Odbor riadenia kybernetickej a informačnej bezpečnosti
Verzia 1.0 | kyberbezpecnost@mirri.gov.sk | august 2023

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Definovanie technických a procesných nástrojov a postupov na splnenie bezpečnostného minima

Obsah

Obsah 2
1 Správa dokumentu 3
2 Úvod 4
2.1 Účel dokumentu 4
2.2 Rozsah platnosti 4
3 Skratky a definície 5
3.1 Súvisiace legislatívne akty 6
4 Organizačné opatrenia 7
5 Technické opatrenia 9
6 Zoznam rolí a ich oprávnení 15

1 Správa dokumentu

Tento dokument je metodickým materiálom slúžiacim pre potreby orgánov verejnej moci, ktorý nie je povinný na použitie a ani nie je záväzný. Dokument je poskytnutý voľne a bezplatne na využitie podľa potrieb konkrétnej organizácie.

Vytvorený dokument je možné použiť i pre potreby vzdelávania pracovníkov organizácií v oblasti kybernetickej a informačnej bezpečnosti.

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

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

MIRRI si vyhradzuje právo na zmenu/úpravu predmetného dokumentu alebo čiastkových textov a tabuliek, a to v potrebnom rozsahu vrátane zmien verzií dokumentov. Dokument je pilotným projektom v rámci Reformy Štandardizácia technických a procesných riešení kybernetickej a informačnej bezpečnosti (Plán obnovy a odolnosti).

2 Úvod

2.1 Účel dokumentu

Bezpečnostné minimum je definované ako minimálny bezpečnostný základ, ktorý je potrebné implementovať pred samotným zaradením (identifikáciou a klasifikáciou) OVM do jednotlivých kategórií (kategória I, kategória II, kategória III) podľa vyhlášky č. 179/2020 Z. z.

Cieľom je, aby boli tieto minimálne požiadavky (bezpečnostné minimum) identifikované a implementované bezodkladne, aby bola dosiahnutá minimálna požadovaná úroveň kybernetickej odolnosti danej organizácie (OVM).

Bezpečnostné minimum pozostáva z organizačných opatrení (definovanie a schválenie základných procesov riadenia KIB) a technických opatrení (návrh minima technických opatrení – bez uvedenia konkrétnych produktov). Výber opatrení je nastavený s cieľom pokryť implementovanými bezpečnostnými opatreniami najpravdepodobnejšie riziká, ktoré sú identifikovateľné pre všetky kategórie OVM bez vykonania analýzy rizík.

2.2 Rozsah platnosti

Tento dokument je platný pre všetkých zamestnancov organizácie a tiež všetky relevantné tretie strany.

3 Skratky a definície

Špecialis*ta KIB*: súhrnný názov pre zamestnancov VS zabezpečujúci činnosti v oblasti informačnej a kybernetickej bezpečnosti (napr. bezpečnostní manažéri, bezpečnostní architekti, administrátori bezpečnostných systémov, špecialisti manažmentu IT rizík, audítori bezpečnosti informačných systémov, bezpečnostní analytici, kryptológovia či vyšetrovatelia bezpečnostných incidentov).

Manažér kybernetickej bezpečnosti (MKIB): označenie konkrétneho zamestnanca, ktorý riadi stratégiu kybernetickej bezpečnosti organizácie a jej implementáciu s cieľom zabezpečiť, aby digitálne systémy, služby a aktíva boli primerane zabezpečené a chránené.

Vyhláška č. 179/2020 Z. z.: Vyhláška č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy.

Segmentácia siete: rozdelenie siete OVM na menšie časti, pričom platí zásada, že segmentácia má znížiť riziko rýchleho rozšírenia škodlivého kódu alebo vírusu, alebo prekaziť, prípadne sťažiť pohyb útočníka po sieti s cieľom získať informácie , vykonať škodlivú aktivitu alebo spustiť škodlivý kód.

Šifrovanie: šifrovanie dostatočne silnou schválenou technikou v aktuálnom období považovanou za dostatočne silné bezpečnostné opatrenie na zašifrovanie súborov, prípadne celých diskových partícií (diskov).

Antimalware: riešenie alebo aplikácia, ktorá monitoruje súbory alebo procesy na úrovni operačného systému s cieľom zabrániť infiltrácii škodlivého kódu (všeobecne označovaného malware).

Antispam: riešenie alebo aplikácia, ktorá je inštalovaná na emailovom serveri alebo je v niektorých prípadoch súčasťou emailového klienta na pracovnej stanici s cieľom zabrániť šíreniu nevyžiadanej pošty (spam).

