Vysoká škola: Žilinská univerzita v Žiline, KC KYB UNIZA	
Kód kurzu: ŠKBVS	**Názov kurzu:** Špecialista kybernetickej bezpečnosti vo verejnej správe
Druh, rozsah a metóda vzdelávacích činností:	
ISCED_F kód odboru	103, 061
Kapacita kurzu	Max. 25
Metóda, akou sa vzdelávacia činnosť uskutočňuje	Výučba sa uskutočňuje prezenčne alebo online
Metódy dosiahnutia výsledkov vzdelávania	Odporúčané metódy a techniky vyučovania: Prednáška: motivačné rozprávanie (možnosti využitia výsledkov vzdelávania v praxi), výklad, problémový výklad, prezentácia, prezentácia s podporou multimédií, interaktívna prednáška s diskusiou, metóda otázok a odpovedí. Diskusia a praktické cvičenia: diskusia a práca v skupine, riešenie problémov, príprava zadaní, testovanie nadobudnutých vedomostí a zručností.
Záťaž študenta: 50 hodín.	

Podmienky na absolvovanie kurzu:

Vstupné požiadavky:

- Zamestnanec verejnej správy

Priebežné hodnotenie:

- Účasť na kurze: minimálne 75 % (37,5 hodiny z 50).
- Nástroj hodnotenia: prezenčná listina

Záverečné hodnotenie:

- Podmienkou pre úspešné absolvovanie kurzu je získanie minimálne 55 % správnych odpovedí z testu.
- Nástroj hodnotenia: osvedčenie

Výsledky/výstupy vzdelávania:
Absolvent kurzu Špecialista kybernetickej bezpečnosti vo verejnej správe získa rozsiahle teoretické vedomosti v oblasti kybernetickej bezpečnosti, pričom kurz je rozdelený do ôsmich tematických blokov, ktoré systematicky pokrývajú kľúčové oblasti informačnej bezpečnosti a jej riadenia. Jeho absolvovanie poskytuje ucelený teoretický základ pre pochopenie princípov kybernetickej bezpečnosti a umožňuje absolventovi orientovať sa v kľúčových oblastiach ochrany informačných a komunikačných systémov. Absolvent získa schopnosť analyzovať bezpečnostné hrozby, navrhovať opatrenia na minimalizáciu rizík a porozumieť legislatívnym a normatívnym požiadavkám v oblasti informačnej bezpečnosti.

Na úvod sa kurz venuje Riadeniu bezpečnosti, kde absolvent získa poznatky o organizácii a riadení kybernetickej bezpečnosti v súlade s národnými a európskymi reguláciami (NIS2, GDPR, zákon o KB,

ISO/IEC 27000+). Osvojí si koncept systémov manažérstva informačnej bezpečnosti (ISMS), princípy bezpečnostnej dokumentácie a metodiky hodnotenia bezpečnostnej vyspelosti organizácie. Naučí sa zásady správy informačných aktív, riadenia kybernetických rizík a kontinuity činností v prípade incidentov.

Následne kurz prechádza k technickým oblastiam, kde v rámci druhého tematického bloku sa absolvent oboznámi s návrhom a implementáciou bezpečnostnej architektúry IKT infraštruktúry. Bude rozumieť princípom sieťovej bezpečnosti, základným bezpečnostným mechanizmom a riešeniam, ako sú firewally, IDS/IPS, VPN, NAC (Network Access Control), a ich úlohe pri ochrane organizácie. Pochopí prístupy ochrany ako Defense in Depth a Zero Trust a princípy zabezpečenia sieťových topológií.

Následne sa prechádza na problematiku kryptografia a bezpečnej komunikácie, kde sa kurz zameriava na osvojenie si teoretických poznatkov o kryptografických mechanizmoch, vrátane symetrického a asymetrického šifrovania, digitálnych podpisov, PKI infraštruktúry a certifikátov. Kurz sa venuje aj bezpečnosti komunikácie, pričom účastníci získajú prehľad o VPN riešeniach (IPSec, SSL VPN, OpenVPN), bezpečnosti prenosu dát a autentifikácii komunikácie.

Významnú časť kurzu sa venuje ochrane koncových zariadení, kde v bloku Ochrana koncových zariadení a detekcii hrozieb sa absolvent oboznámi s hrozbami pre koncové zariadenia a stratégiami ochrany pred škodlivým kódom. Kurz sa venuje konceptom ako Endpoint Detection and Response (EDR), Extended Detection and Response (XDR), ako aj princípom hostiteľských systémov na prevenciu narušenia (HIPS). V nasledujúcej súvisiacej časti ochrany koncových zariadení sa oboznámi s princípmi Správy zariadení a bezpečnostných nastavení IT systémov. Absolvent pochopí princípy hardeningu systémov a ochrany pred rôznymi typmi malware útokov a nadobudne vedomosti o správe bezpečnosti IKT infraštruktúry, pričom sa oboznámi s procesmi hodnotenia zraniteľností, riadenia záplat a bezpečnej správy zariadení. Získa prehľad o zraniteľnostiach sieťových protokolov (L2, L3, L7), útokoch na IP služby a ich dôsledkoch na bezpečnosť IT infraštruktúry. Bude rozumieť princípom identifikácie a manažmentu zraniteľností (CVE, CWE, CVSS) a možnostiam ich mitigácie pomocou bezpečnostných opatrení a aktualizačných mechanizmov.

