé identifikované aktívum sa musia identifikovať významné hrozby, ktoré majú potenciál spôsobiť škodu na aktívach.
* Pri identifikácií hrozieb by sa mali brať do úvahy hrozby v nasledovných kategóriách:
  + externé a interné,
  + ľudské, technologické a hrozby prostredia,
  + úmyselné a neúmyselné.
* Pri identifikácii a ohodnotení hrozieb sa musí spolupracovať s vlastníkmi a používateľmi aktív.
* Pri ohodnotení hrozieb organizácia musí použiť vopred definovanú stupnicu. Odporúča sa použiť stupnicu aspoň v nasledovnom rozsahu:
  + N (nízka),
  + S (stredná),
  + V (vysoká).

### Identifikácia a ohodnotenie zraniteľností

* Pre každú identifikovanú zraniteľnosť konkrétneho aktíva sa musia identifikovať zraniteľnosti, ktoré môže táto hrozba využiť (napr. nedostatočne vyškolený zamestnanec, chýbajúce zálohovanie, nedostatočná ochrana pracovných staníc pred škodlivým softvérov, atď).
* Pri identifikácií zraniteľnosti sa musí spolupracovať s vlastníkmi a používateľmi aktív.
* Pri ohodnotení zraniteľností organizácia musí použiť vopred definovanú stupnicu. Odporúča sa použiť stupnicu aspoň v nasledovnom rozsahu:
  + N (nízka) – využitie zraniteľnosti hrozbou je málo pravdepodobné,
  + S (stredná) - využitie zraniteľnosti hrozbou je pravdepodobné,
  + V (vysoká) - využitie zraniteľnosti hrozbou je veľmi pravdepodobné.

### Výpočet rizika a vyhodnotenie rizík

* Hodnota rizika sa musí vypočítať na základe vopred definovaného kľúča ako kombinácia hodnoty hrozby a pravdepodobnosti zneužitia zraniteľnosti hrozbou.
* Odporúča sa použiť hodnotiacu tabuľku rizík aspoň v nasledovnom rozsahu:
  + Hodnota rizika môže nadobudnúť hodnoty od 0 do 6, pričom 0 je najnižšie riziko a 6 najvyššie riziko.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Riziko | Hrozba | N | | | S | | | V | | |
| Zraniteľnosť | N | S | V | N | S | V | N | S | V |
| Aktívum | 1 | 0 | 1 | 2 | 1 | 2 | 3 | 2 | 3 | 4 |
| 2 | 1 | 2 | 3 | 2 | 3 | 4 | 3 | 4 | 5 |
| 3 | 1 | 3 | 4 | 2 | 4 | 5 | 3 | 5 | 6 |

### Rozhodnutie o správe rizík

Organizácia musí vykonávať správu rizík aspoň v rozsahu:

* redukcia rizika (hodnotu rizika sa znižuje prijatím vhodných opatrení)
* znížením pravdepodobnosti, že bude využitá zraniteľnosť
* obmedzením možného dopadu v prípade, že sa riziko vyskytne
* prijatie rizika (nevykonajú sa žiadne opatrenia)
* vyhnutie sa riziku (vyhnutie sa činnosti, alebo podmienke, ktorá dáva impulz k vzniku rizika)
  + nevykonávaním určitých aktivít
  + premiestnením aktív mimo oblasť rizika
* prenos rizika (prenos rizika na inú stranu)
  + poistenie
  + outsourcing

Organizácia musí rozhodnúť o správe rizík na základe ich kategorizácie aspoň v rozsahu:

* akceptovateľné riziko (hodnoty 0 - 2) - nevyžaduje sa žiadna akcia, je ho možné akceptovať (pokiaľ legislatívne alebo zmluvné požiadavky neukladajú povinnosť ho riadiť).
* významné riziko (hodnoty 3 – 4) – musia sa prijať opatrenia na redukciu rizika (s ohľadom na pomer nákladov na prijatie opatrení a prípadných škôd),
* neakceptovateľné riziko (hodnoty 5 - 6) - musia sa prijať opatrenia na redukciu rizika a procesy by nemali byť spustené skôr, ako sa riziko zníži na akceptovateľnú úroveň.

### Návrh a implementácia opatrení

* Na základe výsledkov ohodnotenia rizík a rozhodnutia o správe rizík je následne sa musia vybrať vhodné opatrenia na redukciu rizík.
* Organizácia musí viesť Plán zvládania rizík, aspoň v rozsahu:
  + úlohy v rámci ktorých budú opatrenia realizované,
  + potrebné zdroje na realizáciu opatrení,
  + termíny úloh,
  + zodpovednosti za realizáciu úloh.

