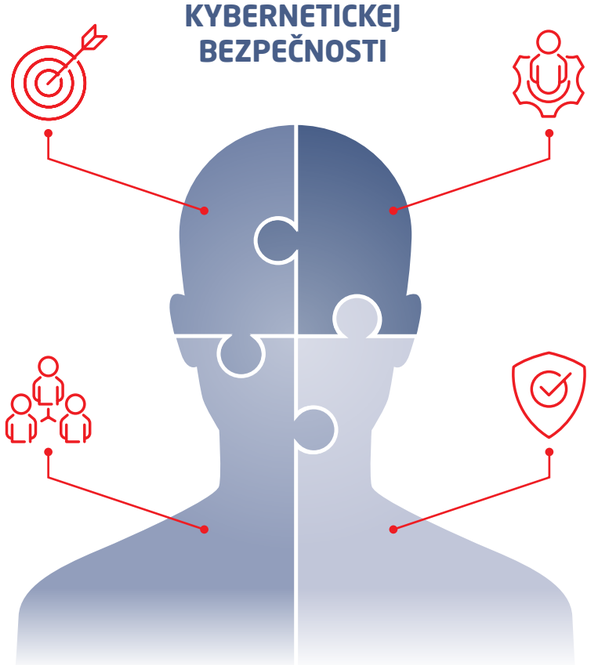
MANAŽÉR KYBERNETICKEJ BEZPEČNOSTI



Integrácia

MKB rozumie poslaniu a úlohám organizácie. Navrhuje a presadzuje opatrenia kybernetickej bezpečnosti tak, aby boli v súlade s poslaním a podporili plnenie cieľov organizácie.

Komunikácia

MKB vysvetľuje a presadzuje bezpečnostnú stratégiu s pomocou ostatných manažérov, spolupracuje. Vhodnou komunikáciou sa rieši aj zdieľanie informácií o hrozbách a rizikách, implementácii bezpečnostných opatrení aj neustále zvyšovanie bezpečnostného povedomia.

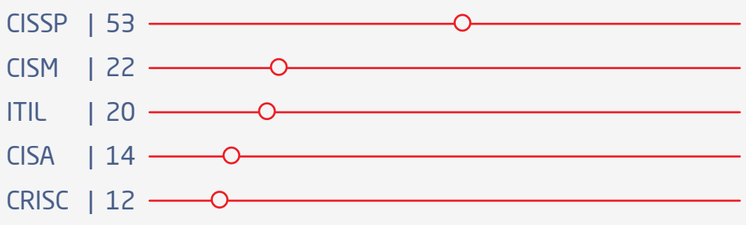
Zodpovednosť

Určujúcimi prvkami kybernetickej bezpečnosti sú ľudia, procesy a technológie. MKB je zodpovedný za manažment týchto prvkov v kontexte kybernetickej bezpečnosti.

Expertíza

MKB je skúsený v oblasti právnej úpravy ochrany informačných aktív, riadenia bezpečnostných hrozieb a rizík, strategického riadenia bezpečnosti, technologických riešení kybernetickej bezpečnosti a výkonu prevádzkových bezpečnostných činností.

5 TYPICKÝCH ODBORNÝCH CERTIFIKÁTOV MANAŽÉROV KYBERNETICKEJ BEZPEČNOSTI PODĽA FORTUNE 100



(Zdroj: The anatomy of a CISO: a breakdown of today's top security leaders, Digital Guardian's Blog, 2017; Fortune 100 je každoročný rebríček podnikov zostavený a vydaný časopisom Fortune)

