Špecialista riadenia rizík

Rola:	**Špecialista riadenia rizík**	
Vedomosti:	**Riadenie bezpečnosti**	
	1) procesy, systémy a zásady riadenia informačnej a kybernetickej bezpečnosti, vrátane zásad riadenia fyzickej a objektovej bezpečnosti	BL4
	2) zásady organizácie informačnej a kybernetickej bezpečnosti	BL5
	3) terminológia a skratky v oblasti informačnej a kybernetickej bezpečnosti	BL5
	4) princípy riadenia IT služieb, správy systémov a správy počítačových sietí	BL5
	5) hodnotiace a validačné kritériá v oblasti kybernetickej bezpečnosti (KPI, KRI, metodiky merania vyspelosti atď.)	BL5
	6) zdroje, charakteristiky a použitie informačných aktív organizácie	BL5
	7) organizačné politiky, organizačné štruktúry a koncepty plánovania vzťahov s internými a/alebo externými organizáciami	BL5
	8) koncepcie zlepšovania organizačných procesov a modely hodnotenia vyspelosti procesov (napr. CMMI)	BL5
	9) základy Business Continuity Managementu (BCM)	BL3
	10) poznanie základných procesov pri riadení a obstarávaní informačných systémov vrátane vyhodnocovania dôveryhodnosti dodávateľa alebo výrobku	BL3
	11) nové a rozvíjajúce sa informačné technológie a technológie kybernetickej bezpečnosti	BL4
	12) štandardy a metodiky klasifikácie údajov založených na citlivosti a iných rizikových faktoroch	BL5
	13) terminológia dátovej komunikácie (napr. sieťové protokoly, Ethernet, IP, šifrovanie, optické zariadenia, vymeniteľné médiá)	BL4
	14) typy sieťovej komunikácie (napr LAN, WAN, MAN, WLAN, WWAN)	BL4
	15) typy webových stránok, správa, funkcie a systémy na správu obsahu (CMS)	BL4
	16) základy sieťovej a internetovej komunikácie (t. j. zariadenia, konfigurácia zariadení hardvér, softvér, aplikácie, porty/protokoly, adresovanie, sieťová architektúra a infraštruktúra, smerovanie, operačné systémy atď.)	BL4

	17) princípy zraniteľností bezdrôtových sietí	BL4
	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	BL6
	3) zásady aplikačnej bezpečnosti	BL4
	4) teória, koncepty a metódy systémového inžinierstva	BL4
	5) bezpečnostné koncepty v operačných systémoch	BL3
	6) všeobecné koncepty operačných technológií a riadiacich systémov (OT/ICS)	BL4*
	7) základné postupy etického hackingu	BL3
	8) princípy a zdroje získavania informácií o zraniteľnostiach (napr. varovania, rady, bulletiny)	BL5
	9) triedy a vektory útokov	BL4
	Aplikácia bezpečnostných opatrení	
	1) navrhovanie opatrení na ošetrenie bezpečnostných rizík	BL6
	2) bezpečnostné mechanizmy a spôsob ich implementácie	BL3
	3) základné princípy bezpečnostných mechanizmov.	BL3
	4) zásady personálnej bezpečnosti	BL5
	5) opatrenia týkajúce sa používania, spracovania, uchovávania a prenosu údajov	BL5
	6) zásady a princípy riadenia identít a prístupov	BL4
	7) kryptografické bezpečnostné mechanizmy	BL4
	8) koncepcie a technológie vzdialeného prístupu	BL4
	9) virtualizačné technológie, vývoj a údržba virtuálnych strojov	BL4
	Výkon operatívnych bezpečnostných činností	
	1) procesy riešenia kybernetických bezpečnostných incidentov	BL4
	2) znalosti o štádiách kybernetického útoku (napr. Prieskum, skenovanie, získanie prístupu, eskalácia oprávnení, využitie, zahladenie stôp)	BL4
	3) zásady určovania bezpečnostne relevantných zdrojov informácií a princípy tvorby prípadov použitia	BL5
	4) princípy logovania a bezpečnostného monitorovania	BL4
	5) princípy korelácie bezpečnostných udalostí	BL4

	6) princípy a mechanizmy zabezpečenia siete (napr. šifrovanie, brány firewall, autentifikácia, medové pasce, ochrana perimetra)	BL4
	7) princípy hĺbkovej ochrany a architektúry sieťovej bezpečnosti	BL3
	8) princípy sieťových demilitarizovaných zón	BL3
	9) princípy súborových systémov (napr. NTFS, FAT a iné)	BL3
	10) programy, úlohy a zodpovednosti a metódy reakcie na incidenty v organizácii	BL5
	11) zásady riadenia bezpečnosti prostredia cloudu	BL3
	Riadenie súladu	
	1) právne predpisy, požiadavky na súlad a technické normy vzťahujúce sa na kybernetickú bezpečnosť a ochranu osobných údajov	BL6
	2) požiadavky právnych predpisov na bezpečnostnú dokumentáciu a bezpečnostné politiky	BL6
	3) princípy posudzovania kybernetickej bezpečnosti	BL6
	4) politiky, procesy a postupy pre riadenie ľudských zdrojov v organizácii	BL5
	5) štandardy bezpečnosti platobných kariet (PCI)	BL3*
	6) štandardy a procesy riadenia rizík v dodávateľskom reťazci	BL6
	7) metódy testovania a vyhodnocovania bezpečnosti systémov	BL3
Zručnosti:	**Riadenie bezpečnosti** • podpora riadenia informačnej a kybernetickej bezpečnosti organizácie **Riadenie hrozieb a rizík** a) implementácia procesov a nástrojov identifikácie, analýzy a monitoringu bezpečnostných hrozieb a rizík b) posudzovanie hrozieb a rizík c) návrh opatrení na ošetrovanie rizík d) účasť v procesoch obnovy prevádzkových činnosti (tzv. Business Continuity Management) vrátane účasti v riadení procesov plánovania obnovy systémov po havárii (tzv. Disaster Recovery Planning) **Aplikácia bezpečnostných opatrení** a) podpora riadenia bezpečnostnej architektúry	

	b) monitorovanie plnenia a efektivity bezpečnostných mechanizmov a opatrení **Výkon operatívnych bezpečnostných činností** a) výkon činností súvisiacich so zaručením bezpečnosti informačných aktív v zmysle najlepšej praxe b) aplikácia metodík pre klasifikáciu informačných aktív a kategorizáciu sietí a informačných systémov **Riadenie súladu** a) pravidelné preskúmavanie stavu kybernetickej a informačnej bezpečnosti b) poskytovanie súčinnosti internému a externému auditu informačnej a kybernetickej bezpečnosti
Špecifické kľúčové kompetencie	a) schopnosť prijímať rozhodnutia b) schopnosť myslieť a konať v súvislostiach c) analytické myslenie d) prezentačná zručnosť e) schopnosť organizovania a plánovania práce f) strategické a koncepčné myslenie

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