### Vyhodnotenie opatrení a preskúmavanie zvyškového rizika

* Organizácia musí vykonávať vyhodnocovanie efektivity opatrení jeden krát ročne.
* Základnými zdrojmi vyhodnocovania efektivity opatrení sú:
  + zistenia interných auditov,
  + výsledky ohodnotenia rizík,
  + záznamy bezpečnostných incidentov.
* Ohodnotenie rizík sa musí vykonávať raz ročne, alebo operatívne v prípade výskytu mimoriadnych udalostí ako napr:
  + výskyt nových hrozieb,
  + zvýšené množstvo bezpečnostných incidentov,
  + významná zmena v aktívach alebo v strategických cieľoch organizácie.

**Úlohy** (všetky organizácie verejnej správy a prvky kritickej infraštruktúry)

* Názov úlohy: Vykonať analýzu rizík bezpečnosti informačných systémov raz ročne.
  + Periodicita : Raz ročne
  + Typ úlohy : povinná

### 

* Rezortná / sektorová autorita musí pre zodpovedajúci rezort / sektor vykonávať analýzu rizík.
* Na účely vykonanie rezortnej / sektorovej analýzy rizík by sa mala zostaviť pracovná skupina zo zástupcov organizácií rezortu/sektora.

**Úlohy** (rezortné / sektorové autority)

* Názov úlohy : Vykonať analýzu rizík bezpečnosti informačných systémov.
  + Periodicita : raz za tri roky a pri významných zmenách.
  + Typ úlohy : povinná

**Národná úroveň**

* Národná autorita musí vykonávať analýzu rizík na národnej úrovni.
* Na účely vykonanie národnej analýzy rizík by sa mala zostaviť medzirezortná pracovná skupina.

**Úlohy** (národná autorita)

* Názov úlohy : Vykonať analýzu rizík bezpečnosti národného kybernetického priestoru.
  + Periodicita : Raz za tri roky a pri významných zmenách
  + Typ úlohy : povinná
* (Alternatíva) Názov úlohy : Vytvoriť metodiku na analýzu rizík v spolupráci s akademickou obcou a odbornou verejnosťou.
  + Periodicita : Jednorázovo
  + Typ úlohy : Odporúčaná

## Audit informačnej bezpečnosti

**Úroveň organizácie**

Auditom informačnej bezpečnosti na úrovni organizácie sa rozumie kontrolná činnosť pre opatrenia informačnej bezpečnosti z pohľadu odolnosti organizácie voči kybernetickým útokom vykonaný vlastným zamestnancom alebo zmluvným audítorom[[43]](#footnote-43). Z pohľadu odolnosti organizácie voči kybernetickým útokom nie je možné auditovať iba technické opatrenia nakoľko tieto závisia od administratívnych, organizačných a personálnych opatrení, preto je potrebné vykonávať audit informačnej bezpečnosti z pohľadu odolnosti voči kybernetickým útokom systematicky a vychádza z potreby komplexnej analýzy celkového prostredia organizácie.

Príklad priebehu etáp auditu informačnej bezpečnosti s dôrazom na odolnosť organizácie voči kybernetickým útokom.

### Príprava

* Pred vykonaním samotného auditu organizácia musí vymenovať vedúceho audítora, ktorý bude poverený zostaviť auditný tím a vykonať samotný audit.
* Pred vykonaním auditu by auditný tím mal vykonať a nechať odsúhlasiť vedením auditovanej organizácie:
  + určenie cieľov, predmetu a rozsahu auditu,
  + identifikácia kľúčových (kritických) IS, procesov a infraštruktúry,
  + identifikácia dokumentácie potrebnej na audit 1. stupňa,
  + identifikácia zdrojov potrebných na audit 2. stupňa,
  + návrh termínu auditu,
  + identifikácia procesov, ktoré musia byť auditované a ich previazanosť,
  + zistenie úrovne vyspelosti bezpečnostných opatrení,
* Auditnému tímu musí byť sprístupnená všetka relevantná dokumentácia na účely efektívneho naplánovania auditu. Odporúča sa poskytnúť aspoň nasledovné dokumenty:
  + bezpečnostná politika/bezpečnostný zámer,
  + smernice pre narábanie s informačnými systémami a IKT,
  + havarijné plány/plány na obnovu,
  + dokumentácia k jednotlivým informačným systémom,
  + vnútorné predpisy ohľadom nástupu a odchodu zamestnancov,
  + smernica ohľadom disciplinárneho konania,
  + vzorová zmluva s dodávateľom informačných systémov alebo ich súčastí,
  + vzorová pracovná zmluva so zamestnancom,
  + dokumentácia o aplikačných a sieťových prepojeniach,
  + prevádzková dokumentácia IS,
  + dokumentácia súvisiaca s riadením prístupu používateľov k IS,
  + zoznam kritických procesov,
  + akákoľvek iná dokumentácia súvisiaca s IS.

