Vzdelávací program: Architekt kybernetickej bezpečnosti

Profil absolventa

Absolvent vzdelávacieho programu „Architekt kybernetickej bezpečnosti“ je odborník schopný navrhovať, implementovať a optimalizovať komplexné bezpečnostné architektúry a stratégie pre informačné systémy organizácie. Disponuje hĺbkovými vedomosťami o riadení kybernetickej bezpečnosti, podnikových architektúrach, sieťových technológiách, kryptografických mechanizmoch a riadení rizík. Je pripravený navrhovať bezpečnostné riešenia, podporovať riadenie bezpečnostných procesov a koordinovať projekty kybernetickej bezpečnosti. Absolvent kombinuje technické, analytické a strategické zručnosti na zabezpečenie ochrany informačných aktív v súlade s právnymi a technickými normami.

Kľúčové kompetencie absolventa:

1. **Vedomosti**:
   - Ovláda procesy riadenia kybernetickej bezpečnosti, vrátane fyzickej a objektovej bezpečnosti (BL 5–6).
   - Rozumie terminológii, štandardom (napr. TOGAF, CMMI, PCI) a metodikám hodnotenia vyspelosti procesov (BL 5–6).
   - Pozná princípy podnikovej architektúry, sieťových technológií, kryptografických algoritmov a správy dát (BL 4–6).
   - Chápe procesy riadenia rizík, kontinuity činností, havarijnej obnovy a analýzy hrozieb (BL 3–6).
   - Má prehľad o nových technológiách, sieťových protokoloch, virtualizácii, cloudových prostrediach a bezpečnostných mechanizmoch (BL 5–6).
   - Rozumie právnym predpisom a normám týkajúcim sa kybernetickej bezpečnosti a ochrany údajov (BL 5).
2. **Zručnosti**:
   - Navrhuje a implementuje bezpečnostné architektúry a stratégie.
   - Podporuje riadenie bezpečnostných procesov a koordinuje projekty kybernetickej bezpečnosti.
   - Identifikuje a analyzuje bezpečnostné hrozby, navrhuje opatrenia na ich mitigáciu.
   - Implementuje bezpečnostné mechanizmy (napr. šifrovanie, VPN, hardening systémov).
   - Aplikuje metodiky klasifikácie aktív a kategorizácie sietí.
   - Poskytuje odborné stanoviská k zmenám v IT infraštruktúre a buduje bezpečnostné povedomie.
3. **Postoje**:
   - Proaktívny a strategický prístup k návrhu bezpečnostných riešení.
   - Zodpovednosť za ochranu informačných aktív a súlad s normami.
   - Etické správanie pri práci s citlivými údajmi a technológiami.
   - Schopnosť efektívne komunikovať s technickými tímami a vedením.
4. **Špecifické kompetencie**:
   - Schopnosť prijímať rozhodnutia a myslieť v súvislostiach.

- Analytické a strategické myslenie pri návrhu architektúr.
- Tvorivosť a prezentačné zručnosti pri navrhovaní a obhajobe riešení.

Požiadavky na vstup:

- **Vzdelanie**: Úplné stredné všeobecné alebo odborné, vysokoškolské I., II. alebo III. stupňa.
- **Odborná prax**:
  - Minimálne 1–3 roky praxe v oblasti informačných technológií, v závislosti od úrovne vzdelania.

Metódy vzdelávania

Vzdelávací program kombinuje teoretické, praktické a projektové metódy zamerané na rozvoj technických a strategických zručností:

