**Manažér kybernetickej bezpečnosti**

| Rola: | **Manažér kybernetickej bezpečnosti** | |
|---|---|---|
| Vedomosti: | **Riadenie bezpečnosti** | |
| | 1) procesy, systémy a zásady riadenia kybernetickej bezpečnosti vrátane zásad riadenia fyzickej a objektovej bezpečnosti | BL5 |
| | 2) organizácia kybernetickej bezpečnosti | BL6 |
| | 3) terminológia a skratky v oblasti kybernetickej bezpečnosti | BL6 |
| | 4) princípy riadenia IT služieb, správy systémov a správy počítačových sietí | BL5 |
| | 5) hodnotiace a validačné kritériá v oblasti kybernetickej bezpečnosti (KPI, KRI atď.) | BL5 |
| | 6) zdroje, charakteristiky a použitie informačných aktív organizácie | BL6 |
| | 7) organizačné politiky, organizačné štruktúry a koncepty plánovania vzťahov s internými a/alebo externými organizáciami | BL6 |
| | 8) koncepcie zlepšovania organizačných procesov a modely hodnotenia vyspelosti procesov (napr. CMMI) | BL6 |
| | 9) zásady a techniky plánovania kapacity a plánovania zdrojov | BL5 |
| | 10) princípy riadenia ľudských zdrojov | BL6 |
| | 11) rozpočtové pravidlá, zásady plánovania a riadenia nákladov a plánovania a riadenia investícií | BL5 |
| | 12) základy compliance v oblasti kybernetickej bezpečnosti (právny rámec aspoň na úrovni zákona o ITVS, GDPR, ePrivacy, ISO 20000) | BL3 |
| | 13) výskumné stratégie a znalostný manažment | BL4 |
| | 14) princípy podnikovej architektúry, koncepcie bezpečnostnej architektúry a referenčné modely podnikovej architektúry (napr. TOGAF, Zachman, FEA atď.) | BL5 |
| | 15) koncepty, terminológia a princípy prevádzky elektronických komunikačných systémov (počítačové a telefónne siete, satelitné, optické, bezdrôtové atď.) | BL4 |
| | 16) model OSI, mapovanie siete, topológia sietí, hlavné sieťové protokoly | BL5 |
| | 17) princípy sieťových zariadení (rozbočovače, prepínače, smerovače, brány, firewall atď.) | BL2 |

| | | |
|---|---|---|
| | 18) zásady riadenia dodávateľských služieb a obstarávania informačných systémov vrátane vyhodnocovania dôveryhodnosti dodávateľa alebo výrobku | BL6 |
| | **Riadenie hrozieb a rizík** | |
| | 1) procesy riadenia rizík, postupy a metodiky analýzy rizík | BL6 |
| | 2) typické kybernetické bezpečnostné hrozby a zraniteľnosti a metódy ich identifikácie | BL4 |
| | 3) zásady aplikačnej bezpečnosti | BL4 |
| | 4) teória, koncepty a metódy systémového inžinierstva | BL4 |
| | 5) metódy a techniky softvérového inžinierstva vrátane modelov vývoja softvéru, princípy životného cyklu vývoja systémov a zásady bezpečného vývoja softvéru | BL4 |
| | 6) bezpečnostné koncepty v operačných systémoch | BL4 |
| | 7) bezpečnostné mechanizmy a metódy v softvérovom inžinierstve (napr. modularizácia, vrstvenie, abstrakcia, maskovanie, šifrovanie, pseudonymizácia, minimalizácia spracúvania atď.) | BL5 |
| | 8) techniky a metódy riadenia konfigurácií a vplyv konfigurácií na bezpečnosť | BL3 |
| | 9) nástroje na posudzovanie zraniteľností | BL3 |
| | 10) sieťové protokoly a adresárové služby | BL3 |
| | 11) základná architektúra operačných systémov (napr. riadenie systémových procesov, štruktúra adresárov, inštalácia a spúšťanie procesov a aplikácií) | BL3 |
| | 12) bezpečnostné riziká cloud computingu | BL4 |
| | 13) všeobecné koncepty operačných technológií a riadiacich systémov (OT/ICS) | BL5* |
| | **Aplikácia bezpečnostných opatrení** | |
| | 1) princípy navrhovania opatrení na ošetrenie bezpečnostných rizík | BL6 |
| | 2) bezpečnostné mechanizmy a spôsob ich implementácie | BL3 |
| | 3) bezpečnostné opatrenia vo fyzickej a objektovej bezpečnosti | BL4 |
| | 4) nástroje, metódy a techniky navrhovania bezpečnostných systémov | BL4 |
| | 5) zásady personálnej bezpečnosti | BL5 |
| | 6) opatrenia týkajúce sa používania, spracúvania, uchovávania a prenosu údajov | BL6 |
| | 7) zásady a princípy riadenia identít a prístupov | BL4 |
| | 8) základy kryptografických bezpečnostných mechanizmov | BL4 |