### Audit prvého stupňa

* Počas auditu prvého stupňa by mal auditný tím preskúmať dokumentáciu a na jej základe vypracovať plán auditu.

### Plán auditu

* Plán auditu musí vypracovať vedúci audítor a musí v ňom presný časový rozvrh auditovania jednotlivých procesov/činností/oblastí.
* Pri tvorení plánu auditu ba sa mali brať do úvahy:
  + kritické informačné systémy,
  + IT architektúru/topológia siete,
  + previazanosť jednotlivých procesov.
* Plán auditu musí obsahovať:
  + ciele a predmet auditu,
  + kritéria auditu a referenčné dokumenty (napr. zákony, štandardy zmluvné požiadavky),
  + dátum a miesta, kde majú byť činnosti auditu vykonané,
  + identifikácia organizačných a funkčných útvarov alebo procesov, ktoré majú byť auditované,
  + predpokladaný začiatok a trvanie auditu pre jednotlivé činnosti, vrátane stretnutí s vedením a stretnutí audítorov,
  + určenie rolí a zodpovedností členov auditného tímu a prípadných ďalších osôb prítomných na audite,
  + štruktúru správy z auditu (vrátane spôsobu posudzovania nezhôd), formát a očakávaný termín spracovania auditnej správy a jej distribúcie,
  + organizačné záležitosti,
  + otázky zachovania dôvernosti,
  + popis následných činností.
* Plán auditu musí byť preskúmaný a odsúhlasený auditovaným pred vykonaním auditu.

### Auditný tím

* Auditný tím by bal byť na základe návrhu vedúceho audítora schválený vedením organizácie.
* Hlavnými kritériami pre výber audítorov sú:
  + znalosť štandardov a legislatívy v oblasti bezpečnosti IS VS minimálne v rozsahu znalostného štandardu vypracovaného pre vedúcich pracovníkov v oblasti informačnej bezpečnosti[[44]](#footnote-44),
  + znalosť techník, potrebných na preukázanie zhody/nezhody s požiadavkami,
  + znalosť oblastí IT,
  + technická znalosť činností, ktoré sú predmetom auditu,
  + vhodné osobnostné vlastnosti (dobrý poslucháč, tvorca poznámok, komunikatívny, spravodlivý, systematický, trpezlivý, diplomatický, asertívny),
  + skúsenosti s výkonom auditu,
  + nezávislosť.

### Audit druhého stupňa

* Audit druhého stupňa musí byť vykonaný auditným tímom na mieste výkonu auditovaných činností/procesov.
* Auditný tím by mal počas tejto fázy zabezpečiť aspoň nasledovné činnosti:
  + vykonať úvodné stretnutie
  + auditné pohovory, preskúmavanie a posudzovanie záznamov,
  + zber dôkazov o vykonaných opatreniach a dôkazov súladu,
  + zahrnúť všetkých relevantných zamestnancov z rôznych úrovní a funkčných zaradení.
  + preverovanie poskytnutých informácií,
  + preveriť všetky IS a procesy zahrnuté do rozsahu auditu,
  + vykonať záverečné stretnutie.

### Správa z auditu

* Správu z auditu musí vypracovať vedúci audítor po vykonaní auditu druhého stupňa bez zbytočného odkladu.
* Do správy musí zahrnúť zistenia všetkých členov auditného tímu.
* Správa z auditu musí byť odovzdaná vedeniu organizácie a mala by obsahovať aspoň nasledujúce informácie:
  + dátum auditu,
  + meno osoby zodpovednej za spracovanie správy,
  + mená a role audítorov a hlavných predstaviteľov organizácie,
  + názvy a adresy lokalít, ktoré sú predmetom auditu,
  + predmet auditu a odkaz na preverovanú normu/štandard/legislatívu,
  + mená účastníkov úvodného a záverečného stretnutia,
  + zoznam nájdených nezhôd, pozorovaní/príležitostí na zlepšenie,
  + komentár k zhode systému s požiadavkami,
  + vyjadrenie auditného tímu k rozsahu, v akom organizácia plní požiadavky,
  + návrh opatrení na odstránenie identifikovaných nezhôd,
  + popis problémov, ktoré ovplyvnili priebeh auditu a prijaté opatrenia,
  + zoznam osôb, ktorým bude správa distribuovaná,
  + stanovenie doby, počas ktorej bude správa z auditu uchovaná a náležitosti zachovania mlčanlivosti.