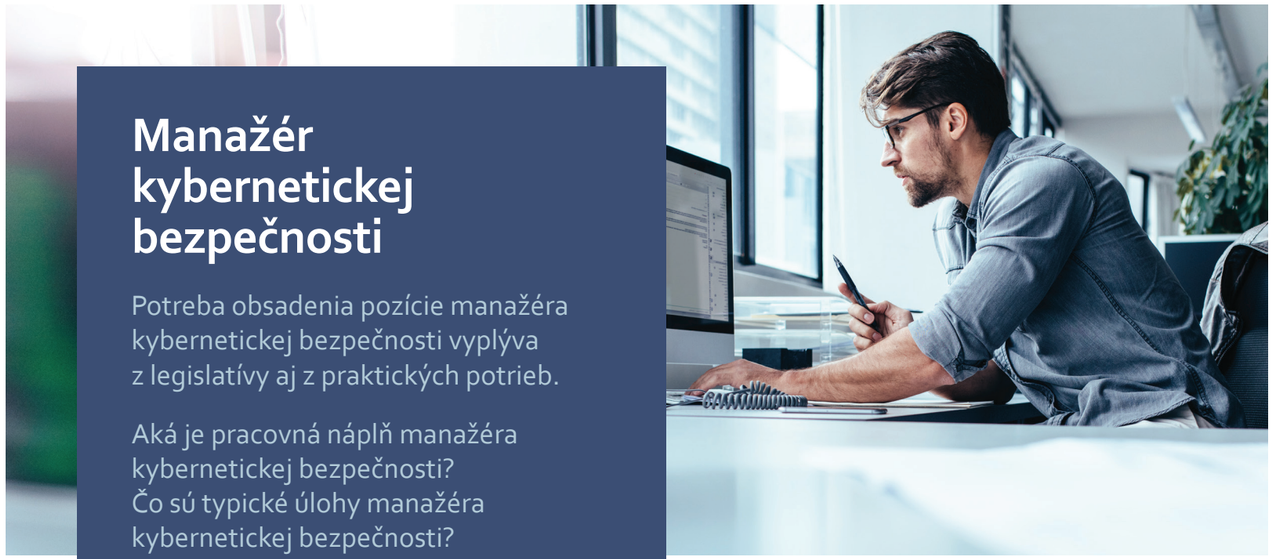
Tu uvedený informačný obsah vychádza z verejne dostupných a nám známych informácií a slúži na získanie všeobecného obrazu vo veciach, ktorých sa týka. Preto ho nemožno považovať za univerzálny, súhrnný alebo komplexný. Nezodpovedáme za skutočnosti, ku ktorým nemáme dostatočné informácie alebo ktoré majú základ v nepresných alebo nesprávnych informáciách alebo informáciách, ktoré nám nie sú známe. Informačný obsah ďalej nie je možné považovať za právne záväzný výklad právnych predpisov, ako ani za normatívny, individuálny alebo hybridný správny akt.

Kompetečné a certifikačné centrum kybernetickej bezpečnosti

poradna@cybercompetence.sk www.cybercompetence.sk FAQ www.cybercompetence.sk/casto-kladene-otazky-riadenie-kb/

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD



Manažér kybernetickej bezpečnosti

Potreba obsadenia pozície manažéra kybernetickej bezpečnosti vyplýva z legislatívy aj z praktických potrieb.

Aká je pracovná náplň manažéra kybernetickej bezpečnosti?
Čo sú typické úlohy manažéra kybernetickej bezpečnosti?
A ako by mal v praxi tieto úlohy plniť?

Požiadavka na určenie roly

V zmysle *§ 20 ods. 3 zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti* (ďalej len „zákon") sa bezpečnostné opatrenia prijímajú aj pre oblasť organizácie bezpečnosti. Požiadavka určenia manažéra kybernetickej bezpečnosti je explicitne uvedená v *§ 20 ods. 4 písm. a) zákona* ako aj v *§ 5 písm. a) vyhlášky Národného bezpečnostného úradu č. 362/2018 Z. z.,* ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.

V kontexte správy informačných systémov verejnej správy je rovnaká požiadavka zdôraznená aj v niekoľkých ustanoveniach *vyhlášky Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z.z.* ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy.

Pre manažéra kybernetickej bezpečnosti a jeho činnosť musia byť v organizácii vytvorené viaceré predpoklady.