1. **Interaktívne prednášky**:
   - Vysvetlenie podnikových architektúr (napr. TOGAF, Zachman), kryptografických mechanizmov a riadenia rizík.
   - Diskusie o štandardoch (napr. PCI, ISO) a nových technológiách (napr. cloud, virtualizácia).
2. **Praktické laboratóriá**:
   - Návrh bezpečnostných architektúr a konfigurácia bezpečnostných mechanizmov (napr. firewally, VPN).
   - Simulácie kybernetických útokov a analýza zraniteľností pomocou nástrojov (napr. Nessus, Wireshark).
   - Nácvik hardeningu systémov a správy sietí.
3. **Prípadové štúdie**:
   - Analýza reálnych scenárov návrhu bezpečnostnej architektúry alebo reakcie na incidenty.
   - Skupinové projekty na kategorizáciu informačných aktív a návrh plánov obnovy.
4. **Workshopy a simulácie**:
   - Workshopy na návrh bezpečnostných riešení a implementáciu kryptografických mechanizmov.
   - Role-playing scenáre na koordináciu bezpečnostných projektov a komunikáciu s dodávateľmi.
5. **E-learning a samoštúdium**:
   - Prístup k online kurzom, technickým manuálom a certifikačným prípravám (napr. CISSP, TOGAF).
   - Interaktívne moduly na precvičenie správy sietí, šifrovania a analýzy rizík.
6. **Mentorované projekty**:
   - Samostatné alebo tímové projekty na návrh bezpečnostnej architektúry alebo plánu kontinuity.
   - Mentorovanie zamerané na rozvoj strategického myslenia a technických zručností.

Forma vzdelávania

Program je navrhnutý ako kombinovaný, aby vyhovoval odborníkom s rôznymi časovými a technickými požiadavkami:

1. **Prezenčná forma**:
    - Intenzívne školenia v technologických laboratóriách vybavených na simuláciu sietí a bezpečnostných systémov.
    - Vhodné na praktické cvičenia, workshopy a tímové projekty.
    - Trvanie: 4 dni.
2. **Online forma**:
    - Vzdelávanie cez bezpečné videokonferenčné platformy s dôrazom na teoretické prednášky a diskusie.
    - Prístup k e-learningovým platformám s nahratými prednáškami a samoštudijnými materiálmi.
    - Vhodné pre samoštúdium a vzdialený prístup.
3. **Kombinovaná forma**:
    - Kombinácia prezenčných laboratórií a online samoštúdia.
    - Účastníci absolvujú praktické cvičenia na mieste a teoretickú časť online, čo zvyšuje flexibilitu.

Metódy hodnotenia

Hodnotenie je zamerané na overenie teoretických vedomostí, technických zručností a schopnosti navrhovať bezpečnostné riešenia:

1. **Znalostné testy**:
    - Písomné alebo online testy zamerané na podnikové architektúry, kryptografiu, riadenie rizík a právne normy.
    - Formát: kombinácia otázok s výberom odpovedí, esejí a analýzy scenárov.
2. **Praktické projekty**:
    - Návrh bezpečnostnej architektúry pre modelovú organizáciu.
    - Implementácia bezpečnostných mechanizmov (napr. VPN, šifrovanie) v simulačnom prostredí.
    - Hodnotí sa technická presnosť, kreativita a súlad s normami.
3. **Prípadové štúdie**:
    - Analýza hypotetického alebo reálneho bezpečnostného scenára a návrh opatrení.
    - Hodnotí sa schopnosť identifikovať hrozby, navrhnúť riešenia a kategorizovať aktíva.
4. **Prezentácie a ústne skúšanie**:
    - Prezentácia návrhu bezpečnostnej architektúry alebo stratégie pred komisiou.
    - Hodnotí sa prezentačná zručnosť, argumentácia a schopnosť obhájiť riešenia.
5. **Simulácie projektov**:
    - Koordinácia modelového bezpečnostného projektu (napr. návrh siete s ochranou perimetra).
    - Hodnotí sa schopnosť riadiť projekt, aplikovať metodiky a komunikovať s tímom.

Kritériá úspešnosti:

- Úspešné absolvovanie programu vyžaduje dosiahnutie minimálne 80 % úspešnosti v znalostných testoch, praktických projektoch a simuláciách.
- Účastníci obdržia certifikát o absolvovaní programu po splnení všetkých požiadaviek.

Záver

Vzdelávací program „Architekt kybernetickej bezpečnosti“ pripravuje odborníkov na návrh a implementáciu komplexných bezpečnostných architektúr v dynamickom technologickom prostredí. Kombinácia teoretických prednášok, praktických laboratórií a projektov zaisťuje, že absolventi sú schopní navrhovať efektívne bezpečnostné riešenia, podporovať riadenie bezpečnosti a zabezpečovať súlad s právnymi a technickými normami.