**Úlohy** (Organizácie s vyššími požiadavkami na bezpečnosť a prvky kritickej infraštruktúry)

* Názov úlohy: Vykonať audit informačnej bezpečnosti organizácie.
  + Periodicita : Raz ročne
  + Typ úlohy : povinná

**Úroveň rezortu**

* Rezortná autorita musí vykonávať externý audit organizácií zo svojho zodpovedajúceho rezortu.
* Pred vykonaním samotného auditu musí rezortná autorita vymenovať vedúceho audítora, ktorý bude poverený zostaviť auditný tím a vykonávať samotný audit.

**Úlohy** (rezortné autority)

* Názov úlohy : Vykonať externý audit informačnej bezpečnosti organizácií zo zodpovedajúceho rezortu.
  + Periodicita : priebežne
  + Typ úlohy : odporúčaná

**Národná úroveň**

* Národná autorita by mala vykonávať externý audit rezortných / sektorových autorít.
* Pred vykonaním samotného auditu musí národná autorita vymenovať vedúceho audítora, ktorý bude poverený zostaviť auditný tím a vykonávať samotný audit.

**Úlohy** (národná autorita)

* Názov úlohy : Vykonať externý audit informačnej bezpečnosti rezortných / sektorových autorít.
  + Periodicita : priebežne
  + Typ úlohy : povinná

## Posúdenie zraniteľností

**Úroveň organizácie**

Posúdenie zraniteľností informačnej bezpečnosti na úrovni organizácie sa musí vykonávať ako externé posúdenie zraniteľností (vulnerability scan) vykonané vlastným zamestnancom, sektorovou/rezortnou jednotkou CSIRT, resp. inou jednotkou CSIRT, alebo zmluvným špecialistom.

Organizácia musí vykonávať posúdenie zraniteľností aspoň pre:

* verejne poskytované služby,
* internú infraštruktúru
* webové aplikácie.

### Príprava

* Pred vykonaním posúdenia zraniteľností musí organizácia požiadať niektorý rezortný / sektorový tím CSIRT , vládny tím CSIRT alebo tretiu stranu o vykonanie posúdenia zraniteľností.
* V prípade, že posúdenie zraniteľností nevykonáva kmeňový zamestnanec organizácie, organizácia musí uzavrieť dohodu o vykonaní posúdenia zraniteľností so špecialistom, v ktorom sa uvedie aspoň:
  + primárny a sekundárny kontakt,
  + kontakt na špecialistu,
  + IP adresy, z ktorých bude prebiehať testovanie,
  + IP adresy, ktoré budú predmetom testovania,
  + ciele posúdenia zraniteľností,
  + dátum a čas testovania,
  + mlčanlivosť o zistených skutočnostiach.

### Vykonanie posúdenia zraniteľností

* Špecialista na posúdenie zraniteľností musí vykonávať skenovanie pre výskyt bezpečnostných zraniteľností v dohodnutom rozsahu automatizovanými nástrojmi.
* Zber dôkazov o zistených zraniteľnostiach.
* Špecialista na posúdenie zraniteľností musí identifikované zraniteľnosti kategorizovať do úrovní podľa závažnosti, minimálne však v rozsahu:
  + nízka,
  + stredná,
  + vysoká.

### Správa z posúdenia zraniteľností

* Záverečnú správu musí vypracovať špecialista na posúdenie zraniteľností po jeho vykonaní bez zbytočného odkladu.
* Správa z posúdenia zraniteľností musí byť odovzdaná vedeniu organizácie a mala by obsahovať aspoň nasledujúce informácie:
  + dátum vykonania posúdenia zraniteľností,
  + meno osoby zodpovednej za spracovanie správy,
  + rozsah a spôsob testovania,
  + použité metódy a nástroje,
  + názvy a adresy lokalít, ktoré boli predmetom posúdenia,
  + predmet posúdenia a odkaz na normu/štandard, podľa ktorého sa posudzovanie vykonalo,
  + zoznam nájdených zraniteľností a ich kategorizácia,
  + návrh opatrení na odstránenie identifikovaných zraniteľností,
  + popis problémov a obmedzení, ktoré ovplyvnili priebeh posúdenia zraniteľností a prijaté opatrenia,
  + zoznam osôb, ktorým bude správa distribuovaná.