Názov roly

Manažér kybernetickej bezpečnosti je v slovenských podmienkach nová riadiaca pracovná pozícia, pre ktorú zatiaľ nie je v slovenčine ustálená skratka. Po prijatí zákona sa prirodzene ponúka skratka „MKB" a skratku používame aj v tomto dokumente. Vo svete i na Slovensku v komerčnom prostredí sa táto rola už mnoho rokov **zvyčajne uvádza pod skratkou „CISO"** (z anglického „Chief Information Security Officer").

Priamy prístup ku štatutárnemu orgánu

MKB má mať možnosť komunikovať a predkladať návrhy a oznamovať informácie v oblasti kybernetickej bezpečnosti priamo štatutárnemu orgánu. MKB nesmie byť „hlboko utopený" v štruktúre organizácie. V komplikovaných a rozsiahlych organizačných štruktúrach je však akceptovateľné, ak sa právomoc priameho prístupu ku štatutárnemu orgánu upraví procesne, napríklad interným predpisom.

Nezávislosť od prevádzky

Postavenie MKB musí byť nezávislé od útvaru zaisťujúceho prevádzku IT. Úlohou MKB je najmä zaistiť odolnosť organizácie voči kybernetickým bezpečnostným hrozbám, riadiť súvisiace riziká a riešiť bezpečnostné incidenty. MKB je často „bezpečnostnou protiváhou" útvarom vývoja a prevádzky IT. Výrazne sa podieľa na ochrane aktív organizácie, niekedy dokonca musí rozhodnúť o zastavení rizikovej činnosti organizácie. Samozrejme, v závislosti od jeho kompetencií.

Ak MKB bude závislý od prevádzky a vývoja technologických služieb, existuje riziko, že rozhodnutia v oblasti kybernetickej bezpečnosti budú aj v krízových situáciách ovplyvnené najmä cieľmi útvarov zodpovedných za IT služby a prevádzku organizácie.

KVALIFIKAČNÉ POŽIADAVKY

Minimálne požiadavky na vzdelanie a prax

Minimálne kvalifikačné požiadavky na úroveň vzdelania a prax certifikovaného profesionála, ktorý vykonáva úlohy MKB sú stanovené v certifikačnej schéme overovania odbornej spôsobilosti manažéra kybernetickej bezpečnosti zverejnenej na stránkach NBÚ.

Vzdelanie a požadovaný doklad	Prax a spôsob jej preukázania (alternatívy predložených dokumentov)
Úplné stredné všeobecné vzdelanie a úplné stredné odborné vzdelanie (doklad o získanom stupni vzdelania a o získanej kvalifikácii)	• skúsenosti v oblasti informačných technológií - najmenej **10 rokov praxe** (životopis s uvedením kontaktu na overiteľnú referenciu), • skúsenosti v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT - najmenej **7 rokov praxe** • medzinárodný certifikát[1] sa považuje za započítateľnú odbornú **prax 3 roky**
Vysokoškolské vzdelanie prvého stupňa (doklady o absolvovaní štúdia)	• skúsenosti v oblasti informačných technológií - najmenej **7 rokov praxe** (životopis s uvedením kontaktu na overiteľnú referenciu), • skúsenosti v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT - najmenej **5 rokov praxe** • medzinárodný certifikát[1] sa považuje započítateľnú odbornú prax **3 roky**
Vysokoškolské vzdelanie druhého stupňa (doklady o absolvovaní štúdia)	• skúsenosti v oblasti informačných technológií - najmenej **5 rokov praxe** (životopis s uvedením kontaktu na overiteľnú referenciu), • skúsenosti v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT - najmenej **3 roky praxe** • medzinárodný certifikát[1] sa považuje za započítateľnú odbornú prax prax **3 roky**

Tieto požiadavky môžu orientačne poslúžiť aj pri obsadzovaní pozície MKB necertifikovaným profesionálom.

