

Tester kybernetickej bezpečnosti

| Rola: | Tester kybernetickej bezpečnosti | |
|------------|--|--|
| Vedomosti: | <p>Riadenie bezpečnosti</p> <ol style="list-style-type: none"> 1) zásady organizácie informačnej a kybernetickej bezpečnosti BL3 2) terminológia a skratky v oblasti informačnej a kybernetickej bezpečnosti BL3 3) princípy riadenia IT služieb, správy systémov a správy počítačových sietí BL3 4) hodnotiace a validačné kritériá v oblasti kybernetickej bezpečnosti (KPI, KRI, metodiky merania vyspelosti atď.) BL3 5) zdroje, charakteristiky a použitie informačných aktív organizácie BL3 6) princípy podnikovej architektúry, koncepcie bezpečnostnej architektúry a referenčné modely podnikovej architektúry (napr. TOGAF, Zachman, FEA atď.) BL3 7) koncepty, terminológia a princípy prevádzky elektronických komunikačných systémov (počítačové a telefónne siete, satelitné, optické, bezdrôtové atď.) BL3 8) model OSI, mapovanie siete, topológia sietí, hlavné sieťové protokoly a sieťové služby BL3 9) princípy sieťových zariadení (rozbočovače, prepínače, smerovače, brány, firewall atď.) BL3 10) charakteristiky fyzických a virtuálnych nosičov údajov BL3 11) elektronické zariadenia (napr. počítačové systémy/komponenty, zariadenia na kontrolu prístupu, digitálne fotoaparáty, digitálne skenery, pevné disky, pamäťové karty, modemy, sieťové komponenty, sieťové zariadenia, sieťové domáce ovládacie zariadenia, tlačiarne, vymeniteľné úložné zariadenia, telefóny, faxy atď.) BL3 12) elektrotechnika aplikovaná na architektúru počítačov (napr. základné dosky, procesory, čipy a iný počítačový hardvér) BL3 13) koncepcia a mechanizmy zálohovania a obnovy dát BL3 14) kryptografické algoritmy BL3 15) kryptografické mechanizmy pre ochranu dôvernosti údajov (napr. šifrovacie algoritmy a steganografia) BL3 16) kryptografické mechanizmy pre ochranu integrity a nepopierateľnosti údajov BL3 17) metódy a politiky správy a štandardizácie údajov BL3 | |

| | |
|---|-----|
| 18) nové a rozvíjajúce sa informačné technológie a technológie kybernetickej bezpečnosti | BL3 |
| 19) princípy dolovania a ukladania údajov | BL3 |
| 20) princípy elektronickej pošty, vyhľadávacích/analytických techník, nástrojov a používania súborov cookie | BL3 |
| 21) princípy webových služieb (napr. architektúra orientovaná na služby, protokol SOAP a jazyk HTML) | BL3 |
| 22) princípy zálohovania a obnovy dát | BL3 |
| 23) programovacie rozhrania pre prístup k databázam | BL3 |
| 24) šifrovacie algoritmy pre lokálne bezdrôtové siete (WLAN) | BL3 |
| 25) systémy riadenia bázy dát a ich správa, dopytovacie jazyky, tabuľkové vzťahy | BL3 |
| 26) štandardy a metodiky klasifikácie údajov založených na citlivosti a iných rizikových faktoroch | BL3 |
| 27) technológie filtrovania webového obsahu | BL3 |
| 28) terminológia dátovej komunikácie (napr. sieťové protokoly, Ethernet, IP, šifrovanie, optické zariadenia, vymeniteľné médiá) | BL3 |
| 29) typy sieťovej komunikácie (napr. LAN, WAN, MAN, WLAN, WWAN) | BL3 |
| 30) typy webových stránok, správa, funkcie a systémy na správu obsahu (CMS) | BL3 |
| 31) XML schémy (Extensible Markup Language) | BL3 |
| 32) koncepty kybernetických operácií, terminológia/slovník (t. j. príprava prostredia, kybernetický útok, kybernetická obrana), zásady, obmedzenia a účinky | BL3 |
| 33) základy sieťovej a internetovej komunikácie (t. j. zariadenia, konfigurácia zariadení hardvér, softvér, aplikácie, porty, protokoly, adresovanie, sieťová architektúra a infraštruktúra, smerovanie, operačné systémy atď.) | BL3 |
| 34) princípy zraniteľností bezdrôtových sietí | BL3 |
| Riadenie hrozieb a rizík | |
| 1) procesy riadenia rizík, postupy a metodiky analýzy rizík | BL3 |
| 2) typické kybernetické bezpečnostné hrozby a zraniteľnosti a metódy ich identifikácie | BL3 |
| 3) zásady aplikačnej bezpečnosti | BL3 |
| 4) teória, koncepty a metódy systémového inžinierstva | BL3 |
| 5) metódy a techniky softvérového inžinierstva vrátane modelov vývoja softvéru, princípy životného cyklu vývoja systémov a zásady bezpečného vývoja softvéru | BL3 |

