Vzdelávací program: Špecialista kybernetickej bezpečnosti

Profil absolventa

Absolvent vzdelávacieho programu „Špecialista kybernetickej bezpečnosti“ je odborník schopný navrhovať, implementovať a spravovať procesy a opatrenia informačnej a kybernetickej bezpečnosti v organizácii. Disponuje hĺbkovými vedomosťami o riadení bezpečnosti, hrozieb, rizík, aplikácii bezpečnostných opatrení a súladu s právnymi predpismi. Ovláda pokročilé techniky správy sietí, kryptografických mechanizmov, forenznej analýzy a monitorovania bezpečnostných incidentov. Absolvent je pripravený na riadenie bezpečnostných projektov, spoluprácu s audítormi a orgánmi verejnej moci, ako aj na budovanie bezpečnostného povedomia zamestnancov.

Kľúčové kompetencie absolventa:

1. **Vedomosti**:
    - Ovláda procesy riadenia informačnej a kybernetickej bezpečnosti, vrátane fyzickej a objektovej bezpečnosti (BL 4–6).
    - Rozumie terminológii, štandardom a metodikám kybernetickej bezpečnosti (napr. KPI, KRI, CMMI, TOGAF) (BL 4–6).
    - Pozná princípy správy IT služieb, sietí, databáz, kryptografických algoritmov a technológií (napr. šifrovanie, VPN, hardening systémov) (BL 4–6).
    - Chápe koncepty kybernetických operácií, forenznej analýzy, sieťovej bezpečnosti a riadenia kontinuity činností (BL 3–6).
    - Rozumie právnym predpisom a normám týkajúcim sa kybernetickej bezpečnosti, ochrany údajov a bezpečnostnej dokumentácie (BL 3–5).
    - Má prehľad o nových a rozvíjajúcich sa technológiách a ich bezpečnostných aspektoch (BL 6).
2. **Zručnosti**:
    - Implementuje a spravuje procesy kybernetickej bezpečnosti v súlade s právnymi predpismi a internými politikami.
    - Identifikuje, analyzuje a ošetruje bezpečnostné hrozby a riziká, vrátane technických zraniteľností.
    - Navrhuje a implementuje bezpečnostné opatrenia, vrátane kryptografických mechanizmov, VPN a správy identít.
    - Vykonáva operatívne činnosti, ako je monitorovanie bezpečnostných incidentov, forenzná analýza a testovanie prieniku.
    - Podporuje audity, školenia zamestnancov a budovanie bezpečnostného povedomia.
    - Riadi bezpečnostné projekty a spolupracuje s dodávateľmi a orgánmi verejnej moci.
3. **Postoje**:
    - Proaktívny a zodpovedný prístup k riadeniu bezpečnosti a ochrane údajov.
    - Strategické a analytické myslenie pri navrhovaní bezpečnostných riešení.
    - Etické správanie pri manipulácii s citlivými údajmi a riešení bezpečnostných incidentov.

    - Schopnosť efektívne komunikovať a školiť zamestnancov v oblasti bezpečnosti.
4. **Špecifické kompetencie**:
    - Schopnosť rozhodovania, analytické a strategické myslenie.
    - Kreativita pri navrhovaní bezpečnostných riešení.
    - Prezentačné zručnosti a schopnosť odovzdávať znalosti.
    - Organizačné a plánovacie schopnosti.

Požiadavky na vstup:

- **Vzdelanie**: Úplné stredné všeobecné alebo odborné, vysokoškolské I., II. alebo III. stupňa.
- **Odborná prax**:
    - Minimálne 2–3 roky praxe v oblasti IT.
    - Z toho aspoň 1 rok v riadení IT služieb, informačnej bezpečnosti, riadenia rizík alebo IT architektúry.

