

## Architekt kybernetickej bezpečnosti

Rola:	Architekt kybernetickej bezpečnosti
Vedomosti:	<p><b>Riadenie bezpečnosti</b></p> <p>1) procesy, systémy a zásady riadenia informačnej a kybernetickej bezpečnosti vrátane zásad riadenia fyzickej a objektovej bezpečnosti <span style="float: right;">BL5</span></p> <p>2) zásady organizácie informačnej a kybernetickej bezpečnosti <span style="float: right;">BL5</span></p> <p>3) terminológia a skratky v oblasti informačnej a kybernetickej bezpečnosti <span style="float: right;">BL5</span></p> <p>4) princípy riadenia IT služieb, správy systémov a správy počítačových sietí <span style="float: right;">BL5</span></p> <p>5) hodnotiace a validačné kritériá v oblasti kybernetickej bezpečnosti (KPI, KRI, metodiky merania vyspelosti atď.) <span style="float: right;">BL5</span></p> <p>6) zdroje, charakteristiky a použitie informačných aktív organizácie <span style="float: right;">BL5</span></p> <p>7) organizačné politiky, organizačné štruktúry a koncepty plánovania vzťahov s internými a/alebo externými organizáciami <span style="float: right;">BL5</span></p> <p>8) koncepcie zlepšovania organizačných procesov a modely hodnotenia vyspelosti procesov (napr. CMMI) <span style="float: right;">BL5</span></p> <p>9) procesy riadenia continuity činností a plánovania havarijnej obnovy prevádzky <span style="float: right;">BL6</span></p> <p>10) princípy podnikovej architektúry, koncepcie bezpečnostnej architektúry a referenčné modely podnikovej architektúry (napr. TOGAF, Zachman, FEA atď.) <span style="float: right;">BL6</span></p> <p>11) koncepty, terminológia a princípy prevádzky elektronických komunikačných systémov (počítačové a telefónne siete, satelitné, optické, bezdrôtové atď.) <span style="float: right;">BL6</span></p> <p>12) model OSI, mapovanie siete, topológia sietí, hlavné sieťové protokoly a sieťové služby <span style="float: right;">BL5</span></p> <p>13) princípy sieťových zariadení (rozbočovače, prepínače, smerovače, brány, firewall atď.) <span style="float: right;">BL5</span></p> <p>14) zásady riadenia dodávateľských služieb a obstarávania informačných systémov vrátane vyhodnocovania dôveryhodnosti dodávateľa alebo výrobcu <span style="float: right;">BL2</span></p> <p>15) charakteristiky fyzických a virtuálnych nosičov údajov <span style="float: right;">BL5</span></p> <p>16) elektronické zariadenia (napr. počítačové systémy/komponenty, zariadenia na kontrolu prístupu, <span style="float: right;">BL5</span></p>

	digitálne fotoaparáty, digitálne skenery, pevné disky, pamäťové karty, modemy, sieťové komponenty, sieťové zariadenia, sieťové domáce ovládacie zariadenia, tlačiarne, vymeniteľné úložné zariadenia, telefóny, faxy atď.)	
17)	elektrotechnika aplikovaná na architektúru počítačov (napr. základné dosky, procesory, čipy a iný počítačový hardvér)	BL4
18)	konceptia a mechanizmy zálohovania a obnovy dát	BL6
19)	kryptografické algoritmy	BL5
20)	kryptografické mechanizmy pre ochranu dôvernosti údajov (napr. šifrovacie algoritmy a steganografia)	BL5
21)	kryptografické mechanizmy pre ochranu integrity a nepopierateľnosti údajov	BL5
22)	metódy a politiky správy a štandardizácie údajov	BL5
23)	nové a rozvíjajúce sa informačné technológie a technológie kybernetickej bezpečnosti	BL6
24)	princípy dolovania a ukladania údajov	BL5
25)	princípy elektronickej pošty, vyhľadávacích/analytických techník, nástrojov a používania súborov cookie	BL6
26)	princípy webových služieb (napr. architektúra orientovaná na služby, protokol SOAP a jazyk HTML)	BL6
27)	princípy zálohovania a obnovy dát	BL6
28)	programovacie rozhrania pre prístup k databázam	BL4
29)	šifrovacie algoritmy pre lokálne bezdrôtové siete (WLAN)	BL5
30)	systémy riadenia bázy dát a ich správa, dopytovacie jazyky, tabuľkové vzťahy	BL4
31)	štandardy a metodiky klasifikácie údajov založených na citlivosti a iných rizikových faktoroch	BL5
32)	technológie filtrovania webového obsahu	BL5
33)	terminológia dátovej komunikácie (napr. sieťové protokoly, Ethernet, IP, šifrovanie, optické zariadenia, vymeniteľné médiá)	BL6
34)	typy sieťovej komunikácie (napr. LAN, WAN, MAN, WLAN, WWAN)	BL6
35)	typy webových stránok, správa, funkcie a systémy na správu obsahu (CMS)	BL5
36)	XML schémy (Extensible Markup Language)	BL4
37)	koncepty kybernetických operácií, terminológia/slovník (t. j. príprava prostredia, kybernetický útok, kybernetická obrana), zásady, obmedzenia a účinky	BL5
38)	základy sieťovej a internetovej komunikácie (t. j. zariadenia, konfigurácia zariadení hardvér, softvér,	BL5