Ďalej je vhodné primerane zohľadniť:

osobnostné predpoklady,

najmä: schopnosť prijímať rozhodnutia, myslieť a konať v súvislostiach, riešiť konflikty, poskytovať spätnú väzbu, delegovať úlohy, podporovať procesy vzdelávania a odovzdávania znalostí, schopnosť viesť pracovný tím

všeobecné kľúčové kompetencie,

najmä: digitálnu, ekonomickú a finančnú gramotnosť, znalosť cudzieho jazyka, znalosť štátneho jazyka, matematickú gramotnosť, mediálnu a technickú gramotnosť, osobnostné a emocionálne kompetencie, schopnosť učiť sa, sociálne kompetencie, technickú gramotnosť

špecifické kľúčové kompetencie,

najmä: schopnosť organizovania a plánovania práce, schopnosť prijímať rozhodnutia a niesť zodpovednosť, analytické myslenie, strategické a koncepčné myslenie, tvorivosť (kreativitu), prezentačnú zručnosť

odborné kompetencie

Na vydanie osobitného predpisu ktorým sa určujú znalostné štandardy v oblasti kybernetickej bezpečnosti je v *§ 32 ods. 1 písm. d) zákona* splnomocnený Národný bezpečnostný úrad.

Požiadavky na znalosti a zručnosti sú stanovené aj v certifikačnej schéme overovania odbornej spôsobilosti manažéra kybernetickej bezpečnosti, napríklad:

- Znalosť procesov a systému riadenia informačnej a kybernetickej bezpečnosti
- Znalosť zásad organizácie informačnej a kybernetickej bezpečnosti
- Znalosti v oblasti informačných a komunikačných technológii
- Znalosť princípov riadenia IT služieb
- Znalosť právnych predpisov, požiadaviek na súlad a noriem vzťahujúcich sa na kybernetickú bezpečnosť a ochranu osobných údajov
- Zručnosť v navrhovaní a uplatňovaní bezpečnostných stratégií a politík
- Znalosť procesov riadenia rizík a postupov a metodík analýzy rizík
- Znalosť typických hrozieb a postupov pre identifikáciu hrozieb a zraniteľností
- Znalosť bezpečnostných mechanizmov
- Znalosť princípov podnikovej architektúry
- Znalosť procesov riešenia kybernetických bezpečnostných incidentov
- Znalosť procesov riadenia kontinuity činností a plánovania havarijnej obnovy prevádzky
- Znalosť princípov testovania a posudzovania kybernetickej bezpečnosti
- Zručnosť v hodnotení bezpečnostných mechanizmov a riešení
- Zručnosť v riadení projektov

ÚLOHY MANAŽÉRA KYBERNETICKEJ BEZPEČNOSTI

Vyhláškami sú určené iba základné rámce, resp. minimálne požiadavky, kladené na manažéra kybernetickej bezpečnosti. Rola pri výkone svojej činnosti typicky zodpovedá za niekoľko oblastí priamo alebo nepriamo súvisiacich s kybernetickou a informačnou bezpečnosťou. Pre lepšie pochopenie sú v ďalšom texte uvedené formálne zákonné ale aj typické praktické povinnosti manažéra kybernetickej bezpečnosti, pochádzajúce z dobrej praxe.

Riadenie bezpečnosti

- strategické riadenie informačnej a kybernetickej bezpečnosti organizácie
- vypracovanie, a prezentácia bezpečnostných stratégií a konceptov
- implementácia a riadenie procesov informačnej a kybernetickej bezpečnosti podľa všeobecne záväzných právnych predpisov, bezpečnostnej stratégie a ostatných interných riadiacich aktov
- zabezpečenie vypracovanie, udržiavanie a aktualizácie bezpečnostnej dokumentácie informačnej a kybernetickej bezpečnosti a ďalších interných riadiacich aktov vo vzťahu k bezpečnosti organizácie
- návrh požiadaviek na rozpočet a na iné zdroje súvisiace s bezpečnostnými opatreniami a procesmi relevantnými z hľadiska informačnej a kybernetickej bezpečnosti
- metodické usmerňovanie správcov a gestorov informačných a komunikačných technológií, vlastníkov procesov, vlastníkov aktív, vedúcich zamestnancov a ďalších zodpovedných zamestnancov vo vzťahu k dosahovaniu bezpečnostných cieľov organizácie
- poskytovanie informácií bezpečnostnému výboru a/alebo štatutárnemu orgánu o stave informačnej a kybernetickej bezpečnosti v organizácii
- poskytovanie informácií bezpečnostnému výboru organizácie a/alebo štatutárnemu orgánu o závažných bezpečnostných rizikách, kybernetických bezpečnostných incidentoch a významných bezpečnostných udalostiach
- riadenie informačnej a kybernetickej bezpečnosti vo vzťahu s dodávateľmi a pri zaobstarávaní, projektovaní a vývoji softvéru a systémov
- správa bezpečnosti informačných aktív organizácie