**Úlohy** (všetky organizácie verejnej správy a prvky kritickej infraštruktúry)

* Názov úlohy: Vykonať externé posúdenie zraniteľností informačných systémov.
  + Periodicita : Aspoň raz ročne
  + Typ úlohy : povinná
* Názov úlohy: Vykonať odstránenie nedostatkov zistených externým posúdením zraniteľností a zaslať správu o prijatých opatreniach rezortnej / sektorovej autorite.
  + Periodicita : Neodkladne
  + Typ úlohy : povinná

## Penetračné testovanie

**Úroveň organizácie**

Vykonanie penetračného testovania na úrovni organizácie sa musí vykonávať vlastným zamestnancom, sektorovou/rezortnou jednotkou CSIRT, resp. inou jednotkou CSIRT, alebo zmluvným špecialistom.

**Penetračné testovanie sa vykonáva vo forme:**

* externého penetračného testu a/alebo
* interného penetračného testu.

### Externé penetračné testovanie

* Organizácia musí vykonávať penetračné testovanie na simuláciu aktivít útočníka z externého prostredia.

**Príprava**

* Pred vykonaním samotného penetračného testu musí organizácia požiadať niektorý rezortný / sektorový tím CSIRT , vládny tím CSIRT alebo tretiu stranu o vykonanie penetračného testovania.
* Všetky zúčastnené strany musia byť informované aspoň o nasledovných skutočnostiach:
  + typ testu,
  + spôsob vykonania testu,
  + pravidlá a obmedzenia pri testovaní,
  + cieľ testovania,
  + rozsah testovania,
  + zoznam poskytnutej dokumentácie,
* V prípade, že penetračné testovanie nevykonávajú kmeňoví zamestnanci organizácie, organizácia musí uzavrieť dohodu o vykonaní posúdenia zraniteľností s organizáciou, ktorá penetračné testovanie vykoná, v ktorom sa uvedie aspoň:
  + primárny a sekundárny kontakt,
  + kontakt na špecialistu,
  + IP adresy, z ktorých bude prebiehať testovanie,
  + IP adresy, ktoré budú predmetom testovania,
  + ciele penetračného testu,
  + dátum a čas testovania,
  + mlčanlivosť o zistených skutočnostiach.

**Vykonanie penetračného testu**

* Vykonanie penetračného testu musí byť vykonané minimálne v rozsahu:
  + Získavanie informácií o systéme a infraštruktúre.
  + Automatizovaná detekcia známych zraniteľností.
  + Manuálne overenie detegovaných zraniteľností a manuálne detegovanie zraniteľností.
  + Overenie použiteľnosti nájdených zraniteľností na exploitáciu, prípadne eskaláciu oprávnení.
  + Napísanie správy popisujúcej nájdené zraniteľnosti, ich kategorizáciu a návrhy na ich odstránenie.
* Tím na penetračné testovanie musí identifikované zraniteľnosti kategorizovať do úrovní podľa závažnosti, minimálne však v rozsahu:
  + nízka,
  + stredná,
  + vysoká.

**Následné činnosti**

* Po ukončení penetračného testu by mal tím na penetračné testovanie poskytnúť testovanej organizácii zoznam všetkých zmien v systéme, ktoré boli počas testu vykonané.
* Organizácia musí bez zbytočného odkladu po získaní informácií o identifikovaných či zneužitých zraniteľnostiach vykonať ich odstránenie.
* Po odstránení zraniteľností by mal byť vykonaný opakovaný test na preverenie implementovaných opatrení.