	<p>aplikácie, porty/protokoly, adresovanie, sieťová architektúra a infraštruktúra, smerovanie, operačné systémy atď.)</p>	
39)	princípy zraniteľností bezdrôtových sietí	BL5
	<b>Riadenie hrozieb a rizík</b>	
1)	procesy riadenia rizík, postupy a metodiky analýzy rizík	BL3
2)	typické kybernetické bezpečnostné hrozby a zraniteľnosti a metódy ich identifikácie	BL6
3)	zásady aplikačnej bezpečnosti	BL6
4)	teória, koncepty a metódy systémového inžinierstva	BL6
5)	metódy a techniky softvérového inžinierstva vrátane modelov vývoja softvéru, princípy životného cyklu vývoja systémov a zásady bezpečného vývoja softvéru	BL6
6)	bezpečnostné koncepty v operačných systémoch	BL5
7)	bezpečnostné mechanizmy a metódy v softvérovom inžinierstve (napr. modularizácia, vrstvenie, abstrakcia, maskovanie, šifrovanie, pseudonymizácia, minimalizácia spracúvania atď.)	BL6
8)	techniky a metódy riadenia konfigurácií a vplyv konfigurácií na bezpečnosť	BL6
9)	nástroje na posudzovanie zraniteľností	BL5
10)	sieťové protokoly a adresárové služby	BL6
11)	architektúra operačných systémov (napr. riadenie systémových procesov, štruktúra adresárov, inštalácia a spúšťanie procesov a aplikácií)	BL6
12)	prevádzka webových stránok (napr. webové servery, hosting, DNS, webové jazyky atď.)	BL6
13)	všeobecné koncepty operačných technológií a riadiacich systémov (OT/ICS)	BL6*
14)	posudzovanie sieťových útokov a vzťahu jednotlivých typov sieťových útokov k hrozbám a zraniteľnostiam	BL5
15)	princípy a techniky etického hackingu	BL3
16)	princípy a zdroje získavania informácií o zraniteľnostiach (napr. varovania, rady, bulletiny)	BL5
17)	triedy a vektory útokov	BL6
	<b>Aplikácia bezpečnostných opatrení</b>	
1)	navrhovanie opatrení na ošetrovanie bezpečnostných rizík	BL6
2)	bezpečnostné mechanizmy a spôsob ich implementácie	BL6
3)	bezpečnostné opatrenia vo fyzickej a objektovej bezpečnosti	BL6

4) nástroje, metódy a techniky navrhovania bezpečnostných systémov	BL6
5) zásady personálnej bezpečnosti	BL6
6) opatrenia týkajúce sa používania, spracovania, uchovávania a prenosu údajov	BL6
7) zásady a princípy riadenia identít a prístupov	BL6
8) kryptografické bezpečnostné mechanizmy	BL6
9) koncepcie a technológie vzdialeného prístupu	BL6
10) virtualizačné technológie, vývoj a údržba virtuálnych strojov	BL6
11) zabezpečenie virtuálnych privátnych sietí (VPN)	BL6
12) techniky a metódy správy systémov a hardeningu systémov	BL6
<b>Výkon operatívnych bezpečnostných činností</b>	
1) znalosti o štádiách kybernetického útoku (napr. prieskum, skenovanie, získanie prístupu, eskalácia oprávnení, využitie, zahľadanie stôp)	BL5
2) zásady určovania bezpečnostne relevantných zdrojov informácií a princípy tvorby prípadov použitia	BL6
3) princípy logovania a bezpečnostného monitorovania	BL6
4) princípy korelácie bezpečnostných udalostí	BL6
5) bezdrôtové technológie (napr. celulárne, satelitné, GSM) zahŕňajúce základnú štruktúru, architektúru a dizajn moderných bezdrôtových komunikačných systémov	BL5
6) charakteristiky komunikačných sietí (napr. kapacita, funkčnosť, trasy, kritické uzly)	BL2
7) forenzné súvislosti štruktúry a procesov operačného systému	BL2
8) koncepcia architektúry sietí vrátane topológie, protokolov, komponentov a bezpečnostných princíпов	BL6
9) mechanizmy zabezpečenia siete (napr. Host based IDS, IPS, ACL) vrátane ich funkcií a umiestnenia v sieti	BL6
10) metódy a nástroje analýzy sieťového prenosu	BL5
11) porty a služby Windows/Unix	BL6
12) princípy a mechanizmy zabezpečenia siete (napr. šifrovanie, brány firewall, autentifikácia, medové pasce, ochrana perimetra)	BL6
13) princípy hĺbkovej ochrany a architektúry sieťovej bezpečnosti	BL6
14) princípy súborových systémov (napr. NTFS, FAT a iné)	BL6
15) programy, úlohy a zodpovednosti a metódy reakcie na incidenty v organizácii	BL6

