

Zásady kybernetické bezpečnosti pro každodenní praxi úředníka

Akreditace Ministerstva vnitra České republiky

Parametry kurzu

Místo Triniti Office Center, Trnitá 491/3, Brno

Lektor Mgr. Emil Budín

Termín 8. července 2020, 9.00 - 15.00

Cena 1 990 Kč (Pro úředníky ÚSC osvobozeno od DPH, pro ostatní plus DPH 21 %)

Postupující proces elektronizace (nejen) v oblasti veřejné správy, spolu se souvisejícími legislativními požadavky, klade na úředníky nové nároky na **kompetence často opomíjené, a to v oboru kybernetické bezpečnosti**. Ochrana počítačového vybavení a digitálních dat, se kterými úředník každý den pracuje totiž neleží pouze na bedrech oddělení ICT nebo bezpečnosti, ale do značné míry závisí na úrovni počítačové a bezpečnostní gramotnosti každého zaměstnance. Od r. 2018, kdy vešlo v platnost obecné nařízení Evropské unie na ochranu údajů, známé též pod akronymem GDPR, je kladen **zvýšený důraz na správné zacházení s osobními údaji občanů právě v souladu s principy kybernetické bezpečnosti**.

Cíle kurzu

Vzdělávací program „Zásady kybernetické bezpečnosti pro každodenní praxi“ si klade za cíl seznámit posluchače s nejdůležitějšími zásadami bezpečné práce s počítačem, a zejména pak s daty na něm zpracovávanými či ukládanými.

Po obecném úvodu do problematiky oboru kybernetické bezpečnosti pokračuje kurz postupným seznamováním jeho účastníků se zásadami počítačové bezpečnosti, které mohou využít nejen v zaměstnání při výkonu své profese úředníka, ale také při práci s jakýmkoliv počítačem či mobilním zařízením kdekoli jinde.

Ochrana digitálních informací před kybernetickými útoky je ústředním problémem oboru kybernetické bezpečnosti, proto je této oblasti věnována náležitá pozornost také v navrhovaném

Cíle kurzu

vzdělávacím programu. Probíraná témata zahrnují klasifikaci informací, problematiku přístupových účtů, hesel, sdílení informací, práci s osobními údaji (mj. v kontextu nařízení GDPR), zabezpečení bankovníctví a dat o kreditních kartách, vč. uvedení souvislostí s relevantními právními předpisy.

Účastníci kurzu budou dále provedeni nejčastějšími kybernetickými hrozbami a vybranými, v minulosti realizovanými, útoky se zaměřením na praktické ukázky, doplněné o objasnění, jaké jsou konkrétní možnosti ochrany proti nim.

Závěrečná část vzdělávacího programu je věnována shrnutí všech – v kurzu probraných – témat patřících do oboru kybernetické bezpečnosti, diskuzi nad složitějšími otázkami a individuálním konzultacím konkrétních problémů vzešlých z praxe účastníků kurzu.

Obsah kurzu

1. Úvod do kybernetické bezpečnosti

2. Počítačová bezpečnost

- Fyzické zabezpečení
- Antivirus
- Firewall
- Aktualizace software
- Šifrování dat
- Zálohování
- E-mailová schránka
- Přístup k internetu

3. Ochrana digitálních informací

- Klasifikace informací
- Přístupové účty, hesla, vícefaktorová autentizace
- Sdílení informací, externí zařízení, cloudová úložiště
- Osobní údaje a GDPR
- Bankovníctví a kreditní karty
- Legislativa

4. Kybernetické hrozby a útoky

- Viry, trojské koně, červi
- Sociální inženýrství
- Phishing, spearphishing, scam
- Ransomware
- Cryptojacking
- Aktuální hrozby

5. Závěr

- Shrnutí
- Diskuze
- Konzultace

Lektor kurzu

Mgr. Emil Budín

Specialista kybernetické bezpečnosti s mnohaletou praxí na různých pozicích ve firmách působících v oborech informačních a bezpečnostních technologií, spoluautor a lektor kurzu počítačové gramotnosti.