**Správa o penetračnom testovaní**

* Záverečnú správu musí vypracovať vedúci tímu na penetračné testovanie po jeho vykonaní bez zbytočného odkladu.
* Správa z penetračného testu musí byť odovzdaná vedeniu organizácie a mala by obsahovať aspoň nasledujúce informácie:
  + manažérske zhrnutie,
  + dátum vykonania posúdenia zraniteľností,
  + meno osoby zodpovednej za spracovanie správy,
  + rozsah a spôsob testovania,
  + použité metódy a nástroje,
  + scenár testovania,
  + názvy a adresy lokalít, ktoré boli predmetom posúdenia,
  + zoznam nájdených zraniteľností a ich kategorizácia,
  + spôsob zneužitia zraniteľností,
  + návrh opatrení na odstránenie identifikovaných zraniteľností,
  + popis problémov a obmedzení, ktoré ovplyvnili priebeh posúdenia zraniteľností a prijaté opatrenia,
  + potreba vykonania opakovaného testu,
  + zoznam osôb, ktorým bude správa distribuovaná.

### Interné penetračné testovanie

* Organizácia by mala vykonávať penetračné testovanie na simuláciu aktivít útočníka z interného prostredia.

**Príprava**

* Pred vykonaním samotného penetračného testu musí organizácia požiadať niektorý rezortný / sektorový tím CSIRT , vládny tím CSIRT alebo tretiu stranu o vykonanie penetračného testovania.
* Všetky zúčastnené strany musia byť informované aspoň o nasledovných skutočnostiach:
  + typ testu,
  + spôsob vykonania testu,
  + pravidlá a obmedzenia pri testovaní,
  + cieľ testovania,
  + rozsah testovania,
  + zoznam poskytnutej dokumentácie,
* V prípade, že penetračné testovanie nevykonávajú kmeňoví zamestnanci organizácie, organizácia musí uzavrieť dohodu o vykonaní posúdenia zraniteľností s organizáciou, ktorá penetračné testovanie vykoná, v ktorom sa uvedie aspoň:
  + primárny a sekundárny kontakt,
  + kontakt na špecialistu,
  + IP adresy, z ktorých bude prebiehať testovanie,
  + IP adresy, ktoré budú predmetom testovania,
  + ciele penetračného testu,
  + dátum a čas testovania,
  + mlčanlivosť o zistených skutočnostiach.

**Vykonanie penetračného testu**

* Vykonanie penetračného testu musí byť vykonané minimálne v rozsahu:
  + Získavanie informácií o systéme a infraštruktúre.
  + Automatizovaná detekcia známych zraniteľností.
  + Manuálne overenie detegovaných zraniteľností a manuálne detegovanie zraniteľností.
  + Overenie použiteľnosti nájdených zraniteľností na exploitáciu, prípadne eskaláciu oprávnení.
  + Napísanie správy popisujúcej nájdené zraniteľnosti, ich kategorizáciu a návrhy na ich odstránenie.
* Tím na penetračné testovanie musí identifikované zraniteľnosti kategorizovať do úrovní podľa závažnosti, minimálne však v rozsahu:
  + nízka,
  + stredná,
  + vysoká.

**Následné činnosti**

* Po ukončení penetračného testu by mal tím na penetračné testovanie poskytnúť testovanej organizácii zoznam všetkých zmien v systéme, ktoré boli počas testu vykonané.
* Organizácia musí bez zbytočného odkladu po získaní informácií o identifikovaných či zneužitých zraniteľnostiach vykonať ich odstránenie.
* Po odstránení zraniteľností by mal byť vykonaný opakovaný test na preverenie implementovaných opatrení.

**Správa o penetračnom testovaní**

* Záverečnú správu musí vypracovať vedúci tímu na penetračné testovanie po jeho vykonaní bez zbytočného odkladu.
* Správa z penetračného testu musí byť odovzdaná vedeniu organizácie a mala by obsahovať aspoň nasledujúce informácie:
  + manažérske zhrnutie,
  + dátum vykonania posúdenia zraniteľností,
  + meno osoby zodpovednej za spracovanie správy,
  + rozsah a spôsob testovania,
  + použité metódy a nástroje,
  + scenár testovania,
  + názvy a adresy lokalít, ktoré boli predmetom posúdenia,
  + zoznam nájdených zraniteľností a ich kategorizácia,
  + spôsob zneužitia zraniteľností,
  + návrh opatrení na odstránenie identifikovaných zraniteľností,
  + popis problémov a obmedzení, ktoré ovplyvnili priebeh posúdenia zraniteľností a prijaté opatrenia,
  + potreba vykonania opakovaného testu,
  + zoznam osôb, ktorým bude správa distribuovaná.

