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

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Metodika pre vznik odborných bezpečnostných pracovísk v prostredí verejnej správy

Obsah

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 výstupom v rámci Reformy Štandardizácia technických a procesných riešení kybernetickej a informačnej bezpečnosti (Plán obnovy a odolnosti).

2 Úvod

2.1 Účel dokumentu

Účelom tohto dokumentu je poskytnúť metodický materiál pre vytvorenie adekvátne personálne a technicky vybavených odborných pracovísk, ktoré majú byť kreované v rámci organizačnej štruktúry príslušného orgánu verejnej moci, určených pre riadenie kybernetickej bezpečnosti a súvisiacich procesov, bezpečnostný monitoring sietí a informačných systémov, implementáciu bezpečnostných opatrení, riadenie rizík, riešenie kybernetických bezpečnostných incidentov a podobne, a to v diferenciácii pre jednotlivé OVM podľa ich zaradenia do jednotlivých kategórií OVM, ako sú definované nižšie v tomto dokumente.

Úlohou týchto odborných pracovísk bude okrem vykonávania preventívnych a reaktívnych opatrení v oblasti ich pôsobnosti aj spolupráca a poskytovanie relevantných informácií o kybernetických incidentoch národnej jednotke CSIRT a vládnej jednotke CSIRT.

Jednou z hlavných úloh dokumentu je vypracovať štruktúru odborných bezpečnostných pracovísk v kontexte budovania celonárodného riadenia incidentov kybernetickej bezpečnosti, čím budú pokryté preventívne a reaktívne služby pre podsektor ISVS.

Tento dokument reflektuje metodické usmernenia definujúce požiadavky pri vytváraní odborných bezpečnostných pracovísk v zmysle požiadaviek zákona o kybernetickej bezpečnosti a súvisiacich vykonávacích predpisov[1] (vrátane požiadaviek na odbornosť jednotlivých členov bezpečnostných pracovísk, stanovenie minimálnych požiadaviek na technické vybavenie odborných pracovísk a definovania priamo súvisiacich služieb), s cieľom dosiahnutia primeranej kybernetickej odolnosti jednotlivých OVM, ako aj včasných a efektívnych reakcií OVM na kybernetické bezpečnostné incidenty v prostredí verejnej správy.

2.2 Definície a skratky

- IS – informačný systém
- ISVS – informačné systémy verejnej správy
- SR – Slovenská republika
- EÚ – Európska únia
- UPVS - ústredný portál verejnej správy
- HW – hardvér
- SW – softvér
- OS – operačný systém
- FW – firewall
- CMDB - databáza správy konfigurácie
- KB – kybernetická bezpečnosť
- OVM – orgány verejnej moci
- MIRRI - Ministerstvo investícií, regionálneho rozvoja a informatizácie
- NBÚ - Národný bezpečnostný úrad

[1] Vrátane návrhu znenia vyhlášky Národného bezpečnostného úradu, ktorou sa ustanovujú znalostné štandardy v oblasti kybernetickej bezpečnosti, aktuálne dostupné na https://www.slov-lex.sk/legislativne-procesy/-/SK/dokumenty/LP-2022-323

- CSIRT - jednotka pre riešenie kybernetických bezpečnostných incidentov/Computer Security Incident Response Team
- BP – bezpečnostné pracovisko
- IDM – správa identít
- PAM – správa privilegovaných prístupov
- SIEM - security incident and event management
- JISKB - jednotný informačný systém kybernetickej bezpečnosti
- BP – bezpečnostné pracovisko.
- IKT – informačné a komunikačné technológie
- IT – informačné technológie
- BCP - plán kontinuity činností
- DRP – plán obnovy po katastrofe
- BIA - analýza vplyvu na podnikanie
- MKB – manažér kybernetickej a informačnej bezpečnosti
- Zákon o kybernetickej bezpečnosti – zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov, v znení neskorších predpisov.

3 Prehľad rolí v oblasti kybernetickej bezpečnosti

Táto kapitola obsahuje základný popis pracovných rolí, ktoré budú priradené k jednotlivým bezpečnostným pracoviskám. Táto kapitola vychádza z Vyhlášky NBÚ č. 492/2022 Z. z., ktorou sa ustanovujú znalostné štandardy v oblasti kybernetickej bezpečnosti. Sú v nej uvedené detailné popisy jednotlivých pracovných rolí.

Pracovné role nevyhnutné pre vznik a prevádzku bezpečnostných pracovísk boli identifikované nasledovne:

Manažér kybernetickej a informačnej bezpečnosti

Pracovná rola	Manažér kybernetickej a informačnej bezpečnosti
Krátky popis	Riadi stratégiu kybernetickej bezpečnosti organizácie a jej implementáciu s cieľom zabezpečiť, aby digitálne systémy, služby a aktíva boli primerane zabezpečené a chránené.
Misia	Definuje, udržiava a komunikuje víziu, stratégiu, riziká, politiku, ľudské zdroje a postupy kybernetickej bezpečnosti. Riadi implementáciu politiky kybernetickej bezpečnosti v celej organizácii. Zabezpečuje výmenu informácií s externými regulačnými orgánmi a odbornými orgánmi. Má na starosti procesy riešenia kybernetických bezpečnostných incidentov.

Špecialista pre riešenie kybernetických incidentov

Pracovná rola	Špecialista pre riešenie kybernetických incidentov
Krátky popis	Monitoruje stav kybernetickej bezpečnosti organizácie, rieši incidenty počas kybernetických útokov a zabezpečuje nepretržitú prevádzku IKT systémov.
Misia	Monitoruje a hodnotí stav kybernetickej bezpečnosti systémov. Analyzuje, vyhodnocuje a zmierňuje vplyv incidentov kybernetickej bezpečnosti. Identifikuje hlavné príčiny kybernetických incidentov. Podľa plánu reakcie na incidenty organizácie, obnovuje funkčnosť systémov a procesov do prevádzkového stavu, zhromažďuje dôkazy a dokumentuje prijaté opatrenia.

Špecialista pre riadenie súladu

Pracovná rola	Špecialista pre riadenie súladu
Krátky popis	Riadi dodržiavanie súladu s normami, právnymi a regulačnými rámcami súvisiacimi s kybernetickou bezpečnosťou na základe stratégie organizácie a na základe zákonných požiadaviek.
Misia	Dohliada a zabezpečuje súlad s právnymi, regulačnými rámcami a politikami týkajúcimi sa kybernetickej bezpečnosti a údajov v súlade so stratégiou organizácie a so zákonnými požiadavkami. Prispieva k činnostiam organizácie súvisiacim s ochranou údajov. Poskytuje poradenstvo ohľadom právnych aspektov pri vývoji procesov riadenia kybernetickej bezpečnosti organizácie a odporúčaných nápravných stratégií/riešení na zabezpečenie súladu.

Špecialista pre vyšetrovanie kybernetických incidentov

Pracovná rola	Špecialista pre vyšetrovanie kybernetických incidentov
Krátky popis	Zhromažďuje, spracúva, analyzuje údaje a informácie s cieľom vytvárať použiteľné správy o kybernetických hrozbách a šíriť ich cieľovým zainteresovaným stranám.
Misia	Riadi životný cyklus šírenia informácií o kybernetických hrozbách vrátane zhromažďovania informácií o kybernetických hrozbách, analýzy a vytvárania použiteľných správ a ich šírenia medzi zainteresované strany v oblasti bezpečnosti na taktickej, operačnej a strategickej úrovni. Identifikuje a monitoruje taktiky, techniky a postupy používané aktérmi kybernetických hrozieb a ich trendy, sleduje aktivity aktérov hrozieb a sleduje, ako môžu nekybernetické bezpečnostné udalosti ovplyvniť kybernetickú bezpečnosť.

Architekt kybernetickej bezpečnosti

Pracovná rola	Architekt kybernetickej bezpečnosti
Krátky popis	Plánuje a navrhuje špecifické riešenia kybernetickej bezpečnosti (infraštruktúry, systémov, aktív, softvérov, hardvéru a služieb) a kontroly kybernetickej bezpečnosti.
Misia	Navrhuje riešenia založené na princípoch zabezpečenia už od návrhu po implementáciu. Vytvára a neustále zdokonaľuje modely architektúry a vyvíja vhodnú dokumentáciu a špecifikácie kybernetickej bezpečnosti. Koordinuje bezpečný vývoj, integráciu a údržbu komponentov kybernetickej bezpečnosti v súlade s právnymi normami a ďalšími súvisiacimi požiadavkami organizácie.

