Bezpečnostné povedomie zamestnancov - vstupné preškolenie

Kód kurzu: BPZ-A

Dvojdňový kurz školí bežných zamestnancov a užívateľov na podnikovú bezpečnosť informácií a ochranu osobných údajov (INFOSEC, ISMS, GDPR), jej požiadavky a zodpovednosť pracovníkov samotných. Kurz je zakončený testom, po jeho úspešnom zložení získa účastník osvedčenie o spôsobilosti. Jedná sa o prvotné dvojdňovej preškolenie. Neskôr je už možné opakovane navštevovať len jednodňový nadväzujúci kurz BPZ-B.

Pre koho je kurz určený

Kurz je určený všetkým užívateľom informačných technológií, najmä zamestnancom organizácií, ktorí majú na starosti bezpečnosť informácií (INFOSEC, ISMS) alebo sú správcovia, alebo majú na starosti spracovanie osobných údajov (GDPR).

Čo vás na kurze naučíme

- Porozumieť dôvodom a dôležitosti ochrany informácií v organizácii
- Pochopiť, čo sú a čo naopak nie sú osobné údaje a ako sa k nim správať
- Byť schopný prijať vlastnú zodpovednosť za svoje správanie pri nakladaní s citlivými podnikovými a osobnými údajmi
- Vedieť ako si správne zvoliť a chrániť heslá a iné prihlasovacie údaje
- Chápať na čo je potrebné šifrovanie, na čo sa využíva a ako si skontrolovať, že sa naozaj šifruje
- Aké sú riziká pri prístupe k podnikovým informáciám z mobilných zariadení, z internetu všeobecne a ako to robiť bezpečne
- Čo znamená fyzická bezpečnosť a ako je nebezpečné nechávať počítačové vybavenie bez dozoru
- Aké existujú technické bezpečnostné opatrenia a aká je alebo nie je ich schopnosť zabrániť útokom a strate dát
- Vidieť niektoré útoky na vlastné oči a pochopiť ako to môže byť jednoduché, ak si človek nedáva pozor

Skúška spôsobilosti

- Na konci kurzu prebieha 30 minútový test
- Odpovede na otázky účastníci vypĺňajú do elektronického testovacieho systému, ktorý výsledok okamžite vyhodnotí
- Odpovede na otázky sa vyberajú z niekoľkých možných, každá otázka môže mať viac správnych odpovedí, ktoré je v takomto prípade potrebné zvoliť všetky (multi-select)
- K testu nesmie mať účastník po ruke nič, nie sú dovolené ani mobilné telefóny, ceruzky ani poznámkové bloky, pripojenie k internetu je odpojené, nie sú povolené ani iné "inteligentné" zariadenia ako hodinky a pod.
- Akákoľvek spolupráca testovaných je zakázaná, v priebehu testu nie je možné opúšťať testovaciu miestnosť
- Úspešné ukončenie skúšky je pri dosiahnutí aspoň 70% správnych odpovedí
- Pri úspešnom zložení skúšky dostane účastník osvedčenie o spôsobilosti na prácu s informáciami v zabezpečenom prostredí
- Osvedčenie o spôsobilosti sa vydáva na dobu neurčitú, ale obsahuje výrazne uvedený dátum jeho získania a postupom času teda prirodzene stráca na aktuálnosti

Osnova kurzu

- Dôležitosť informačnej bezpečnosti pre fungovanie organizácie (ISMS, Infosec)
- Zákonné požiadavky na ochranu osobných údajov (GDPR)
- Čo sú osobné údaje, ako sa k nim správať a na čo nezabudnúť
- Na čo si dať pozor pri zverejňovaní osobných údajov na sociálnych sieťach
- Používateľské mená a heslá pre prihlasovanie do podnikovej počítačovej siete
- Zásady pre správnu voľbu dĺžky a vlastností heslaň
- Čo je a prečo sa používa viac-faktorové prihlasovanie do počítačov a mobilných zariadení
- Ako chrániť prihlasovacie údaje proti útokom ako je keylogger
- Ukladať alebo radšej neukladať heslá na počítačoch?
- Šifrovanie komunikácie ako napríklad HTTPS a ako sa o tom uistiť

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk

Bezpečnostné povedomie zamestnancov - vstupné preškolenie

- Zásady bezpečného pripájania k firemnej pošte a vnútorným webom z mobilných zariadení
- Odkiaľ sa môžem pripájať a odkiaľ naopak nesmiem
- Šifrovaná a nešifrované WiFi, bezpečné VPN pripojenie, pripojenie na vzdialenú plochu
- Šifrovanie diskov a mobilných zariadení ako ochrana proti fyzickému útoku na počítače
- Opatrnosť pri ústnom a papierovom zdieľaní informácií
- Prečo fyzická bezpečnosť, vstupy s kartou a visačkou, hlásenie incidentov a straty alebo krádeže
- Ako rozoznať phishing a ako si dávať pozor na spúšťanie nebezpečných príloh
- Čo sú zero-day útoky, ransomware a (ne) schopnosť antivírusu nákazu odhaliť a zablokovať

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk