

NABÍDKA SPECIALIZOVANÝCH KURZŮ



Nabídka kurzů KB

KB Kurz 1 - Základní pojmy a přehled Kybernetické bezpečnosti (včetně testování účastníka)

Vstupní kurz do problematiky řízení kybernetické bezpečnosti, jehož obsahem je pojmosloví a přehled v rozsahu:

- Základní pojmy
- Rozdělení kybernetické bezpečnosti
- Ohrožení, zranitelnosti, útoky a útočníci
- 7 opatření pro kybernetickou bezpečnost
- Identifikace aktiv, stanovení rizik a priorit bezpečnosti
- Definování bezpečnostního plánu
- Kybernetická bezpečnost homeoffice v režimu BYOD pro uživatele
- Řízení bezpečnosti = PDCA model

KB Kurz 2 - Praktické aspekty kybernetické bezpečnosti (včetně testování účastníka)

Kurz je zaměřen na seznámení se s praktickými aspekty kybernetické bezpečnosti pro uživatele organizace. Rozsah kurzu:

- Legislativa
- Důvěrnost, integrita, dostupnost
- Útoky sociálním inženýrstvím
- Běžné formy škodlivého SW
- Časté chyby při práci s ICT
- Způsoby zabezpečení webových prohlížečů
- Bezpečné používání emailu
- Bezpečné používání sociálních sítí
- Používání šifrování
- Rizika vzdáleného přístupu k IS
- Zajištění wifi s ukázkou
- Bezpečné používání mobilních zařízení
- Bezpečné používání internetu věcí
- Organizační aspekty bezpečnosti orgánu řízení
- Co dělat v případě vzniku bezpečnostního incidentu
- Nejzajímavější incidenty v nedávném období
- Doporučení na závěr

KB Kurz 3 - "10 přikázání" bezpečnosti (bez testování)

Kurz je zaměřen na zvýšení povědomí běžných uživatelů o bezpečnostních rizicích spojených s používáním internetu formou doporučení / podle autora P. Chudý (2013)/

Nabídka kurzů GDPR

GDPR Kurz 1 - Základní školení pro organizace k ochraně osobních údajů (včetně testování účastníka)

Kurz je zaměřen pro zaměstnance organizací. V tomto modulu jsou podrobné informace o problematice ochrany osobních údajů, legislativní základ, souhrn práv a povinností provozovatele a jeho zaměstnanců ve vztahu k dotyčným osobám. Rozsah kurzu:

- Legislativa
- Požadavky na ochranu osobních údajů v SK a EU legislativě
- Soukromí jednotlivce, kontroly a oznámení, transparentnost pravidel, IT
- Základní zásady GDPR
- Základní pojmy ochrany osobních údajů
- Primární aktiva ochrany OÚ
- Co považovat za osobní údaj?
- Kategorie osobních údajů
- Zpracování OÚ zaměstnanců
- Zákonost zpracovávání § 13 právní základy
- Agendy - informační systémy, zpracovatelské činnosti
- Analýza agendy podle účelu
- Zranitelnosti
- Informační povinnost provozovatele
- Odpovědnost organizací za bezpečnost
- Porušení bezpečnosti § 5m
- Dostupnost, důvěrnost, integrita, bezpečnostní incident
- Nejčastější chyby vedoucí k bezpečnostním incidentům
- Bezpečnostní opatření § 39
- Nejvyšší čas věnovat pozornost IT bezpečnosti
- Konkrétní opatření
- Kdo nám ochranu OÚ kontroluje a proč?
- Polehčující okolnosti při porušení ochrany OÚ
- Náhrada škody a nemajetkové újmy
- Komplexnost ochrany OÚ
- Řízení ochrany OÚ
- Vzdělávání zaměstnanců

GDPR Kurz 2 - Bezpečnostní opatření k ochraně osobních údajů (včetně testování účastníka)

Kurz je zaměřen pro zaměstnance organizací. V tomto modulu jsou podrobně rozebrány bezpečnostní opatření na ochranu citlivých aktiv - osobních údajů a vlivu hrozeb prostřednictvím rizik na možnost vzniku bezpečnostních incidentů, návrh, implementace a dodržování bezpečnostních opatření. Rozsah kurzu:

- Primární aktiva ochrany OÚ
- Odpovědnost organizací za bezpečnost
- Porušení bezpečnosti § 5m
- Nejčastější chyby vedoucí k bezpečnostním incidentům - nesoulad ochrany OÚ
- Bezpečnostní opatření § 39
- Příklady standardní ochrany
- Příklady specificky navržené ochrany
- Základní bezpečnostní cíle
- Základní bezpečnostní opatření
- Nejvyšší čas věnovat pozornost IT bezpečnosti
- Ochrana osobních údajů vs. informační bezpečnost
- Ochrana kritické infrastruktury
- Informační a kybernetická bezpečnost
- Konkrétní opatření

GDPR Kurz 3 - Kamerové systémy

Kurz je zaměřen na kamerové systémy z pohledu ochrany osobních údajů / GDPR. Rozsah kurzu:

- Negativní vymezení věcné působnosti GDPR
- Výjimky z působnosti GDPR pro domácí činnosti
- Povinnosti - definování účelu zpracování
- Určení právního základu zpracování
- Oprávněný zájem
- Existence oprávněných zájmů
- Souhlas dotčené osoby při monitorování
- Práva dotčené osoby
- Transparentnost a informační povinnost (1. a 2. vrstva informace)
- Doba uchování a povinnost likvidace
- Technické a organizační opatření

Nabídka kurzů protikorupčního PROGRAM

Protikorupční program Kurz 1 - Základní pojmy a zásady, priority, protikorupční opatření, monitorování a vyhodnocování (včetně testování účastníka)

Kurz je zaměřen na problematiku protispolečenské činnosti. Rozsah kurzu:

- Základní pojmy
- Nepřípustné jednání zaměstnance
- Účel protikorupčního programu
- Legislativa
- Protikorupční zásady
- Priority a cíle
- Seznam protikorupčních opatření
- Monitorování a vyhodnocování

Protikorupční program Kurz 2 - Řízení rizik (včetně testování účastníka)

Kurz je zaměřen na problematiku řízení protikorupčních rizik. Rozsah kurzu:

- Základní pojmy
- Fáze procesu řízení korupčních rizik
- Kritéria pro hodnocení korupčních rizik
- Stupeň významnosti korupčního rizika
- Postup při řízení korupčních rizik v organizaci
- Odpovědnost zaměstnanců při řízení korupčních rizik