Audítor kybernetickej bezpečnosti

Pracovná rola	Audítor kybernetickej bezpečnosti
Krátky popis	Vykonávanie auditov kybernetickej bezpečnosti v ekosystéme organizácie. Zabezpečenie súladu so zákonnými, regulačnými a politikou informačnej bezpečnosti, bezpečnostnými požiadavkami, odvetvovými normami a osvedčenými postupmi.
Misia	Vykonáva nezávislé preskúmania informačnej bezpečnosti s cieľom posúdiť účinnosť procesov a kontrolných mechanizmov a celkový súlad s právnymi a regulačnými rámcami organizácie. Hodnotí, testuje a overuje produkty súvisiace s kybernetickou bezpečnosťou (systémy, hardvér, softvér a služby), funkcie a politiky, čím zabezpečuje súlad s usmerneniami, normami a predpismi.

Lektor kybernetickej bezpečnosti

Pracovná rola	Lektor kybernetickej bezpečnosti
Krátky popis	Zlepšuje znalosti, zručnosti a kompetencie zamestnancov v oblasti kybernetickej bezpečnosti.
Misia	Navrhuje, vyvíja a realizuje programy zvyšovania povedomia, odbornej prípravy a vzdelávania v oblasti kybernetickej bezpečnosti a ochrany údajov. Používa vhodné metódy, techniky a nástroje výučby a odbornej prípravy na sprostredkovanie a zvyšovanie kultúry, schopností, znalostí a zručností ľudských zdrojov v oblasti kybernetickej bezpečnosti. Propaguje význam kybernetickej bezpečnosti a upevňuje jej postavenie v organizácii.

Špecialista kybernetickej bezpečnosti

Pracovná rola	Špecialista kybernetickej bezpečnosti
Krátky popis	Vyvíjať, zavádzať a prevádzkovať riešenia kybernetickej bezpečnosti (systémy, prostriedky, softvér, kontroly a služby) v infraštruktúrach a produktoch.
Misia	Zabezpečuje technický vývoj, integráciu, testovanie, implementáciu, prevádzku, údržbu, monitorovanie a podporu riešení kybernetickej bezpečnosti. Zabezpečuje dodržiavanie špecifikácií a požiadaviek na súlad, zabezpečuje správny výkon a rieši technické problémy požadované v riešeniach organizácie súvisiacich s kybernetickou bezpečnosťou (systémy, aktíva, softvér, kontroly a služby), infraštruktúrach a produktoch.

Výskumný pracovník v oblasti kybernetickej bezpečnosti

Pracovná rola	Výskumný pracovník v oblasti kybernetickej bezpečnosti
Krátky popis	Má na starosti výskum v oblasti kybernetickej bezpečnosti a zapracovanie výsledkov do riešení kybernetickej bezpečnosti.
Misia	Vykonáva základný a aplikovaný výskum a uľahčuje inovácie v oblasti kybernetickej bezpečnosti prostredníctvom spolupráce s inými zainteresovanými stranami. Analyzuje trendy a vedecké poznatky v oblasti kybernetickej bezpečnosti.

Špecialista riadenia rizík

Pracovná rola	Špecialista riadenia rizík
Krátky popis	Riadi riziká súvisiace s kybernetickou bezpečnosťou organizácie v súlade so stratégiou organizácie. Vyvíja, udržiava a komunikuje procesy a správy o riadení rizík.
Misia	Priebežne riadi (identifikuje, analyzuje, hodnotí, odhaduje, zmierňuje) riziká súvisiace s kybernetickou bezpečnosťou infraštruktúry, systémov a služieb IKT plánovaním, uplatňovaním, podávaním správ a oznamovaním výsledkov analýzy, hodnotenia a ošetrenia rizík. Stanovuje stratégiu riadenia rizík pre organizáciu a zabezpečuje, aby riziká zostali na prijateľnej úrovni pre organizáciu výberom zmierňujúcich opatrení a kontrolných mechanizmov.

