

Analytik kybernetickej bezpečnosti

Rola:	Analytik kybernetickej bezpečnosti	
Vedomosti:	<p>Riadenie bezpečnosti</p> <ol style="list-style-type: none"> 1) procesy, systémy a zásady riadenia informačnej a kybernetickej bezpečnosti vrátane zásad riadenia fyzickej a objektovej bezpečnosti 2) organizácia informačnej a kybernetickej bezpečnosti 3) terminológia a skratky v oblasti informačnej a kybernetickej bezpečnosti 4) princípy riadenia IT služieb, správy systémov a správy počítačových sietí 5) hodnotiace a validačné kritériá v oblasti kybernetickej bezpečnosti (KPI, KRI atď.) 6) zdroje, charakteristiky a použitie informačných aktív organizácie 7) organizačné politiky, organizačné štruktúry a koncepty plánovania vzťahov s internými a/alebo externými organizáciami 8) koncepcie zlepšovania organizačných procesov a modely hodnotenia vyspelosti procesov (napr. CMMI) 9) zásady a techniky plánovania kapacity a plánovania zdrojov 10) princípy riadenia ľudských zdrojov 11) rozpočtové pravidlá, zásady plánovania a riadenia nákladov a plánovania a riadenia investícií 12) procesy riadenia continuity činností a plánovania havarijnej obnovy prevádzky 13) výskumné stratégie a znalostný manažment 14) princípy podnikovej architektúry, koncepcie bezpečnostnej architektúry a referenčné modely podnikovej architektúry (napr. TOGAF, Zachman, FEA atď.) 15) koncepty, terminológia a princípy prevádzky elektronických komunikačných systémov (počítačové a telefónne siete, satelitné, optické, bezdrôtové atď.) 16) model OSI, mapovanie siete, topológia sietí, hlavné sieťové protokoly 17) princípy sieťových zariadení (rozbočovače, prepínače, smerovače, brány, firewall atď.) 18) zásady riadenia dodávateľských služieb a obstarávania informačných systémov vrátane vyhodnocovania dôveryhodnosti dodávateľa alebo výrobku 	<p>BL5</p> <p>BL6</p> <p>BL6</p> <p>BL5</p> <p>BL5</p> <p>BL6</p> <p>BL6</p> <p>BL6</p> <p>BL5</p> <p>BL6</p> <p>BL5</p> <p>BL6</p> <p>BL5</p> <p>BL6</p> <p>BL4</p> <p>BL5</p> <p>BL4</p> <p>BL5</p> <p>BL4</p> <p>BL5</p> <p>BL4</p> <p>BL6</p>

	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	BL5
3)	zásady aplikačnej bezpečnosti	BL5
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	BL4
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 ošetrovanie bezpečnostných rizík	BL6
2)	bezpečnostné mechanizmy a spôsob ich implementácie	BL5
3)	bezpečnostné opatrenia vo fyzickej a objektivej bezpečnosti	BL5
4)	nástroje, metódy a techniky navrhovania bezpečnostných systémov	BL4
5)	zásady personálnej bezpečnosti	BL5
6)	opatrenia týkajúce sa používania, spracovania, uchovávanía a prenosu údajov	BL6
7)	zásady a princípy riadenia identít a prístupov	BL5
8)	základy kryptografických bezpečnostných mechanizmov	BL4
9)	koncepce a technológie vzdialeného prístupu	BL4
10)	virtualizačné technológie, vývoja a údržby virtuálnych strojov	BL4

	<p>11) zabezpečenie virtuálnych privátnych sietí (VPN) BL4</p> <p>12) techniky a metódy správy systémov a hardeningu systémov BL4</p> <p>Výkon operatívnych bezpečnostných činností</p> <p>1) procesy riešenia kybernetických bezpečnostných incidentov BL6</p> <p>2) zásady riadenia bezpečnosti prostredia cloudu BL5</p> <p>3) zásady určovania bezpečnostne relevantných zdrojov informácií a princípy tvorby prípadov použitia BL4</p> <p>4) princípy logovania a bezpečnostného monitorovania BL4</p> <p>5) princípy korelácie bezpečnostných udalostí BL4</p> <p>6) základné postupy pri spracovaní digitálnych stôp BL4</p> <p>7) princípy, nástroje a techniky testovania prieniku BL4</p> <p>Riadenie súladu</p> <p>1) právne predpisy, požiadavky na súlad a technické normy vzťahujúce sa na kybernetickú bezpečnosť a ochranu osobných údajov BL6</p> <p>2) právne predpisy, požiadavky na súlad a technické normy vzťahujúce sa na prevádzku informačných a komunikačných technológií BL6</p> <p>3) požiadavky právnych predpisov na bezpečnostnú dokumentáciu a bezpečnostné politiky BL6</p> <p>4) princípy posudzovania kybernetickej bezpečnosti BL5</p> <p>5) politiky, procesy a postupy pre riadenie ľudských zdrojov v organizácii BL6</p> <p>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</p> <p>7) zásady a metódy tvorby učebných plánov, výuky jednotlivcov a skupín BL6</p> <p>8) štandardy bezpečnosti platobných kariet (PCI) BL5*</p> <p>9) štandardy a procesy riadenia rizík v dodávateľskom reťazci BL6</p> <p>10) metódy testovania a vyhodnocovania bezpečnosti systémov BL6</p>
Zručnosti:	<p>Riadenie bezpečnosti</p> <p>a) strategické riadenie informačnej a kybernetickej bezpečnosti organizácie</p> <p>b) vypracovanie a prezentácia bezpečnostných stratégií a konceptov</p>

- c) implementácia a riadenie procesov informačnej a kybernetickej bezpečnosti podľa všeobecne záväzných právnych predpisov, bezpečnostnej stratégie a ostatných interných riadiacich aktov
- d) zabezpečenie, vypracovanie, udržiavanie a aktualizácie bezpečnostnej dokumentácie informačnej a kybernetickej bezpečnosti a ďalších interných riadiacich aktov vo vzťahu k bezpečnosti organizácie
- e) návrh požiadaviek na rozpočet a na iné zdroje súvisiace s bezpečnostnými opatreniami a procesmi relevantnými z hľadiska informačnej a kybernetickej bezpečnosti vrátane riadenia nákladov a riadenia investícií
- f) 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
- g) poskytovanie informácií bezpečnostnému výboru alebo štatutárnemu orgánu o stave informačnej a kybernetickej bezpečnosti v organizácii, o závažných bezpečnostných rizikách, kybernetických bezpečnostných incidentoch a významných bezpečnostných udalostiach
- h) riadenie informačnej a kybernetickej bezpečnosti vo vzťahu s dodávateľmi a pri obstarávaní a vývoji softvéru a systémov

Riadenie hrozieb a rizík

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

Aplikácia bezpečnostných opatrení

- a) riadenie návrhov, implementácie, zmien a optimalizácie bezpečnostných riešení s víziou a konceptom ich bežného prevádzkovania

- b) zabezpečovanie implementácie technických a organizačných bezpečnostných opatrení
- c) riadenie návrhov, zmien a integrácie bezpečnostných technológií a riešení
- d) riadenie bezpečnostnej architektúry
- e) predkladanie odborných stanovísk k novým zmenám v IT infraštruktúre, ktoré môžu mať potenciálny vplyv na bezpečnosť informačných aktív organizácie
- f) monitorovanie plnenia a efektivity bezpečnostných mechanizmov a opatrení

Výkon operatívnych bezpečnostných činností

- a) manažment výkonu činností súvisiacich so zaručením bezpečnosti informačných aktív v zmysle najlepšej praxe
- b) vedenie tímu zamestnancov útvaru informačnej a kybernetickej bezpečnosti, ak je taký organizačný útvar zriadený
- c) návrh a aplikácia metodík pre klasifikáciu informačných aktív a kategorizáciu sietí a informačných systémov
- d) riadenie bežnej prevádzky technických bezpečnostných opatrení
- e) zabezpečovanie udržateľnosti organizačných opatrení vrátane vyspelosti bezpečnostných procesov
- f) zaistenie uplatňovania princípu oddelenia právomocí a zodpovedností v celej organizačnej štruktúre organizácie
- g) riadenie projektov kybernetickej bezpečnosti

Riadenie súladu

- a) riadenie procesov zaručenia súladu (tzv. Compliance Management) v oblasti informačnej a kybernetickej bezpečnosti
- b) zabezpečenie pravidelného preskúmania stavu kybernetickej a informačnej bezpečnosti
- c) vyhodnocovanie plnenia vnútorných predpisov súvisiacich s riadením kybernetickej bezpečnosti
- d) poskytovanie súčinnosti internému a externému auditu informačnej a kybernetickej bezpečnosti
- e) navrhovanie metrik a kľúčových indikátorov pre sledovanie vývoja a stavu bezpečnosti a vývoja bezpečnostných rizík
- f) zabezpečovanie školení zamestnancov v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti
- g) zabezpečovanie kontinuálneho vzdelávania pre pracovné roly relevantné z hľadiska kybernetickej bezpečnosti
- h) zabezpečovanie budovania bezpečnostného povedomia pre oblasť informačnej a kybernetickej bezpečnosti a ochrany osobných údajov

	i) 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:	<ul style="list-style-type: none"> • najmenej 7 rokov praxe v oblasti informačných technológií • z toho najmenej 5 rokov praxe v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT • medzinárodný certifikát sa považuje za započítateľnú odbornú prax 1 rok 	<ul style="list-style-type: none"> • najmenej 5 rokov praxe v oblasti informačných technológií • z toho najmenej 3 roky praxe v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT • medzinárodný certifikát sa považuje za započítateľnú odbornú prax 1 rok 	<ul style="list-style-type: none"> • najmenej 3 roky praxe v oblasti informačných technológií • z toho najmenej 1 rok praxe v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT • medzinárodný certifikát sa považuje za započítateľnú odbornú prax 1 rok
Špecifické kľúčové kompetencie	a) schopnosť prijímať rozhodnutia b) schopnosť myslieť a konať v súvislostiach c) schopnosť riešiť konflikty d) schopnosť poskytovať spätnú väzbu e) schopnosť delegovať úlohy f) schopnosť podporovať procesy vzdelávania a odovzdávania znalostí g) schopnosť viesť pracovný tím h) schopnosť organizovania a plánovania práce i) analytické myslenie j) strategické a koncepčné myslenie k) tvorivosť (kreativita) l) prezentačná zručnosť		