| | |
|--|------|
| 6) bezpečnostné koncepty v operačných systémoch | BL3 |
| 7) bezpečnostné mechanizmy a metódy v softvérovom inžinierstve (napr. modularizácia, vrstvenie, abstrakcia, maskovanie, šifrovanie, pseudonymizácia, minimalizácia spracúvania atď.) | BL3 |
| 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) architektúra operačných systémov (napr. riadenie systémových procesov, štruktúra adresárov, inštalácia a spúšťanie procesov a aplikácií) | BL3 |
| 12) prevádzka webových stránok (napr. webové servery, hosting, DNS, webové jazyky atď.) | BL3 |
| 13) všeobecné koncepty operačných technológií a riadiacich systémov (OT/ICS) | BL3* |
| 14) posudzovanie sieťových útokov a vzťahu jednotlivých typov sieťových útokov k hrozbám a zraniteľnostiam | BL3 |
| 15) princípy a techniky etického hackingu | BL3 |
| 16) princípy a zdroje získavania informácií o zraniteľnostiach (napr. varovania, rady, bulletiny) | BL3 |
| 17) triedy a vektory útokov | BL3 |
| Aplikácia bezpečnostných opatrení | |
| 1) navrhovanie opatrení na ošetrovanie bezpečnostných rizík | BL3 |
| 2) bezpečnostné mechanizmy a spôsob ich implementácie | BL3 |
| 3) bezpečnostné opatrenia vo fyzickej a objektovej bezpečnosti | BL3 |
| 4) nástroje, metódy a techniky navrhovania bezpečnostných systémov | BL3 |
| 5) zásady personálnej bezpečnosti | BL3 |
| 6) opatrenia týkajúce sa používania, spracovania, uchovávaní a prenosu údajov | BL3 |
| 7) zásady a princípy riadenia identít a prístupov | BL3 |
| 8) kryptografické bezpečnostné mechanizmy | BL3 |
| 9) koncepcie a technológie vzdialeného prístupu | BL3 |
| 10) virtualizačné technológie, vývoj a údržba virtuálnych strojov | BL3 |
| 11) zabezpečenie virtuálnych privátnych sietí (VPN) | BL3 |
| 12) techniky a metódy správy systémov a hardeningu systémov | BL3 |
| Výkon operatívnych bezpečnostných činností | |

| | |
|--|-----|
| 1) znalosti o štádiách kybernetického útoku (napr. Prieskum, skenovanie, získanie prístupu, eskalácia oprávnení, využitie, zahľadanie stôp) | BL3 |
| 2) zásady určovania bezpečnostne relevantných zdrojov informácií a princípy tvorby prípadov použitia | BL3 |
| 3) princípy logovania a bezpečnostného monitorovania | BL3 |
| 4) princípy korelácie bezpečnostných udalostí | BL3 |
| 5) identifikácia digitálnych stôp a postupy pri ich spracúvaní | BL3 |
| 6) princípy, nástroje a techniky testovania prieniku | BL3 |
| 7) analýza sieťového prenosu (nástroje, metodiky, procesy) | BL3 |
| 8) bezdrôtové technológie (napr. celulárne, satelitné, GSM) zahŕňajúce základnú štruktúru, architektúru a dizajn moderných bezdrôtových komunikačných systémov | BL3 |
| 9) charakteristiky komunikačných sietí (napr. kapacita, funkčnosť, trasy, kritické uzly) | BL3 |
| 10) forenzné súvislosti štruktúry a procesov operačného systému | BL3 |
| 11) koncepcia architektúry sietí vrátane topológie, protokolov, komponentov a bezpečnostných princípov | BL3 |
| 12) konfigurácia forenzných laboratórií a podporných aplikácií (napr. VMWare, Wireshark) | BL3 |
| 13) mechanizmy zabezpečenia siete (napr. Host based IDS, IPS, ACL) vrátane ich funkcií a umiestnenia v sieti | BL3 |
| 14) metódy a nástroje analýzy sieťového prenosu | BL3 |
| 15) porty a služby Windows/Unix | BL3 |
| 16) princípy a mechanizmy zabezpečenia siete (napr. šifrovanie, brány firewall, autentifikácia, medové pasce, ochrana perimetra) | BL3 |
| 17) princípy hĺbkovej ochrany a architektúry sieťovej bezpečnosti | BL3 |
| 18) princípy sieťových demilitarizovaných zón | BL3 |
| 19) princípy súborových systémov (napr. NTFS, FAT a iné) | BL3 |
| 20) programy, úlohy a zodpovednosti a metódy reakcie na incidenty v organizácii | BL3 |
| 21) bezpečnostné zásady správy a údržby databázových systémov | BL3 |
| 22) zásady riadenia bezpečnosti prostredia cloudu | BL3 |
| 23) základy digitálnej forenznej analýzy pri získavaní použiteľných informácií | BL3 |
| 24) zásady riadenia sieťových systémov, modely, metódy (napr. monitorovanie výkonnosti systémov end-to-end) | BL3 |
| 25) princípy zraniteľností bezdrôtových sietí | BL3 |

| | |
|--------------------------------|---|
| Zručnosti: | <p>Riadenie bezpečnosti</p> <ul style="list-style-type: none"> • podpora riadenia informačnej a kybernetickej bezpečnosti organizácie <p>Riadenie hrozieb a rizík</p> <ol style="list-style-type: none"> a) posudzovanie hrozieb a rizík b) hodnotenie technických zraniteľností systémov c) detekcia, riešenie, evidencia a prevencia kybernetických bezpečnostných incidentov <p>Aplikácia bezpečnostných opatrení</p> <ol style="list-style-type: none"> a) návrhy zmien a integrácie bezpečnostných technológií a riešení b) podpora riadenia bezpečnostnej architektúry c) monitorovanie plnenia a efektivity bezpečnostných mechanizmov a opatrení <p>Výkon operatívnych bezpečnostných činností</p> <ol style="list-style-type: none"> a) výkon činností súvisiacich so zaručením bezpečnosti informačných aktív v zmysle najlepšej praxe b) prevádzka technických bezpečnostných opatrení <p>Riadenie súladu</p> <ol style="list-style-type: none"> a) pravidelné preskúmavanie stavu kybernetickej a informačnej bezpečnosti b) poskytovanie súčinnosti internému a externému auditu informačnej a kybernetickej bezpečnosti |
| Špecifické kľúčové kompetencie | <ol style="list-style-type: none"> a) analytické myslenie b) tvorivosť (kreativita) |

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