Vzdelávací program: Manažér kybernetickej bezpečnosti

Profil absolventa

Absolvent vzdelávacieho programu „Manažér kybernetickej bezpečnosti“ je vysoko kvalifikovaný odborník schopný strategicky riadiť procesy kybernetickej bezpečnosti v organizácii. Disponuje komplexnými vedomosťami o riadení bezpečnosti, hrozieb, rizík, súladu s právnymi predpismi a aplikácii bezpečnostných opatrení. Má zručnosti v oblasti vedenia tímov, tvorby bezpečnostných stratégií, rozpočtovania a koordinácie s dodávateľmi a orgánmi verejnej moci. Absolvent je pripravený navrhovať a implementovať bezpečnostné politiky, riadiť bezpečnostné audity, budovať povedomie zamestnancov a zabezpečovať kontinuitu činností organizácie v prípade incidentov.

Kľúčové kompetencie absolventa:

1. **Vedomosti**:
    - Ovláda strategické procesy riadenia kybernetickej bezpečnosti, vrátane fyzickej a objektovej bezpečnosti (BL 5–6).
    - Rozumie pokročilej terminológii, štandardom (napr. KPI, KRI, CMMI, TOGAF) a právnym rámcom (napr. GDPR, ePrivacy, ISO 20000) (BL 3–6).
    - Pozná princípy riadenia IT služieb, sietí, podnikovej architektúry, rozpočtovania a plánovania zdrojov (BL 5–6).
    - Chápe procesy riadenia rizík, analýzy hrozieb, kontinuity činností a obnovy po havárii (BL 4–6).
    - Má prehľad o sieťových protokoloch, zariadeniach, operačných technológiách a cloudových prostrediach (BL 2–5).
    - Rozumie vzdelávacím stratégiám a metódam budovania bezpečnostného povedomia (BL 6).
2. **Zručnosti**:
    - Strategicky riadi kybernetickú bezpečnosť a vypracováva bezpečnostné stratégie a dokumentáciu.
    - Implementuje procesy riadenia rizík, hrozieb a bezpečnostných opatrení v súlade s právnymi predpismi.
    - Vedie tímy, koordinuje audity, školenia a spoluprácu s dodávateľmi a orgánmi verejnej moci.
    - Navrhuje rozpočty, monitoruje efektivitu opatrení a riadi projekty kybernetickej bezpečnosti.
    - Zabezpečuje kontinuitu činností a obnovu po incidentoch (Business Continuity, Disaster Recovery).
    - Aplikuje metodiky klasifikácie aktív, hardening systémov a riadenie identít.
3. **Postoje**:
    - Strategický a proaktívny prístup k riadeniu bezpečnosti a ochrane údajov.
    - Zodpovednosť za bezpečnostné politiky a súlad s normami.
    - Etické správanie pri správe citlivých informácií a vedení tímov.
    - Schopnosť efektívne komunikovať s vedením, audítormi a zamestnancami.
4. **Špecifické kompetencie**:

- Schopnosť prijímať rozhodnutia, riešiť konflikty a delegovať úlohy.
- Analytické, strategické a koncepčné myslenie.
- Prezentačné zručnosti a schopnosť viesť vzdelávacie programy.
- Organizačné schopnosti a kreativita pri tvorbe bezpečnostných riešení.

Požiadavky na vstup:

- **Vzdelanie**: Úplné stredné všeobecné alebo odborné, vysokoškolské I., II. alebo III. stupňa.
- **Odborná prax**:
  - Minimálne 3–7 rokov praxe v oblasti IT, z toho 1–5 rokov v riadení IT služieb, informačnej bezpečnosti, riadenia rizík alebo IT architektúry.
  - Medzinárodný certifikát (napr. CISSP, CISM) sa považuje za 1 rok praxe.