Metódy vzdelávania

Vzdelávací program kombinuje teoretické a praktické metódy s dôrazom na pokročilé technické a strategické zručnosti:

1. **Interaktívne prednášky**:
    - Vysvetlenie komplexných pojmov (napr. kryptografické algoritmy, sieťová bezpečnosť, riadenie rizík) pomocou prezentácií, diagramov a videí.
    - Diskusia o štandardoch (TOGAF, CMMI) a právnych predpisoch.
2. **Praktické laboratóriá**:
    - Simulácie kybernetických útokov (napr. phishing, DDoS) a testovanie prieniku.
    - Konfigurácia bezpečnostných mechanizmov (firewall, VPN, IDS/IPS).
    - Nácvik forenznej analýzy a analýzy sieťového prenosu pomocou nástrojov ako Wireshark.
3. **Prípadové štúdie a analýzy**:
    - Analýza reálnych bezpečnostných incidentov a návrh opatrení na ich prevenciu.
    - Skupinové projekty na návrh bezpečnostnej architektúry alebo plánu obnovy po havárii.
4. **Workshopy a simulácie**:
    - Role-playing scenáre na riešenie bezpečnostných incidentov a koordináciu reakcií.
    - Workshopy na hardening systémov, správu identít a konfiguráciu sietí.
5. **E-learning a samoštúdium**:
    - Prístup k online kurzom, technickým manuálom a certifikačným prípravám (napr. CISSP, CISM).
    - Interaktívne kvízy na overenie vedomostí o sieťových protokoloch, šifrovaní a metodikách.
6. **Mentorované projekty**:
    - Samostatné alebo tímové projekty zamerané na návrh bezpečnostných opatrení alebo analýzu rizík pod dohľadom lektora.

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, serverov a bezpečnostných nástrojov.
   - Vhodné na praktické cvičenia, workshopy a diskusie.
   - Trvanie: 5 dní.
2. **Online forma**:
   - Vzdelávanie cez bezpečné videokonferenčné platformy s dôrazom na praktické ukážky.
   - Prístup k e-learningovým platformám s nahratými prednáškami, technickými simuláciami 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, čím sa zabezpečuje flexibilita.

Metódy hodnotenia

Hodnotenie je zamerané na overenie teoretických vedomostí, praktických zručností a schopnosti aplikovať bezpečnostné princípy:

1. **Znalostné testy**:
   - Písomné alebo online testy zamerané na terminológiu, štandardy (napr. TOGAF, PCI), kryptografiu a právne predpisy.
   - Formát: kombinácia otázok s výberom odpovedí, esejí a priraďovacích úloh.
2. **Praktické skúšky**:
   - Konfigurácia bezpečnostných systémov (napr. firewall, VPN) a analýza sieťového prenosu.
   - Simulácia reakcie na kybernetický incident (napr. detekcia a mitigácia útoku).
   - Návrh bezpečnostnej architektúry alebo plánu obnovy po havárii.
3. **Prípadové štúdie**:
   - Analýza a návrh riešenia reálneho alebo hypotetického bezpečnostného incidentu.
   - Hodnotí sa schopnosť identifikovať hrozby, navrhnúť opatrenia a aplikovať metodiky (napr. riadenie rizík).
4. **Projektové úlohy**:
   - Samostatný alebo tímový projekt (napr. návrh bezpečnostnej politiky, implementácia opatrení).
   - Hodnotí sa kreativita, technická presnosť a súlad s normami.
5. **Ústne skúšanie**:
   - Prezentácia návrhu bezpečnostného riešenia alebo analýzy incidentu pred komisiou.
   - Hodnotí sa schopnosť argumentovať, komunikovať a obhájiť svoje rozhodnutia.

Kritériá úspešnosti:

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

Záver

Vzdelávací program „Špecialista kybernetickej bezpečnosti“ poskytuje komplexnú prípravu na riadenie a implementáciu bezpečnostných procesov v organizácii. Kombinácia teoretických prednášok, praktických laboratórií a projektov zaisťuje, že absolventi sú pripravení na pokročilé úlohy v oblasti kybernetickej bezpečnosti, vrátane riadenia