Hostname: označenie počítača, servera alebo iného zariadenia v sieti, prostredníctvom ktorého je v sieti identifikovateľné.

IP adresa: jedinečná adresa, prostredníctvom ktorej komunikuje zariadenie v sieti. Táto je spravidla označovaná štvorčíslím oddeleným bodkami, pričom číslovanie je v rozmedzí 0-255.

Protokol SSL/https: protokol, ktorý je zabezpečený šifrovaním tak, aby informácie boli čitateľné len pre komunikujúce strany (spravidla web prehliadač na pracovnej stanici a server sprostredkujúci obsah web stránky).

Firewall: špecializované zariadenie v sieti alebo programová súčasť servera alebo sieťového prvku (napríklad smerovač), umiestnené spravidla na rozhraní siete s internetom, ktoré rieši zabezpečenie sieťovej prevádzky filtrovaním alebo jej blokovaním (ak sa jedná o nepovolený obsah). Jeho funkcionalita býva podľa typu firewallu rozšírená o ďalšie funkcie.

Smerovač (alebo angl. Router): špecifické sieťové zariadenie zapojené v uzloch sietí, ktorého úlohou je smerovanie sieťovej prevádzky medzi komunikujúcimi stranami (počítač, server, sieťová tlačiareň a pod.).

Segmentácia siete: rozdelenie internej siete organizácie na menšie sektory alebo zóny (podsiete).

OVM: orgán verejnej moci.

KIB: kybernetická a informačná bezpečnosť.

IS: informačný systém.

OS: operačný systém.

3.1 Súvisiace legislatívne akty

Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.
Vyhláška č. 164/2018 Z. z., ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby).
Vyhláška č. 164/2018 Z. z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov.
Vyhláška č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.
Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov.
Vyhláška č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy.

4 Organizačné opatrenia

OVM musí mať prijaté, schválené a implementované v praxi nasledovné riadiace dokumenty a smernice:

- Bezpečnostná politika (riadiaci dokument),
- Smernica o informačnej a kybernetickej bezpečnosti (viď. vzor smernica), ktorá obsahuje minimálne nasledovné zásady:
  a) Bezpečnostné zásady a opatrenia pre oblasť **používanie IS (používateľ),**
  b) Bezpečnostné zásady a opatrenia pre oblasť **riadenie incidentov**,
  c) Bezpečnostné zásady a opatrenia pre oblasť **zálohovanie**,
  d) Bezpečnostné zásady a opatrenia pre oblasť **ochrana osobných údajov,**
  e) Bezpečnostné zásady a opatrenia pre oblasť **riadenie aktív**.
- Riadenie aktív (Katalóg aktív, Klasifikácia informácií a kategorizácia sietí a informačných systémov, vlastníci aktív).

Implementácia smerníc a riadiacich dokumentov v praxi znamená minimálne nasledovné:

1. Zástupca OVM (špecialista KIB, respektíve MKIB, ak je stanovený) vytvorí daný dokument v súlade s danou štruktúrou v nadväznosti na odsek vyššie – organizačné opatrenia (viď „vzor dokumentu Politika“, viď „vzor dokumentu Smernica“, viď „vzor dokumentu Katalóg aktív“), dokument je dostupný na portáli JMR.

2. Zástupca OVM (špecialista KIB, respektíve MKIB, ak je stanovený) skontroluje štruktúru a obsah dokumentu, ktorý musí obsahovať minimálne náležitosti uvedené v predchádzajúcom odseku (Organizačné opatrenia).

3. Štatutárny zástupca OVM schváli uvedené dokumenty, OVM dokumenty zaradí do svojej evidencie dokumentov (v prípade, že OVM má ISO 9001, dokumenty zaradí do dokumentovej štruktúry podľa požiadaviek ISO 9001).

4. Zástupca OVM (špecialista KIB, respektíve MKIB, ak je stanovený) preukázateľne (proti podpisu) poučí zamestnancov o nových schválených dokumentoch a riadiacich aktoch a upozorní na ich dodržiavanie, pričom podmienky pre zamestnancov musia byť vytvorené tak, aby im zásady uvedené v dokumentoch umožnili dodržiavať (napríklad uzamykateľné skrine alebo zásuvky pre dokumenty s citlivými informáciami alebo osobnými údajmi).

5. Na základe metrík uvedených v dokumentoch (podľa vzorov) bude zástupca OVM (špecialista KIB, respektíve MKIB, ak je stanovený) merať úroveň implementácie procesov zavedených schválením uvedených interných riadiacich aktov.