	<p>16) bezpečnostné zásady správy a údržby databázových systémov BL5</p> <p>17) zásady riadenia bezpečnosti prostredia cloudu BL6</p> <p>18) základy digitálnej forenzej analýzy pri získavaní použiteľných informácií BL4</p> <p>19) zásady riadenia sieťových systémov, modely, metódy (napr. monitorovanie výkonnosti systémov end-to-end) BL5</p> <p>20) princípy zraniteľností bezdrôtových sietí BL5</p> <p><b>Riadenie súladu</b></p> <p>1) právne predpisy, požiadavky na súlad a technické normy vzťahujúce sa na kybernetickú bezpečnosť BL5</p> <p>2) právne predpisy, požiadavky na súlad a technické normy vzťahujúce sa na ochranu osobných údajov BL5</p> <p>3) právne predpisy, požiadavky na súlad a technické normy vzťahujúce sa na prevádzku informačných a komunikačných technológií BL5</p> <p>4) požiadavky právnych predpisov na bezpečnostnú dokumentáciu a bezpečnostné politiky BL5</p> <p>5) princípy posudzovania kybernetickej bezpečnosti BL5</p> <p>6) politiky, procesy a postupy pre riadenie ľudských zdrojov v organizácii BL5</p> <p>7) štandardy bezpečnosti platobných kariet (PCI) BL6*</p> <p>8) štandardy a procesy riadenia rizík v dodávateľskom reťazci BL5*</p> <p>9) metódy testovania a vyhodnocovania bezpečnosti systémov BL5</p>
Zručnosti:	<p><b>Riadenie bezpečnosti</b></p> <p>a) podpora riadenia informačnej a kybernetickej bezpečnosti organizácie</p> <p>b) vypracovanie a prezentácia bezpečnostných stratégií a konceptov</p> <p>c) 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</p> <p><b>Riadenie hrozieb a rizík</b></p> <p>a) podpora implementácie procesov a nástrojov identifikácie, analýzy a monitoringu bezpečnostných hrozieb a rizík</p> <p>b) návrh opatrení na ošetrovanie rizík a na zamedzenie dopadov bezpečnostných udalostí</p> <p>c) hodnotenie technických zraniteľností systémov</p>

	<p><b>Aplikácia bezpečnostných opatrení</b></p> <p>a) návrhy implementácie, zmien a optimalizácie bezpečnostných technológií a riešení</p> <p>b) podpora riadenia bezpečnostnej architektúry</p> <p>c) predkladanie odborných stanovísk k novým zmenám v IT infraštruktúre, ktoré môžu mať potenciálny vplyv na bezpečnosť informačných aktív organizácie</p> <p><b>Výkon operatívnych bezpečnostných činností</b></p> <p>a) výkon činností súvisiacich so zaručením bezpečnosti informačných aktív v zmysle najlepšej praxe</p> <p>b) aplikácia metodík pre klasifikáciu informačných aktív a kategorizáciu sietí a informačných systémov</p> <p>c) riadenie projektov v kybernetickej bezpečnosti</p> <p><b>Riadenie súladu</b></p> <ul style="list-style-type: none"> <li>• budovanie bezpečnostného povedomia pre oblasť informačnej a kybernetickej bezpečnosti a ochrany osobných údajov</li> </ul>		
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"> <li>• najmenej <b>3 roky</b> praxe v oblasti informačných technológií</li> </ul>	<ul style="list-style-type: none"> <li>• najmenej <b>2 roky</b> praxe v oblasti informačných technológií</li> </ul>	<ul style="list-style-type: none"> <li>• najmenej <b>1 rok</b> praxe v oblasti informačných technológií</li> </ul>
Špecifické kľúčové kompetencie	<p>a) schopnosť prijímať rozhodnutia</p> <p>b) schopnosť myslieť a konať v súvislostiach</p> <p>c) analytické myslenie</p> <p>d) tvorivosť (kreativita)</p> <p>e) prezentačná zručnosť</p> <p>f) strategické a koncepčné myslenie</p>		

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