Následne v časti Monitorovanie bezpečnosti a riešenie incidentov sa venuje konceptom súvisiacim s monitorovaním zabezpečenia, kde je predstavený koncept bezpečnostných operačných centier (SOC) a ich úlohou pri detekcii a reakcii na bezpečnostné incidenty. Kurz pokrýva aj oblasť monitorovania sieti a súvisiacich problematických oblastí, či metodiky správy bezpečnostných udalostí pomocou SIEM a SOAR systémov a zásady digitálnej forenznej analýzy kybernetických incidentov. Absolvent sa naučí princípy záznamu a analýzy bezpečnostných logov, identifikácie korelácií medzi bezpečnostnými udalosťami a detekcie anomálií.

K záveru kurzu absolvent získa prehľad o bezpečnostných výzvach spojených s cloud computingom, IoT zariadeniami a využitím umelej inteligencie v kybernetickej bezpečnosti. Kurz pokrýva aj koncept Cyber Threat Intelligence (CTI), ktorý sa využíva na predikciu a analýzu kybernetických hrozieb.

Finálne v časti Penetračné testovanie a bezpečnostné povedomie sa zameriavame na teoretické princípy penetračného testovania a najpoužívanejšie metodiky hodnotenia bezpečnosti systémov, ktoré môžu využiť v svojej praxi. Absolvent sa oboznámi s postupmi etického hackingu, metodológiami ako OWASP a NIST, a princípmi sociálneho inžinierstva. Kurz sa venuje aj stratégiám zvyšovania bezpečnostného povedomia v organizáciách a školeniam zameraným na obranu proti phishingu a iným formám kybernetických útokov.

Profil absolventa:

Absolvent kurzu Špecialista kybernetickej bezpečnosti vo verejnej správe má pokročilé teoretické vedomosti v oblasti riadenia a technických aspektov kybernetickej bezpečnosti a orientuje sa v

legislatívnych požiadavkách (napr. NIS2 Directive, General Data Protection Regulation). Rozumie princípom ISMS, riadeniu rizík, bezpečnostnej architektúre, kryptografii, ochrane zariadení a monitorovaniu bezpečnosti. Je schopný analyzovať hrozby, identifikovať zraniteľnosti a navrhovať opatrenia na ochranu informačných systémov.

Stručná osnova/obsah kurzu:

1. Riadenie bezpečnosti (Blok I):
    a. Organizácia a riadenie informačnej bezpečnosti a kybernetickej bezpečnosti
    b. Správa aktív a riadenie kybernetických rizík
    c. Riadenie kontinuity činností
    d. Riadenie súladu
2. Sieťová bezpečnostná architektúra (Blok II):
    a. Sieťové topológie, bezpečnostné zariadenia a služby
    b. Mechanizmy autentifikácie a autorizácie
    c. Mechanizmy riadenia prístupu
3. Kryptografia, ochrana dát a bezpečná komunikácia (Blok III):
    a. Základy kryptografie a ochrany dát
    b. Bezpečná komunikácia
4. Ochrana koncových zariadení (Blok IV):
    a. Malvér a základné stratégie prevencie a detekcie
    b. Bezpečnostné riešenia na ochranu koncových zariadení
5. Bezpečná správa zariadení
    a. Procesy a nástroje pre bezpečnú správu zariadení
    b. Zraniteľnosti a útoky na sieťové protokoly a služby
    c. Identifikácia, hodnotenie a riešenie zraniteľností
6. Monitorovanie bezpečnostných udalostí, riešenie incidentov, forenzná analýza
    a. Výhody SOC centier
    b. Koncept funkčného monitorovania
    c. SIEM a SOAR
    d. Problémy pri monitorovaní
    e. Riešenie incidentov
    f. Digitálna forenzná analýza
7. Moderné technológie, bezpečnosť cloudu a IoT
    a. Bezpečnosť cloudu
    b. Spravodajstvo o hrozbách (CTI)
    c. Umelá inteligencia v KB
    d. Bezpečnosť IoT
8. Zvyšovanie povedomia o KB a testovanie bezpečnosti
    a. Bezpečnostné povedomie a tréningy zamestnancov
    b. Bezpečnostné testovanie a ofenzívne zručnosti

Kontakt: doc. Ing. Radoslav Jankal, PhD., kcskolenia@uniza.sk, +421 41 513 4459

Garant kurzu: prof. Ing. Pavel Segeč, PhD.

Vyučujúci:
prof. Ing. Tomáš Loveček, PhD., doc. Ing. Katarína Kampová, PhD., prof. Ing. Pavel Segeč, PhD., Ing. Tomáš Majer, PhD., Mgr. Jana Uramová, PhD., doc. Ing. Marek Moravčík, PhD., Ing. Ondrej Škvarek, PhD., doc. Ing. Jozef Papán, PhD., Ing. Martin Kontšek, PhD., Ing. Dalibor Kafka

Schválil: prof. Ing. Pavel Segeč, PhD. (garant ŠP)