Katalóg aktív a riadenie aktív podľa uvedenej smernice:

Zástupca OVM (špecialista KIB) je povinný vyplniť, viesť a aktualizovať katalóg aktív, pričom:

1. Zástupca OVM (špecialista KIB, respektíve MKIB ak je stanovený) si v dokumente Katalóg aktív vyplní evidenciu informačných systémov a jemu prislúchajúcich informačných aktív a následne bude priebežne evidenciu udržiavať aktualizovanú, pričom evidencia obsahuje aj aktíva podľa prílohy č. 1 k vyhláške č. 179/2020 Z. z. najmä zoznam serverov (vrátane OS, hostname, IP adries, licencií, administrátora), zoznam pracovných staníc (vrátane OS, hostname, IP adries používateľa), zoznam aktívnych sieťových a bezpečnostných prvkov (vrátane OS, hostname, IP adries, licencií, administrátora), topológiu siete, zoznam privilegovaných prístupov, zoznam používateľských prístupov, zoznam zakúpených licencií.

2. V zozname informačných systémov určí kritickosť informačného systému na základe určenia dostupnosti, dôvernosti a integrity spracúvaných údajov.

3. OVM začne pracovať s klasifikovanými dokumentami podľa šablóny (vzoru) časti smernice definujúcej klasifikáciu aktív a aplikovať príslušné opatrenia.

4. V zozname informačných systémov určí kategóriu informačných systémov na základe kritérií uvedených v Vyhláške č. 362/2018 a Vyhláške č. 179/2020 (kategória I, kategória II, kategória III).
5. Ďalšie bezpečnostné opatrenia sa uplatňujú pre daný informačný systém podľa kategórie, do ktorej bol zaradený v predchádzajúcom bode. Tieto opatrenia nie sú predmetom bezpečnostného minima.

5 Technické opatrenia

OVM musí mať implementované nasledovné technické a technologické opatrenia:

1. Pre všetky servery a pracovné stanice:
    - Daný operačný systém je podporovaný výrobcom, ktorý teda vytvára a sprístupňuje bezpečnostné aktualizácie (security patch) po celú dobu prevádzky servera alebo pracovnej stanice.
    - Automatické inštalovanie bezpečnostných záplat OS je aktivované a uplatňuje sa.
    - Antivírový software je inštalovaný a aktivovaný (beží, pričom tento má zapnuté automatické aktualizácie – priebežná aktualizácia).

2. Pre všetky servery - opatrenia uvedené v bode č. 1, vrátane:
    - Antimalware riešenie (ak nie je súčasťou antivírového riešenia, pričom tento má zapnuté automatické aktualizácie – priebežná aktualizácia).
    - Aktivovanie (povolenie) len tých služieb (tzv. services), ktoré sú nevyhnutné pre chod/funkcionalitu daného IS/servera.
    - Aktívny firewall (pokiaľ nie je prekážkou pri funkcionalite servera alebo IS alebo služby).
    - Zapnuté zálohovanie (ukladanie záloh na externé sieťové úložisko (NAS, viď. sieťová bezpečnosť)).

3. Pre emailové servery - opatrenia uvedené v bode č. 1 a 2, a musí byť aplikované:
    - V prípade, že OVM má inštalovaný vlastný emailový server, musí mať tento inštalovaný antispam software, alebo antispam riešenie (pričom tento má zapnuté automatické aktualizácie – priebežná aktualizácia).
    - V prípade, že OVM prevádzkuje emailový server prostredníctvom inej spoločnosti (napríklad web hosting), musí mať prevádzkované riešenie inštalovaný antispam software, alebo antispam riešenie (pričom tento má zapnuté automatické aktualizácie – priebežná aktualizácia).

4. Pre web servery - opatrenia uvedené v bode č. 1 a 2 (Technické opatrenia), a musí byť aplikované:
    - Web server OVM má pre zobrazovanie informácií zapnutý výlučne protokol SSL/https.
    - Web server OVM má aktivovanú základnú ochranu vstupov – ošetrenie vstupov na chybu spôsobujúcu zraniteľnosť servera - ak je aplikovateľné (napríklad formulár).