**Úlohy** (rezortné /sektorové autority , Organizácie s vyššími požiadavkami na bezpečnosť a prvky kritickej infraštruktúry)

* Názov úlohy: Vykonať externé penetračné testovanie infraštruktúry organizácie.
  + Periodicita : Aspoň raz za tri roky
  + Typ úlohy : povinná
* Názov úlohy: Vykonať odstránenie zistených nedostatkov a zaslať správu o prijatých opatreniach rezortnej / sektorovej autorite .
  + Periodicita : Neodkladne
  + Typ úlohy : povinná

**Úlohy** (rezortné /sektorové autority ,Organizácie s vyššími požiadavkami na bezpečnosť a prvky kritickej infraštruktúry)

* Názov úlohy: Vykonať interné penetračné testovanie infraštruktúry organizácie.
  + Periodicita : Aspoň raz za tri roky
  + Typ úlohy : povinná
* Názov úlohy: Vykonať odstránenie zistených nedostatkov a zaslať správu o prijatých opatreniach rezortnej / sektorovej autorite .
  + Periodicita : Neodkladne
  + Typ úlohy : povinná

1. Tieto organizácie boli vybrané na základe znalosti vykonávaných činností uvedených organizácií. Zoznam nie je vyčerpávajúci, ale každý zoznam musí obsahovať uvedené inštitúcie/organizácie. [↑](#footnote-ref-1)
2. Definícia, popis a úlohy bezpečnostných tímov sú popísané v kapitole 4 [↑](#footnote-ref-2)
3. Definícia, popis a úlohy CSIRT tímov sú popísané v kapitole 5 [↑](#footnote-ref-3)
4. Tieto časti boli vybrané na základe analýzy stavu informačnej bezpečnosti v organizáciách a na národnej úrovni, identifikovaných a riešených bezpečnostných incidentov ako aj konzultáciami s odbornou verejnosťou. [↑](#footnote-ref-4)
5. V prípade že je to možné odporúčame zbierať vo formáte CPE. [↑](#footnote-ref-5)
6. https://www.csirt.gov.sk/doc/MFSRVzdelavanie/02Vzdelavanie2014/Studijne\_materialy/Stud\_2014\_02\_veduci.pdf [↑](#footnote-ref-6)
7. https://www.csirt.gov.sk/doc/MFSRVzdelavanie/02Vzdelavanie2014/Studijne\_materialy/Stud\_2014\_02\_veduci.pdf [↑](#footnote-ref-7)
8. https://www.csirt.gov.sk/doc/MFSRVzdelavanie/02Vzdelavanie2014/Studijne\_materialy/Stud\_2014\_02\_veduci.pdf [↑](#footnote-ref-8)
9. Napríklad nmap. <https://nmap.org/>. Konfigurácia je dostupná na webovej stránke CSIRT.SK [www.csirt.gov.sk](http://www.csirt.gov.sk) [↑](#footnote-ref-9)
10. https://www.csirt.gov.sk/doc/MFSRVzdelavanie/02Vzdelavanie2014/Studijne\_materialy/Stud\_2014\_02\_veduci.pdf [↑](#footnote-ref-10)
11. https://www.csirt.gov.sk/doc/MFSRVzdelavanie/02Vzdelavanie2014/Studijne\_materialy/Stud\_2014\_02\_laici.pdf [↑](#footnote-ref-11)
12. https://www.csirt.gov.sk/doc/MFSRVzdelavanie/02Vzdelavanie2014/Studijne\_materialy/Stud\_2014\_02\_veduci.pdf [↑](#footnote-ref-12)
13. https://www.csirt.gov.sk/doc/MFSRVzdelavanie/02Vzdelavanie2014/Studijne\_materialy/Stud\_2014\_02\_laici.pdf [↑](#footnote-ref-13)
14. Napr. použitím nástroja FTK Imager http://accessdata.com/product-download/digital-forensics [↑](#footnote-ref-14)
15. Napr. použitím nástrojov netstat, tasklist alebo prostredníctvom wmic, powershell [↑](#footnote-ref-15)
16. Napr. použitím nástroja Autoruns https://technet.microsoft.com/sk-sk/sysinternals/bb963902.aspx [↑](#footnote-ref-16)
17. Napr. použitím služby VirusTotal https://virustotal.com/ [↑](#footnote-ref-17)
18. Napr. prostredníctvom vyhľadávania podozrivých textových reťazcov vo vzorke, vlastností sekcií spustiteľných súborov, importovaných a exportovaných funkcií, využívaných zdrojov (resources) [↑](#footnote-ref-18)