Metódy vzdelávania

Vzdelávací program kombinuje strategické, teoretické a praktické metódy s dôrazom na riadiace a koordinačné zručnosti:

1. **Interaktívne prednášky a semináre**:
   - Vysvetlenie strategických konceptov (napr. riadenie rizík, bezpečnostná architektúra, compliance) pomocou prezentácií a prípadových štúdií.
   - Diskusie o štandardoch (TOGAF, ISO 20000) a právnych rámcoch (GDPR, ePrivacy).
2. **Praktické workshopy**:
   - Simulácie riadenia bezpečnostných incidentov a krízových situácií (napr. koordinácia reakcie na DDoS útok).
   - Nácvik tvorby bezpečnostných politík, rozpočtov a plánov obnovy po havárii.
   - Vedenie modelových tímov a delegovanie úloh.
3. **Prípadové štúdie a strategické projekty**:
   - Analýza reálnych bezpečnostných incidentov a návrh strategických opatrení.
   - Tímové projekty na tvorbu bezpečnostnej stratégie alebo rozpočtu pre IT bezpečnosť.
4. **E-learning a samoštúdium**:
   - Prístup k online kurzom, certifikačným prípravám (napr. CISM, CRISC) a materiálom o compliance.
   - Interaktívne moduly na precvičenie riadenia rizík a monitorovania KPI/KRI.
5. **Mentorované riadiace projekty**:
   - Samostatné alebo tímové projekty na návrh bezpečnostnej dokumentácie, stratégie alebo plánu kontinuity.
   - Mentorovanie zamerané na rozvoj strategického myslenia a prezentačných zručností.
6. **Role-playing a simulácie**:
   - Simulácie rokovaní s vedením, audítormi alebo orgánmi verejnej moci.
   - Cvičenia na koordináciu tímov pri riešení bezpečnostných incidentov.

Forma vzdelávania

Program je navrhnutý ako kombinovaný, aby vyhovoval manažérskym pozíciám s obmedzenou časovou dostupnosťou:

1. **Prezenčná forma**:
    - Intenzívne workshopy a semináre v školiacich centrách, zamerané na strategické plánovanie a tímové aktivity.
    - Trvanie: 3 dni (podľa rozsahu programu).
2. **Online forma**:
    - Videokonferenčné školenia cez bezpečné platformy s dôrazom na strategické diskusie a prezentácie.
    - Prístup k e-learningovým platformám s nahratými prednáškami a samoštudijnými materiálmi.
    - Vhodné pre samoštúdium a vzdialený prístup.
3. **Kombinovaná forma**:
    - Kombinácia prezenčných workshopov (napr. na strategické plánovanie) a online samoštúdia.
    - Účastníci absolvujú praktické cvičenia na mieste a teoretickú časť online, čo zvyšuje flexibilitu.

Metódy hodnotenia

Hodnotenie je zamerané na overenie strategických, riadiacich a praktických kompetencií:

1. **Znalostné testy**:
    - Písomné alebo online testy zamerané na terminológiu, právne rámce, štandardy (napr. GDPR, ISO 20000) a riadenie rizík.
    - Formát: otázky, výber z možností.
2. **Praktické projekty**:
    - Vypracovanie bezpečnostnej stratégie, rozpočtu alebo plánu obnovy po havárii.
    - Návrh bezpečnostnej dokumentácie a metrík (KPI/KRI) pre organizáciu.
    - Hodnotí sa strategický prístup, kreativita a súlad s normami.
3. **Prípadové štúdie**:
    - Analýza komplexného bezpečnostného incidentu a návrh riadiacich opatrení.
    - Hodnotí sa schopnosť koordinovať reakcie, komunikovať s vedením a navrhnúť riešenia.
4. **Prezentácie a ústne skúšanie**:
    - Prezentácia bezpečnostnej stratégie alebo plánu pred komisiou.
    - Hodnotí sa prezentačná zručnosť, argumentácia a schopnosť obhájiť návrhy.
5. **Simulácie riadenia**:
    - Simulácia krízového manažmentu (napr. reakcia na kybernetický útok) s dôrazom na vedenie tímu a koordináciu.
    - Hodnotí sa rozhodovanie, delegovanie a efektivita riadenia.

Kritériá úspešnosti:

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

Záver

Vzdelávací program „Manažér kybernetickej bezpečnosti“ pripravuje odborníkov na strategické riadenie kybernetickej bezpečnosti v komplexných organizačných prostrediach. Kombinácia teoretických prednášok, praktických workshopov, projektov a simulácií zaisťuje, že absolventi sú schopní efektívne viesť tímy, navrhovať bezpečnostné stratégie a zabezpečovať súlad s právnymi a technickými normami.