Vzdelávací program: Odborný zamestnanec

Profil absolventa

Absolvent vzdelávacieho programu „Odborný zamestnanec“ disponuje vedomosťami a zručnosťami v oblasti kybernetickej bezpečnosti, ochrany osobných údajov a bezpečného používania informačných a komunikačných technológií (IKT). Je schopný identifikovať a reagovať na bezpečnostné hrozby, dodržiavať bezpečnostné zásady a politiky organizácie, a efektívne manipulovať s citlivými informáciami. Absolvent je pripravený na bezpečnú prácu s IKT v pracovnom prostredí, vrátane vzdialeného prístupu, a rozumie princípom digitálneho súkromia, autentizácie a ochrany pred útokmi sociálneho inžinierstva. Taktiež chápe právne aspekty súvisiace s kybernetickou bezpečnosťou a ochranou údajov.

Kľúčové kompetencie absolventa:

1. **Vedomosti**:
    - Ovláda základné pojmy kybernetickej bezpečnosti, vrátane typov hrozieb (úmyselné, náhodné, environmentálne) a spôsobov útokov (phishing, malware, DDoS, sociálne inžinierstvo).
    - Rozumie významu osobných údajov, citlivých informačných aktív a digitálneho súkromia.
    - Pozná princípy autentizácie, autorizácie, viacfaktorovej autentizácie a bezpečného používania hesiel.
    - Chápe pojmy digitálny podpis, kvalifikovaný elektronický podpis a časová pečiatka.
    - Má základné vedomosti o trestnom práve v oblasti kybernetickej bezpečnosti.
    - Rozumie bezpečnostným rizikám pri používaní sociálnych sietí a telekonferencií.
2. **Zručnosti**:
    - Bezpečne manipuluje s prostriedkami IKT, osobnými údajmi a citlivými informáciami.
    - Používa stanovené bezpečnostné mechanizmy v pracovných procesoch.
    - Rozpoznáva bezpečnostné incidenty a vie na ne správne reagovať.
    - Dodržiava bezpečnostné zásady a politiky organizácie, vrátane zásad pre prácu na diaľku a telekonferencie.
3. **Postoje**:
    - Zodpovedný prístup k ochrane údajov a digitálnemu súkromiu.
    - Proaktívne uplatňovanie bezpečnostných princípov v pracovnom prostredí.
    - Etické správanie pri používaní IKT a sociálnych sietí.

Metódy vzdelávania

Vzdelávací program kombinuje teoretické a praktické metódy s cieľom zabezpečiť efektívne osvojenie vedomostí a zručností:

1. **Prednášky a teoretické semináre**:

    - Vysvetlenie základných pojmov kybernetickej bezpečnosti, typov hrozieb, autentizácie a právnych aspektov.
    - Použitie vizuálnych pomôcok (prezentácie, schémy, videá) na objasnenie komplexných tém, ako sú útoky sociálneho inžinierstva alebo princípy šifrovania.
2. **Praktické cvičenia**:
    - Simulácie bezpečnostných incidentov (napr. rozpoznávanie phishingových e-mailov, reakcie na malware).
    - Nácvik bezpečného používania hesiel a nastavenia viacfaktorovej autentizácie.
    - Praktické úlohy na bezpečné používanie IKT zariadení a vzdialeného prístupu.
3. **Skupinové diskusie a prípadové štúdie**:
    - Analýza reálnych prípadov kybernetických útokov (napr. phishing, DDoS) a diskusia o spôsoboch prevencie.
    - Skupinové riešenie hypotetických bezpečnostných incidentov s dôrazom na tímovú spoluprácu.
4. **E-learning a samoštúdium**:
    - Prístup k online materiálom, kvízom a videám na prehĺbenie vedomostí (napr. o škodlivom kóde, sociálnom inžinierstve).
    - Interaktívne moduly na precvičenie bezpečnostných postupov.
5. **Workshopy a role-playing**:
    - Simulácia telekonferencií s dôrazom na bezpečnostné zásady a etiketu.
    - Role-playing scenáre na rozpoznanie a reakciu na pokusy o sociálne inžinierstvo.

Forma vzdelávania

Vzdelávací program je poskytovaný v kombinovanej forme, aby vyhovoval rôznym potrebám účastníkov:

1. **Prezenčná forma**:
    - Organizované prezenčné školenia v učebniach vybavených IKT (počítače, projektory).
    - Vhodné na praktické cvičenia, workshopy a skupinové diskusie.
    - Trvanie: 2 dni intenzívneho školenia.
2. **Online forma**:
    - Vzdelávanie cez videokonferenčné platformy (napr., MS Teams) s dôrazom na bezpečnostné zásady telekonferencií.
    - Prístup k e-learningovým platformám s nahratými prednáškami a samoštudijnými materiálmi.
    - Vhodné pre vzdialený prístup a samoštúdium.
3. **Kombinovaná forma**:
    - Kombinácia prezenčných workshopov a online samoštúdia, ktorá umožňuje flexibilitu a hlbšie pochopenie tém.
    - Účastníci absolvujú prezenčné praktické cvičenia a teoretickú časť online.

Metódy hodnotenia

Hodnotenie účastníkov je zamerané na overenie vedomostí, zručností a schopnosti aplikovať nadobudnuté kompetencie:

1. **Znalostné testy**:
    - Písomné alebo online kvízy zamerané na kľúčové pojmy (napr. typy hrozieb, autentizácia, digitálne súkromie).
    - Formát: výber z možností, priraďovanie pojmov.
2. **Praktické úlohy**:
    - Simulované scenáre, kde účastníci musia rozpoznať a reagovať na bezpečnostný incident (napr. phishingový e-mail, podozrivý softvér).
    - Nácvik bezpečného nastavenia hesiel a viacfaktorovej autentizácie na modelových zariadeniach.
3. **Prípadové štúdie**:
    - Analýza konkrétneho bezpečnostného incidentu a návrh riešenia (písomne alebo ústne).
    - Hodnotí sa schopnosť identifikovať hrozbu, navrhnúť opatrenia a aplikovať bezpečnostné zásady.
4. **Ústne skúšanie**:
    - Diskusia s lektorom o konkrétnych situáciách (napr. ako reagovať na pokus o sociálne inžinierstvo).
    - Hodnotí sa schopnosť argumentovať a aplikovať teoretické vedomosti.
5. **Hodnotenie praktických zručností**:
    - Pozorovanie pri praktických cvičeniach (napr. bezpečná manipulácia s IKT, nastavenie vzdialeného prístupu).
    - Hodnotí sa dodržiavanie bezpečnostných postupov a etikety.

Kritériá úspešnosti:

- Úspešné absolvovanie programu vyžaduje dosiahnutie minimálne 70 % úspešnosti v znalostných testoch a praktických úlohách.
- Účastníci obdržia certifikát o absolvovaní programu po splnení všetkých požiadaviek.

Záver

Vzdelávací program „Odborný zamestnanec“ je navrhnutý tak, aby poskytol komplexné vedomosti a praktické zručnosti v oblasti kybernetickej bezpečnosti a ochrany údajov. Flexibilná kombinácia prezenčného a online vzdelávania spolu s rôznorodými metódami hodnotenia zabezpečuje efektívne osvojenie kompetencií potrebných pre bezpečnú prácu v modernom pracovnom prostredí.