19. Napr. použitím využitím nástrojov Process Monitor a WireShark, alebo Cuckoo, prípadne prostredníctvom online služieb. https://technet.microsoft.com/en-us/sysinternals/processmonitor.aspx https://www.wireshark.org/download.html https://cuckoosandbox.org/ https://malwr.com/ [↑](#footnote-ref-19)
20. Napr. dotknuté systémy, IP adresy, porty, DNS a WHOIS záznamy [↑](#footnote-ref-20)
21. Napr. výrobcovia Antimalware produktov, prevádzkovatelia blacklistov [↑](#footnote-ref-21)
22. Napr. použitím nástroja deception token [↑](#footnote-ref-22)
23. Napr. použitím nástroja FTK Imager http://accessdata.com/product-download/digital-forensics [↑](#footnote-ref-23)
24. Napr. použitím nástrojov netstat, tasklist alebo prostredníctvom wmic, powershell [↑](#footnote-ref-24)
25. Napr. použitím nástroja Autoruns https://technet.microsoft.com/sk-sk/sysinternals/bb963902.aspx [↑](#footnote-ref-25)
26. Napr. použitím nástroja Volatility alebo Rekall, AutoPsy. http://www.volatilityfoundation.org/ http://www.rekall-forensic.com/ https://www.sleuthkit.org/autopsy/ [↑](#footnote-ref-26)
27. Napr. použitím port mirroringu alebo zariadení typu network tap, a použitím nástrojov ako WireShark a tcpdump [↑](#footnote-ref-27)
28. Napr. použitím služby VirusTotal https://virustotal.com/ [↑](#footnote-ref-28)
29. Napr. prostredníctvom vyhľadávania podozrivých textových reťazcov vo vzorke, vlastností sekcií spustiteľných súborov, importovaných a exportovaných funkcií, využívaných zdrojov (resources) [↑](#footnote-ref-29)
30. Napr. použitím využitím nástrojov Process Monitor a WireShark, alebo Cuckoo, prípadne prostredníctvom online služieb. https://technet.microsoft.com/en-us/sysinternals/processmonitor.aspx https://www.wireshark.org/download.html https://cuckoosandbox.org/ https://malwr.com/ [↑](#footnote-ref-30)
31. https://www.owasp.org/index.php/Category:OWASP\_Top\_Ten\_Project [↑](#footnote-ref-31)
32. Napr. dotknuté systémy, IP adresy, porty, DNS a WHOIS záznamy [↑](#footnote-ref-32)
33. Napr. výrobcovia Antimalware produktov, prevádzkovatelia blacklistov [↑](#footnote-ref-33)
34. Napr. použitím nástroja deception token [↑](#footnote-ref-34)
35. Napr. TF-CSIRT stretnutia [↑](#footnote-ref-35)
36. https://www.csirt.gov.sk/doc/MFSRVzdelavanie/02Vzdelavanie2014/Studijne\_materialy/Stud\_2014\_02\_veduci.pdf [↑](#footnote-ref-36)
37. https://www.csirt.gov.sk/doc/MFSRVzdelavanie/02Vzdelavanie2014/Studijne\_materialy/Stud\_2014\_02\_IT\_IB\_ucitelia.pdf [↑](#footnote-ref-37)
38. https://www.csirt.gov.sk/doc/MFSRVzdelavanie/02Vzdelavanie2014/Studijne\_materialy/Stud\_2014\_02\_laici.pdf [↑](#footnote-ref-38)
39. https://www.csirt.gov.sk/doc/MFSRVzdelavanie/02Vzdelavanie2014/Studijne\_materialy/Stud\_2014\_02\_veduci.pdf [↑](#footnote-ref-39)
40. https://www.csirt.gov.sk/doc/MFSRVzdelavanie/02Vzdelavanie2014/Studijne\_materialy/Stud\_2014\_02\_IT\_IB\_ucitelia.pdf [↑](#footnote-ref-40)
41. http://www.csirt.gov.sk/aktualne-7d7.html?id=120 [↑](#footnote-ref-41)
42. Uvedené mechanizmy je možné nahradiť ekvivalentnými mechanizmami v prípade, že ich súčasťou budú výstupy špecifikované nižšie. [↑](#footnote-ref-42)
43. Prípadne rezortným/sektorovým alebo národným CSIRT tímom. [↑](#footnote-ref-43)
44. https://www.csirt.gov.sk/doc/MFSRVzdelavanie/02Vzdelavanie2014/Studijne\_materialy/Stud\_2014\_02\_veduci.pdf [↑](#footnote-ref-44)