Špecialista pre analýzu digitálnych stôp

Pracovná rola	Špecialista pre analýzu digitálnych stôp
Krátky popis	Zabezpečuje, aby vyšetrovanie kybernetických incidentov odhalilo všetky dôkazy na preukázanie škodlivej činnosti.
Misia	Spája údaje s fyzickými osobami, zachytáva, obnovuje, identifikuje a uchováva údaje vrátane prejavov, vstupov, výstupov a procesov skúmaných digitálnych systémov. Poskytuje analýzu, rekonštrukciu a interpretáciu digitálnych dôkazov na základe kvalitatívneho stanoviska. Predkladá nezaujatý kvalitatívny názor bez interpretácie výsledných zistení.

Tester kybernetickej bezpečnosti

Pracovná rola	Tester kybernetickej bezpečnosti
Krátky popis	Posudzovať účinnosť bezpečnostných kontrol, odhaľovať a využívať slabé miesta kybernetickej bezpečnosti organizácie a posudzovať ich kritickosť v prípade zneužitia.
Misia	Plánuje, navrhuje, implementuje a vykonáva činnosti penetračného testovania a útočné scenáre na vyhodnotenie účinnosti zavedených alebo plánovaných bezpečnostných opatrení. Identifikuje zraniteľnosti alebo zlyhania technických a organizačných kontrol, ktoré ovplyvňujú dôvernosť, integritu a dostupnosť produktov IKT (napr. systémov, hardvéru, softvéru a služieb). Má prehľad o aktuálnych hrozbách kybernetickej bezpečnosti.

Pracovník zodpovedný za koordináciu kybernetickej bezpečnosti

Pracovná rola	Manažér
Krátky popis	Porozumieť základným pojmom kybernetickej bezpečnosti, rizikám a nadobudnúť schopnosť analyzovať a integrovať požadovanú úroveň ochrany kybernetickej bezpečnosti.
Misia	Riadiaci zamestnanec, ktorý nie je IT manažérom alebo manažérom kybernetickej bezpečnosti a ktorý spravidla zodpovedá za príslušný proces, alebo skupinu procesov a v rámci nich zodpovedá aj za plnenie úloh v oblasti riadenia rizík kybernetickej bezpečnosti.

IT Manažér

Pracovná rola	IT Manažér
Krátky popis	Porozumieť významu, jednotlivým častiam, systému riadenia kybernetickej bezpečnosti. Zabezpečiť implementáciu a vyhodnocovanie účinnosti zavedených bezpečnostných opatrení.
Misia	Riadiaci zamestnanec organizačných jednotiek zodpovedných za poskytovanie IT služieb, návrh, implementáciu, obstaranie, prevádzku, údržbu a posudzovanie prostriedkov IKT. Zabezpečuje presadzovanie politiky kybernetickej bezpečnosti v organizácii.

4 Prehľad nástrojov kybernetickej bezpečnosti

Táto kapitola obsahuje stručný popis typov nástrojov kybernetickej bezpečnosti, ktoré sú potrebné pre vznik bezpečnostných pracovísk. Kapitola má nadväznosť na odborný materiál „Definovanie technických a procesných nástrojov a postupov na splnenie bezpečnostného minima“.
Nástroje sú rozdelené do nasledovných kategórií:

Bezpečnostné monitorovanie – Úlohou nástrojov na monitorovanie je zhromažďovať a analyzovať údaje o bezpečnostných udalostiach vyplývajúcich z aktivít v rámci organizácie, vylaďovať a zlepšovať pravidlá generujúce bezpečnostné výstrahy a následne skúmať indikátory potenciálne škodlivej činnosti, eskalovať incidenty alebo iniciovať reakcie.
Medzi bezpečnostné monitorovacie nástroje patrí SIEM, EDR, XDR a SOAR.

Hodnotenie a riadenie zraniteľnosti – Tieto nástroje vykonávajú hodnotenia hrozieb a zraniteľných miest v rámci IT prostredia, určujú odchýlky od prijateľných konfigurácií, bezpečnostnej politiky, posudzujú úroveň rizika a vyvíjajú a/alebo odporúčajú vhodné zmierňujúce protiopatrenia v prevádzkových a neprevádzkových situáciách.
Medzi nástroje patria: nástroje na správu a testovanie zraniteľností, nástroje na penetračné testovanie, nástroje na testovanie užívateľov a sociálne inžinierstvo.
Riadenie zmien – je štruktúrovaný proces na preskúmanie navrhovaných zmien IT systému alebo služieb. Tento proces prebieha pred implementáciou požadovanej zmeny v sieti organizácie, čím sa minimalizujú alebo eliminujú výpadky siete.
Nástroje: nástroje na správu aktív, nástroje na patch manažment, CMDB.