Manažment hrozieb a rizík

- implementácia a manažment procesov identifikácie, analýzy a monitoringu bezpečnostných hrozieb a rizík
- návrh opatrení na ošetrovanie rizík, a na zamedzenie dopadov bezpečnostných udalostí
- zabezpečovanie procesov hodnotenia technických zraniteľností systémov
- manažment procesov detekcie, riešenia, evidencie a prevencie kybernetických bezpečnostných incidentov
- zabezpečenie funkčných plánov kontinuity a obnovy činností organizácie
- koordinácia a riadenie procesov obnovy prevádzkových činnosti (tzv. Business Continuity Management), vrátane riadenia procesov plánovania obnovy systémov po havárii (tzv. Disaster Recovery Planning)

Aplikácia bezpečnostných opatrení

- riadenie návrhov, implementácie, zmien a optimalizácie bezpečnostných riešení s víziou a konceptom ich bežného prevádzkovania
- zabezpečovanie implementácie technických a organizačných bezpečnostných opatrení
- riadenie návrhov a integrácie bezpečnostných technológií s cieľom tvorby efektívnych bezpečnostných opatrení na ochranu poskytovaných služieb organizácie
- riadenie zmien a optimalizácie bezpečnostných riešení
- riadenie bezpečnostnej architektúry
- predkladanie odborných stanovísk k novým zmenám v IT infraštruktúre, ktoré môžu mať potenciálny vplyv na bezpečnosť informačných aktív organizácie
- monitorovanie plnenia a efektivity bezpečnostných opatrení

Výkon operatívnych bezpečnostných činností

- manažment výkonu činností súvisiacich so zaručením bezpečnosti informačných aktív v zmysle najlepšej praxe
- vedenie tímu zamestnancov útvaru informačnej a kybernetickej bezpečnosti, ak je taký organizačný útvar zriadený
- návrh a aplikácia metodík pre klasifikáciu informačných aktív a kategorizáciu sietí a informačných systémov
- riadenie bežnej prevádzky technických bezpečnostných opatrení
- zabezpečovanie udržateľnosti organizačných opatrení vrátane vyspelosti bezpečnostných procesov
- zaistenie uplatňovania princípu oddelenia právomocí a zodpovedností v celej organizačnej štruktúre organizácie tak, aby rovnaká osoba nebola zodpovedná za vykonávanie a zároveň aj schvaľovanie alebo kontrolu bezpečnostne relevantných aktivít a činností
- riadenie projektov kybernetickej bezpečnosti

Riadenie súladu

- riadenie procesov zaručenia súladu (tzv. Compliance Management) v oblasti informačnej a kybernetickej bezpečnosti
- zabezpečenie pravidelného preskúmavania stavu kybernetickej a informačnej bezpečnosti
- vyhodnocovanie plnenia vnútorných predpisov súvisiacich s riadením kybernetickej bezpečnosti
- poskytovanie súčinnosti internému a externému auditu informačnej a kybernetickej bezpečnosti
- navrhovanie metrík a kľúčových indikátorov pre sledovanie vývoja a stavu bezpečnosti a vývoja bezpečnostných rizík
- zabezpečovanie školení zamestnancov v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti
- zabezpečovanie kontinuálneho vzdelávania pre pracovné roly relevantné z hľadiska kybernetickej bezpečnosti
- zabezpečovanie budovania bezpečnostného povedomia pre oblasť informačnej a kybernetickej bezpečnosti a ochrany osobných údajov
- spolupráca s orgánmi verejnej moci a orgánmi činnými v trestnom konaní