5. Pre všetky pracovné stanice - opatrenia uvedené v bode č. 1, a musí byť aplikované:
    - Inštalovaný antispam software, alebo antispam riešenie (ak nie je súčasťou antivírového riešenia, pričom tento má zapnuté automatické aktualizácie – priebežná aktualizácia).
    - Zapnutý personálny firewall.
    - Zapnuté šifrovanie pevného disku stanice, v prípade, že je pracovná stanica mobilná (notebook) – šifrovací nástroj sa zapína pri inštalácii operačného systému, alebo pri jeho aktivovaní alebo počas prevádzky (potrebné administrátorské privilégiá.
    - Zapnuté zálohovanie (ukladanie pracovných dokumentov na externé sieťové úložisko (NAS, alebo externé USB disky, viď. sieťová bezpečnosť)).

6. Sieťová bezpečnosť:
    OVM musí mať v rámci svojho riešenia usporiadania a topológie vnútornej siete a jej pripojenia na internet minimálne aplikované nasledovné:

- Automatické inštalovanie bezpečnostných záplat OS pre všetky aktívne sieťové prvky (switch, router, wifi router, wifi AP (access point), firewall a pod.), v prípade, že je zariadenie v správe poskytovateľa služby pripojenia na internet, musí túto funkcionalitu garantovať poskytovateľ (optimálne v obchodných alebo zmluvných podmienkach).
- Aktivovaný firewall, nasadený minimálne na perimetri siete OVM a siete internet (na prestupe do internetu), aktivovaná paranoidná politika filtrovania.
- Šifrovanie na pevných diskoch (HDD) na sieťových úložiskách – NAS (v prípade, že OVM používa externé sieťové úložisko NAS na ukladanie záloh alebo pracovných dokumentov).
- Šifrovanie na HDD na externých USB úložiskách (v prípade, že OVM používa externé sieťové úložisko NAS na ukladanie záloh alebo pracovných dokumentov).

7. Všeobecne musí byť ďalej aplikované:
   - OVM musí mať zavedené (aplikované) riadenie prístupových práv. Toto obsahuje minimálne nasledovné zásady:
     a) jedinečné používateľské kontá (každý používateľ má jedinečné prístupové konto do pracovnej stanice alebo informačného systému, pričom zdieľanie (spoločné používanie jedného konta) je zakázané),
     b) privilegované používateľské práva (tzv. administrátorské oprávnenia – možnosť zasahovať do operačného systému, možnosť inštalovať alebo odinštalovať aplikácie, alebo zastavovať/spúšťať systémové procesy operačného systému) sú aktívne len pre administrátora informačných systémov alebo sietí, teda nie pre používateľov alebo manažment OVM,
     c) na bežnú administratívnu prácu sa používajú iba neprivilegované prístupové práva.
   - Vzdialené prístupy do siete OVM sú povoľované len pre nevyhnutné pozície/role OVM, ktoré sú schválené štatutárom OVM.
   - Vzdialené prístupy do siete OVM sú realizované cez VPN (virtual private network – šifrované pripojenie vzdialenej stanice cez šifrovaný kanál).
   - Pre administrátorské vzdialené prístupy je zapnuté šifrovanie sieťového prenosu.
   - OVM má implementované aspoň základné oddelenie sieťových segmentov (segmentácia siete), teda sieť je rozdelená na používateľskú a serverovú časť, informačné systémy sú na oddelených segmentoch siete OVM.
   - V prípade, že OVM využíva cloudové služby (napríklad MS office 365), musí byť vykonaná klasifikácia informácií, ktoré sa do úložiska alebo služby cloud ukladajú alebo sa v nej spracúvajú, pričom najcitlivejšie informácie (prísne chránené) sa z tejto služby vynímajú (je zakázané ich v cloudových službách spracúvať).

Príloha č. 1: Tabuľka opatrení pre dosiahnutie bezpečnostného minima

Kategória opatrení	Opatrenie	Obsah opatrenia/detail	Podkategória	Zodpovedný za realizáciu opatrenia	Poznámka
Organizačné opatrenia	Bezpečnostná politika (riadiaci dokument)			Zástupca OVM (špecialista KIB alebo MKIB)	
	Smernica o informačnej a kybernetickej bezpečnosti	Bezpečnostné zásady a opatrenia pre oblasť **používanie IS** (používateľ)		Zástupca OVM (špecialista KIB alebo MKIB)	
		Bezpečnostné zásady a opatrenia pre oblasť **riadenie incidentov**		Zástupca OVM (špecialista KIB alebo MKIB)	
		Bezpečnostné zásady a opatrenia pre oblasť **zálohovanie**		Zástupca OVM (špecialista KIB alebo MKIB)	
		Bezpečnostné zásady a opatrenia pre oblasť **ochrana osobných údajov**		Zástupca OVM (špecialista KIB alebo MKIB)	
		Bezpečnostné zásady a opatrenia pre oblasť **riadenie aktív**		Zástupca OVM (špecialista KIB alebo MKIB)	
	Riadenie aktív.	Katalóg aktív		Zástupca OVM (špecialista KIB alebo MKIB)	
Technické opatrenia	Servery a pracovné stanice	Daný operačný systém je podporovaný výrobcom		Zástupca OVM (špecialista KIB alebo MKIB)	
		Automatické inštalovanie bezpečnostných záplat OS		Zástupca OVM (špecialista KIB alebo MKIB)	
		Antivírový software		Zástupca OVM	