| | | |
|---|---|---|
| | 9) koncepcie a technológie vzdialeného prístupu | BL4 |
| | 10) základy virtualizačných technológií, vývoja a údržby virtuálnych strojov | BL3 |
| | 11) princípy zabezpečenia virtuálnych privátnych sietí (VPN) | BL3 |
| | 12) techniky a metódy správy systémov a hardeningu systémov | BL3 |
| | **Výkon operatívnych bezpečnostných činností** | |
| | 1) procesy riešenia kybernetických bezpečnostných incidentov | BL6 |
| | 2) zásady riadenia bezpečnosti prostredia cloudu | BL5 |
| | 3) zásady určovania bezpečnostne relevantných zdrojov informácií a princípy tvorby prípadov použitia | BL4 |
| | 4) princípy logovania a bezpečnostného monitorovania | BL4 |
| | 5) princípy korelácie bezpečnostných udalostí | BL4 |
| | 6) základné postupy pri spracovaní digitálnych stôp | BL4 |
| | 7) základy penetračného testovania | BL3 |
| | **Riadenie súladu** | |
| | 1) právne predpisy, požiadavky na súlad a technické normy vzťahujúce sa na kybernetickú bezpečnosť a ochranu osobných údajov | BL6 |
| | 2) základy compliance v oblasti kybernetickej bezpečnosti (právny rámec aspoň na úrovni zákona o ITVS, GDPR, ePrivacy, ISO 20000) | BL3 |
| | 3) požiadavky právnych predpisov na bezpečnostnú dokumentáciu a bezpečnostné politiky | BL6 |
| | 4) princípy posudzovania kybernetickej bezpečnosti | BL5 |
| | 5) politiky, procesy a postupy pre riadenie ľudských zdrojov v organizácii | BL6 |
| | 6) systémy odbornej prípravy, princípy vzdelávacích stratégií, procesov a postupov vzdelávania a zvyšovania povedomia u dospelých v oblasti kybernetickej bezpečnosti vrátane merania efektivity vzdelávania | BL6 |
| | 7) zásady a metódy tvorby učebných plánov, výuky jednotlivcov a skupín | BL6 |
| | 8) štandardy bezpečnosti platobných kariet (PCI) | BL4* |
| | 9) štandardy a procesy riadenia rizík v dodávateľskom reťazci | BL6 |
| | 10) metódy testovania a vyhodnocovania bezpečnosti systémov | BL4 |

| | |
|---|---|
| Zručnosti: | **Riadenie bezpečnosti**<br>1) strategické riadenie kybernetickej bezpečnosti organizácie<br>2) vypracovanie a prezentácia bezpečnostných stratégií a konceptov<br>3) implementácia a riadenie procesov kybernetickej bezpečnosti podľa všeobecne záväzných právnych predpisov, bezpečnostnej stratégie a ostatných interných riadiacich aktov<br>4) zabezpečenie, vypracovanie, udržiavanie a aktualizácie bezpečnostnej dokumentácie kybernetickej bezpečnosti a ďalších interných riadiacich aktov vo vzťahu k bezpečnosti organizácie<br>5) návrh požiadaviek na rozpočet a na iné zdroje súvisiace s bezpečnostnými opatreniami a procesmi relevantnými z hľadiska kybernetickej bezpečnosti vrátane riadenia nákladov a riadenia investícií<br>6) 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<br>7) poskytovanie informácií bezpečnostnému výboru alebo štatutárnemu orgánu o stave kybernetickej bezpečnosti v organizácii, o závažných bezpečnostných rizikách, kybernetických bezpečnostných incidentoch a významných bezpečnostných udalostiach<br>8) riadenie kybernetickej bezpečnosti vo vzťahu s dodávateľmi a pri obstarávaní a vývoji softvéru a systémov<br><br>**Riadenie hrozieb a rizík**<br>1) implementácia a manažment procesov identifikácie, analýzy a monitoringu bezpečnostných hrozieb a rizík<br>2) posudzovanie hrozieb a rizík<br>3) návrh opatrení na ošetrovanie rizík a na zamedzenie dopadov bezpečnostných udalostí<br>4) zabezpečovanie procesov hodnotenia technických zraniteľností systémov<br>5) manažment procesov detekcie, riešenia, evidencie a prevencie kybernetických bezpečnostných incidentov<br>6) zabezpečenie funkčných plánov kontinuity a obnovy činností organizácie<br>7) koordinácia a riadenie procesov obnovy prevádzkových činnosti (tzv. Business Continuity Management) vrátane riadenia procesov plánovania obnovy systémov po havárii (tzv. Disaster Recovery Planning)<br><br>**Aplikácia bezpečnostných opatrení** |

| | |
|---|---|
| | 1) riadenie návrhov, implementácie, zmien a optimalizácie bezpečnostných riešení s víziou a konceptom ich bežného prevádzkovania<br>2) zabezpečovanie implementácie technických a organizačných bezpečnostných opatrení<br>3) riadenie bezpečnostnej architektúry<br>4) predkladanie odborných stanovísk k novým zmenám v IT infraštruktúre, ktoré môžu mať potenciálny vplyv na bezpečnosť informačných aktív organizácie<br>5) monitorovanie plnenia a efektivity bezpečnostných mechanizmov a opatrení<br><br>**Výkon operatívnych bezpečnostných činností**<br><br>1) manažment výkonu činností súvisiacich so zaručením bezpečnosti informačných aktív v zmysle najlepšej praxe<br>2) vedenie tímu zamestnancov útvaru informačnej a kybernetickej bezpečnosti, ak je taký organizačný útvar zriadený<br>3) návrh a aplikácia metodík pre klasifikáciu informačných aktív a kategorizáciu sietí a informačných systémov<br>4) riadenie bežnej prevádzky technických bezpečnostných opatrení<br>5) zabezpečovanie udržateľnosti organizačných opatrení vrátane vyspelosti bezpečnostných procesov<br>6) zaistenie uplatňovania princípu oddelenia právomocí a zodpovedností v celej organizačnej štruktúre organizácie<br>7) základy projektového manažmentu<br><br>**Riadenie súladu**<br><br>1) riadenie procesov zaručenia súladu (Compliance Management) v oblasti kybernetickej bezpečnosti<br>2) zabezpečenie pravidelného preskúmavania stavu kybernetickej a informačnej bezpečnosti<br>3) vyhodnocovanie plnenia vnútorných predpisov súvisiacich s riadením kybernetickej bezpečnosti<br>4) poskytovanie súčinnosti internému a externému auditu kybernetickej bezpečnosti<br>5) navrhovanie metrík a kľúčových indikátorov pre sledovanie vývoja a stavu bezpečnosti a vývoja bezpečnostných rizík<br>6) zabezpečovanie školení zamestnancov v oblasti kybernetickej bezpečnosti<br>7) zabezpečovanie kontinuálneho vzdelávania pre pracovné roly relevantné z hľadiska kybernetickej bezpečnosti<br>8) zabezpečovanie budovania bezpečnostného povedomia pre oblasť informačnej a kybernetickej bezpečnosti a ochrany osobných údajov |

| | | | |
|---|---|---|---|
| | 9) spolupráca s orgánmi verejnej moci a orgánmi činnými v trestnom konaní | | |
| Stupeň vzdelania: | Úplné stredné všeobecné alebo úplné stredné odborné | Vysokoškolské I. stupňa | Vysokoškolské II. a III. stupňa |
| Odborná prax: | • najmenej **7 rokov** praxe v oblasti informačných technológií<br>• z toho najmenej **5 rokov** praxe v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT<br>• medzinárodný certifikát sa považuje za započítateľnú odbornú prax 1 rok | • najmenej **5 rokov** praxe v oblasti informačných technológií<br>• z toho najmenej **3 roky** praxe v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT<br>• medzinárodný certifikát sa považuje za započítateľnú odbornú prax 1 rok | • najmenej **3 roky** praxe v oblasti informačných technológií<br>• z toho najmenej **1 rok** praxe v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT<br>• medzinárodný certifikát sa považuje za započítateľnú odbornú prax 1 rok |
| Špecifické kľúčové kompetencie | a) schopnosť prijímať rozhodnutia<br>b) schopnosť myslieť a konať v súvislostiach<br>c) schopnosť riešiť konflikty<br>d) schopnosť poskytovať spätnú väzbu<br>e) schopnosť delegovať úlohy<br>f) schopnosť podporovať procesy vzdelávania a odovzdávania znalostí<br>g) schopnosť viesť pracovný tím<br>h) schopnosť organizovania a plánovania práce<br>i) analytické myslenie<br>j) strategické a koncepčné myslenie<br>k) tvorivosť (kreativita)<br>l) prezentačná zručnosť | | |

Požiadavky označené * sú odvetvovo závislé. Pre príslušnú rolu sú posudzované v kontexte kompetencií, potrebných na vykonávanie určitej pracovnej činnosti v konkrétnom odvetví.