Detekcia a analýza hrozieb – pod detekciu hrozieb spadá analýza celého bezpečnostného ekosystému s cieľom identifikovať akúkoľvek škodlivú aktivitu, ktorá by mohla ohroziť sieť a fungovanie informačných systémov. Ak sa zistí hrozba, musí sa prijať opatrenie na jej zmiernenie alebo úplne odstránenie, aby sa hrozba riadne neutralizovala skôr, ako bude môcť zneužiť akékoľvek aktuálne zraniteľné miesta.
Nástroje: nástroje na detekciu škodlivého softvéru (firewall, antivírusové riešenia, antibot riešenia, antiransomware riešenia, antispam riešenia, ochrana pred prístupom na nežiaduce webové stránky).

Riadenie incidentov a reakcia - Proces riadenia bezpečnostných incidentov sa zvyčajne začína upozornením, že došlo k incidentu, a zapojením tímu reakcie na incidenty. Reakcia na incidenty je proces, ktorý umožňuje včasnú a efektívnu reakciu na kybernetické útoky. Proces reakcie na incident zahŕňa identifikáciu útoku, pochopenie jeho závažnosti a stanovenie priorít, vyšetrenie a zmiernenie útoku, obnovenie operácií a prijatie opatrení, aby sa zabezpečilo, že sa nebude opakovať.
Nástroje: nástroje na forenznú analýzu, nástroje na zastavenie a izoláciu potenciálne škodlivých kódov (FW, antivírus atď.), nástroje na elimináciu a nápravu incidentov, SIEM, IPS, IDS atď..

Ochrana údajov - Ochrana údajov je súbor postupov zameraných na ochranu údajov uložených v systéme. Ochrana údajov sa týka správy údajov, overovania dostupnosti, prevencie neoprávneného prístupu a zálohy/obnovy údajov v prípade ich straty. Ochrana údajov vyžaduje úsilie od všetkých zamestnancov, ktorí pracujú s citlivými údajmi.
Nástroje: Data discovery and classification, Data loss prevention, Encryption, Data Access governance, Database security, Tokenization, File integrity protection

Správa prístupov - identity manažment (IDM), zabezpečuje, že oprávnení ľudia – a iba autorizovaní ľudia – majú prístup k technologickým zdrojom, ktoré potrebujú na vykonávanie svojich pracovných funkcií.

Nástroje: nástroje na riadenie prístupu k údajom, nástroje na správu prístupov, nástroje na správu privilegovaného prístupu (PAM).

Správa aktív (asset management) - je proces kategorizácie, monitorovania a správy aktív organizácie. Správa aktív poskytuje rámec na dokumentáciu a správu životného cyklu každého aktíva od prvého použitia až po vyradenie aktíva a presuny medzi tým. Softvér na správu aktív umožňuje jednoducho zosúladiť inventár hardvéru a softvéru, vlastníkov a ich pridelených aktív a informácie o polohe na jednom mieste.
Nástroje: softvér na správu aktív

Governance, Risk management and Compliance (GRC) -Nástroje GRC sú nástroje, ktoré môžu podniky použiť na správu politík, hodnotenie rizík, riadenie prístupu používateľov a zefektívnenie dodržiavania predpisov.
Nástroje: nástroje na monitorovanie a správu rizík, nástroje na správu politík

5 Zoznam typov a špecifikácia bezpečnostných pracovísk

Bezpečnostné pracovisko je odborné pracovisko pre riadenie kybernetickej bezpečnosti a súvisiacich procesov, bezpečnostný monitoring sietí a informačných systémov, implementáciu bezpečnostných opatrení, riadenie rizík, riešenie kybernetických bezpečnostných incidentov a podobne. Pod bezpečnostným pracoviskom rozumieme logickú jednotku, ktorú tvorí viac spolupracujúcich oddelení, odborov a pod. Táto kapitola obsahuje vypracovanú podrobnú štruktúru odborných bezpečnostných pracovísk.
Nasledujúca tabuľka obsahuje jednoduchý prehľad základných parametrov pre 3 typy odborných bezpečnostných pracovísk:

Typy bezpečnostných pracovísk – prehľad

BP	Kompetencie	Počet rolí	Minimálna kapacita	Riadenie rizík	Bezpečnostné incidenty	Nahlasovanie incidentov
Typ A	Riadenie rizík kybernetickej bezpečnosti Bezpečnostný monitoring Implementácia bezpečnostných opatrení Riadenie incidentov Riadenie bezpečnosti sietí a IS Riadenie kryptografických opatrení Riadenie zraniteľností a záplat Riadenie kontinuity procesov Forenzná analýza, analýza malvéru, Výskum v oblasti kybernetickej bezpečnosti	12	25 pracovníkov	Identifikácia rizika Posúdenie rizika (pravdepodobnosť, dopad) Ošetrenia rizika Pravidelné preskúmavanie nápravných opatrení	24/7 monitorovanie a analyzovanie udalostí v sieťach a IS použitím nástrojov na monitorovanie bezpečnosti	zodpovedný pracovník nahlasuje kybernetické bezpečnostné incidenty do SK-CERT na NBÚ
Typ B	Riadenie rizík kybernetickej bezpečnosti Riadenie incidentov Riadenie bezpečnosti sietí a IS Riadenie zraniteľností a záplat Riadenie kontinuity procesov	2	2 pracovníci	Identifikácia rizika Posúdenie rizika (pravdepodobnosť, dopad) Ošetrenia rizika Pravidelné preskúmavanie nápravných opatrení	riešenie zistených kybernetických bezpečnostných incidentov a znižovanie ich následkov	MKB nahlasuje kybernetické bezpečnostné incidenty do SK-CERT na NBÚ
Typ C	Riadenie rizík kybernetickej bezpečnosti Riadenie incidentov Riadenie bezpečnosti sietí a IS Riadenie zraniteľností a záplat	2	1 pracovník	Identifikácia rizika Posúdenie rizika (pravdepodobnosť, dopad) Ošetrenia rizika	riešenie zistených kybernetických bezpečnostných incidentov a znižovanie ich následkov	pracovník zodpovedný za koordináciu KB nahlási bezpečnostný incident CSIRT alebo nadradenému

BP	Kompetencie	Počet rolí	Minimálna kapacita	Riadenie rizík	Bezpečnostné incidenty	Nahlasovanie incidentov
						orgánu a ten nahlasuje do CSIRT

Nasledujúce podkapitoly obsahujú karty s podrobným popisom parametrov pre vytvorenie adekvátne odborných a technicky vybavených odborných pracovísk v prostredí verejnej správy.

5.1 Bezpečnostné pracovisko pre OVM kategórie III– typ A

Bezpečnostné pracovisko – typ A	
Kompetencie	- Riadenie rizík kybernetickej bezpečnosti - Bezpečnostný monitoring - Implementácia bezpečnostných opatrení - Riadenie incidentov - Riadenie bezpečnosti sietí a IS - Riadenie kryptografických opatrení - Riadenie zraniteľností a záplat - Riadenie kontinuity procesov - Forenzná analýza, analýza malvéru, - Výskum v oblasti kybernetickej bezpečnosti
Požiadavky na obsadenie pozíciami definovaných špecialistov KBI	- Manažér kybernetickej bezpečnosti - Špecialista na riešenie bezpečnostných incidentov - Špecialista pre riadenie súladu - Špecialista pre vyšetrovanie kybernetických incidentov, - Architekt kybernetickej bezpečnosti, - Audítor kybernetickej bezpečnosti, - Lektor kybernetickej bezpečnosti, - Špecialista kybernetickej bezpečnosti, - Výskumný pracovník v oblasti kybernetickej bezpečnosti, - Špecialista riadenia rizík, - Špecialista pre analýzu digitálnych stôp. - Tester kybernetickej bezpečnosti.
Kapacita	- Minimum 25 pracovníkov
Riadení rizík v oblasti kybernetickej bezpečnosti	- Identifikácia rizika - Posúdenie rizika (pravdepodobnosť, dopad) - Ošetrenia rizika - Pravidelné preskúmavanie nápravných opatrení