				(špecialista KIB alebo MKIB)	
	Servery	Antimalware riešenie		Zástupca OVM (špecialista KIB alebo MKIB)	
		Aktivovanie (povolenie) len nevyhnutných služieb		Zástupca OVM (špecialista KIB alebo MKIB)	
		Aktívny firewall		Zástupca OVM (špecialista KIB alebo MKIB)	
		Zapnuté zálohovanie		Zástupca OVM (špecialista KIB alebo MKIB)	
	E-mailové servery	Antispam software alebo antispam riešenie		Zástupca OVM (špecialista KIB alebo MKIB)	
	Web servery	protokol SSL/https		Zástupca OVM (špecialista KIB alebo MKIB)	
		Základná ochrana formulárov - ošetrenie vstupov		Zástupca OVM (špecialista KIB alebo MKIB)	
	Pracovné stanice	Antispam software alebo antispam riešenie		Zástupca OVM (špecialista KIB alebo MKIB)	
		Zapnutý personálny firewall		Zástupca OVM (špecialista KIB alebo MKIB)	
		Zapnuté šifrovanie pevného disku stanice		Zástupca OVM (špecialista	

				KIB alebo MKIB)	
		Zapnuté zálohovanie		Zástupca OVM (špecialista KIB alebo MKIB)	
	Sieťová bezpečnosť	Automatické inštalovanie bezpečnostných záplat		Zástupca OVM (špecialista KIB alebo MKIB)	
		Aktivovaný firewall, nasadený minimálne na perimetri siete OVM		Zástupca OVM (špecialista KIB alebo MKIB)	
		Šifrovanie na pevných diskoch (HDD) na sieťových úložiskách – NAS		Zástupca OVM (špecialista KIB alebo MKIB)	
		Šifrovanie na HDD na externých USB úložiskách		Zástupca OVM (špecialista KIB alebo MKIB)	
	Všeobecne	Riadenie prístupových práv	jedinečné používateľské kontá	Zástupca OVM (špecialista KIB alebo MKIB)	
			privilegované používateľské práva sú aktívne len pre administrátora	Zástupca OVM (špecialista KIB alebo MKIB)	
			na bežnú administratívnu prácu sa používajú iba neprivilegované prístupové práva	Zástupca OVM (špecialista KIB alebo MKIB)	
		Vzdialené prístupy do siete OVM sú povoľované len pre nevyhnutné pozície/role		Zástupca OVM (špecialista KIB alebo MKIB)	
		Vzdialené prístupy do siete OVM sú realizované cez VPN		Zástupca OVM (špecialista	

				KIB alebo MKIB)	
		Pre administrátorské vzdialené prístupy je zapnuté šifrovanie sieťového prenosu		Zástupca OVM (špecialista KIB alebo MKIB)	
		Základné oddelenie sieťových segmentov		Zástupca OVM (špecialista KIB alebo MKIB)	

6 Zoznam rolí a ich oprávnení

Špecialista KIB – zodpovedný za návrh, implementáciu a monitoring (kontrolu dodržiavania) bezpečnostných požiadaviek. V prípade, že v OVM nie je určený administrátor, špecialista KIB inštaluje bezpečnostné záplaty na operačných systémoch, serverov alebo pracovných staníc. Je taktiež zodpovedný za prideľovanie prístupových práv a ich riadenie (odoberanie, zmena), za požadovanú zmenu konfigurácií informačných systémov, serverov, aktívnych sieťových a bezpečnostných prvkov, externých sieťových úložísk, tlačiarní alebo pracovných staníc (s cieľom zvýšenia informačnej bezpečnosti v OVM, resp. jej kybernetickej odolnosti). Ďalej je zodpovedný za vyplnenie a aktualizáciu katalógu aktív OVM.

Štatutárny zástupca OVM – schvaľuje riadiace akty, je zodpovedný za dodržiavanie bezpečnostných požiadaviek v organizácii a za súlad s legislatívnymi požiadavkami.