	- Riadenie aktív (detailná evidencia aktív s automatizovaným nástrojom pre vyhľadávanie aktuálnych zraniteľností pre jednotlivé aktíva)
Riešenie bezpečnostného monitoringu a riadenia incidentov	- vypracované štandardy a postupy riešenia kybernetických bezpečnostných incidentov, - 24/7 monitorovanie a analyzovanie udalostí v sieťach a IS použitím nástrojov na monitorovanie bezpečnosti - zabezpečenie zberu relevantných informácií o identifikovaných kybernetických bezpečnostných incidentoch, - riešenie zistených kybernetických bezpečnostných incidentov a znižovanie ich následkov, - vyhodnocovanie spôsobu riešenia kybernetických bezpečnostných incidentov po ich vyriešení a prijatí bezpečnostných opatrení,
Nahlasovanie bezpečnostných incidentov (komunikačné väzby)	- zodpovedný pracovník nahlasuje kybernetické bezpečnostné incidenty do do SK-CERT na NBÚ
Minimálne hardvérové a softvérové vybavenie a minimálne opatrenia pre organizácie	- Pracovné stanice, nástroje na bezpečnostný monitoring (SIEM), nástroje na správu a testovanie zraniteľností, nástroje na penetračné testovanie, nástroje na školenie užívateľov používajúcich IS, nástroje na správu aktív, nástroje na patch manažment, nástroje na detekciu škodlivého softvéru (firewall, antivírusové riešenia, antibot riešenia, antiransomware riešenia, antispam riešenia, ochrana pred prístupom na nežiaduce webové stránky) nástroje na forenznú analýzu, nástroje na riadenie prístupu (IDM) a nástroje na riadenie privilegovaného prístupu (PAM), nástroje na ochranu údajov (data loss prevention), nástroje na kryptovanie. - Šírenie osvety o kybernetickej bezpečnosti (e-learnigy pre používateľov IS)
Legislatíva	- Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov a jeho vykonávacie predpisy. - Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov. - Vyhláška ÚPVII č. 179/2020 Z, z, ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy.
Politiky a smernice	- Bezpečnostná politika, - Bezpečnostná stratégia, - Riadenie rizík, - Riadenie bezpečnosti ľudských zdrojov,

	- Riadenie prístupových práv, - Riadenie tretích strán, - Riadenie bezpečnosti IS a sietí, - Riadenie aktív, klasifikácia informácií, kategorizácia IS a sietí - Riadenie bezpečnostných incidentov, - Riadenie fyzickej bezpečnosti, - Riadenie kryptografických opatrení, - Bezpečnostný monitoring - Bezpečný vývoj, - Riadenie zmien, - Riadenie kontinuity procesov (BCP, DRP, BIA), - Riadenie zálohovania, Riadenie zraniteľností a bezpečnostných záplat.

5.2 Bezpečnostné pracovisko pre OVM kategórie II – typ B

Bezpečnostné pracovisko – typ B	
Kompetencie	- Riadenie rizík kybernetickej bezpečnosti - Bezpečnostný monitoring - Riadenie incidentov - Riadenie bezpečnosti sietí a IS - Riadenie zraniteľností a záplat - Riadenie kontinuity procesov
Požiadavky na obsadenie pozíciami definovaných špecialistov KBI	- Manažér kybernetickej bezpečnosti - Špecialista na riešenie bezpečnostných incidentov
Kapacita	- Minimum 2 pracovníkov
Riadení rizík v oblasti kybernetickej bezpečnosti	- Identifikácia rizika - Posúdenie rizika (pravdepodobnosť, dopad) - Ošetrenia rizika - Pravidelné preskúmavanie nápravných opatrení - Riadenie aktív (detailná evidencia aktív)
Riešenie bezpečnostného monitoringu a riadenia incidentov	- vypracované štandardy a postupy riešenia kybernetických bezpečnostných incidentov, - riešenie zistených kybernetických bezpečnostných incidentov a znižovanie ich následkov, vyhodnocovanie spôsobu riešenia kybernetických bezpečnostných

	incidentov po ich vyriešení a prijatí bezpečnostných opatrení,
Nahlasovanie bezpečnostných incidentov (komunikačné väzby)	- MKB nahlasuje kybernetické bezpečnostné incidenty do do SK-CERT na NBÚ
Minimálne hardvérové a softvérové vybavenie a minimálne opatrenia pre organizácie	- Pracovné stanice, nástroje na monitoring siete,nástroje na identifikovanie zraniteľností, nástroje na školenie užívateľov používajúcich IS, nástroje na patch manažment, nástroje na detekciu škodlivého softvéru (firewall, antivírusové riešenia, antibot riešenia, antiransomware riešenia, antispam riešenia, ochrana pred prístupom na nežiaduce webové stránky) nástroje na riadenie prístupu, nástroje na šifrovanie pracovných staníc, nástroje na VPN (šifrovanie prenosu). - Šírenie osvety o kybernetickej bezpečnosti (e-learnig pre používateľov IS)
Legislatíva a smernice	- Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov a jeho vykonávacie predpisy. - Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov. - Vyhláška ÚPVII č. 179/2020 Z, z, ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy.
Politiky a smernice	- Bezpečnostná politika, - Riadenie rizík, - Riadenie prístupových práv, - Riadenie bezpečnosti IS a sietí, - Riadenie aktív, klasifikácia informácií, kategorizácia IS a sietí - Riadenie bezpečnostných incidentov, - Riadenie fyzickej bezpečnosti, - Riadenie zmien, - Riadenie kontinuity procesov (BCP, DRP, BIA), - Riadenie zálohovania.

5.3 Bezpečnostné pracovisko pre OVM kategórie I – typ C

Bezpečnostné pracovisko – typ C	
Kompetencie	- Riadenie rizík kybernetickej bezpečnosti - Riadenie incidentov - Riadenie bezpečnosti sietí a IS - Riadenie zraniteľností a záplat
Požiadavky na	- Pracovník zodpovedný za koordináciu KB

obsadenie pozíciami definovaných špecialistov KBI	- IT Manažér (môže pokryť aj pozíciu pracovníka zodpovedného za koordináciu KB)
Kapacita	- Minimum 1 pracovník
Riadení rizík v oblasti kybernetickej bezpečnosti	- Identifikácia rizika - Posúdenie rizika (pravdepodobnosť, dopad) - Ošetrenia rizika - Evidencia aktív
Riešenie bezpečnostného monitoringu a riadenia incidentov	- vypracované štandardy a postupy riešenia kybernetických bezpečnostných incidentov, - riešenie zistených kybernetických bezpečnostných incidentov a znižovanie ich následkov,
Nahlasovanie bezpečnostných incidentov (komunikačné väzby)	- Pracovník zodpovedný za koordináciu KB nahlási bezpečnostný incident CSIRT alebo nadradenému orgánu a ten nahlasuje do CSIRT
Minimálne hardvérové a softvérové vybavenie a minimálne opatrenia pre organizácie	- Pracovné stanice, nástroje na monitoring siete,nástroje na identifikovanie zraniteľností, nástroje, nástroje na patch manažment, nástroje na detekciu škodlivého softvéru (firewall*, antivírusové riešenia, antibot riešenia, antiransomware riešenia, antispam riešenia, ochrana pred prístupom na nežiaduce webové stránky) nástroje na riadenie prístupu, nástroje na šifrovanie pracovných staníc, nástroje na VPN (šifrovanie prenosu). - Šírenie osvety o kybernetickej bezpečnosti (e-learnigy pre používateľov IS)
Legislatíva a smernice	- - Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov a jeho vykonávacie predpisy. - Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov. - Vyhláška ÚPVII č. 179/2020 Z, z, ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy.
Politiky a smernice	- Bezpečnostná politika, - Riadenie rizík, - Riadenie prístupových práv, - Riadenie bezpečnosti IS a sietí, - Riadenie aktív, klasifikácia informácií, kategorizácia IS a sietí - Riadenie bezpečnostných incidentov, - Riadenie zmien, - Riadenie zálohovania.

*pozn: Obce využívajúce plnú funkcionalitu informačného systému DCOM (IS DCOM) vrátane správy koncových zariadení aktuálne spĺňajú všetky požiadavky na centrálne aplikačné riešenie, aplikačnú bezpečnosť a aj na zabezpečenie koncových zariadení (primárne PC a notebooky).

DataCentrum elektronizácie územnej samosprávy Slovenska (DEUS) je prevádzkovateľom nadrezortného informačného systému IS DCOM v zmysle zákona 305/2013 o eGovernmente.
V zmysle vyhlášky Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu 179/2020 je DEUS v zmysle §3, odsek (4) jedným z povinných subjektov na ktoré sú uplatňované bezpečnostné požiadavky príslušnej bezpečnostnej kategórie.