



Zagrożenia informatyczne dla pracowników sądów

MIEJSCE:

Wybrane przez
Zamawiającego

DATA:

Wybrana przez
Zamawiającego

CENA:

- **4300 zł brutto**

(wersja stacjonarna)- cena
obejmuje grupę do 50 osób*

- **3900 zł brutto**

(wersja on-line)- cena
obejmuje grupę do 100 osób

* w cenę wliczono 15 sztuk
materiałów (druk, długopis, notatnik), każda
kolejna sztuka **6,5 zł brutto**

Ochrona przed cyberatakami to jedno z najpoważniejszych wyzwań dla administracji publicznej. Niewątpliwie, skuteczne przygotowanie instytucji i pracowników na cyberzagrożenia, jest ogromnym wyzwaniem tak organizacyjnym jak i finansowym.

Zgodnie z projektem **Strategii Cyberbezpieczeństwa RP na lata 2017 - 2022**, pracownicy administracji publicznej powinni podnosić kwalifikacje poprzez szkolenia z zakresu cyberbezpieczeństwa. Szkolenia powinny dotyczyć przede wszystkim stosowania procedur ochrony informacji w instytucji, znajomości technik wyłudzenia informacji stosowanych w cyberprzestępczości, konsekwencji złamania zabezpieczeń przez cyberprzestępców oraz procedur obowiązujących w przypadku udanego ataku lub jego próby. Co istotne, szkolenia z zakresu cyberbezpieczeństwa powinny obejmować wszystkich pracowników administracji publicznej, a nie jedynie osoby odpowiedzialne za infrastrukturę teleinformatyczną w jednostce.

Według raportu **Najwyższej Izby Kontroli z 2015 roku na temat przygotowania państwa na cyberzagrożenia, brak szkoleń dla przedstawicieli administracji publicznej uznano za jedno z podstawowych zaniedbań.**

HARMONOGRAM

1. Rodzaje zagrożeń w cyberprzestrzeni, sposoby ochrony i profilaktyka - wstęp
2. Przedstawienie wybranych dokumentów i aktów prawnych:
 - jakie działania związane z cyberatakami kwalifikowane są jako przestępstwa
 - jakie kary grożą za popełnianie cyberprzestępstw
 - jakie prawa ma ofiara, która padła ofiarą cyberprzestępstwa
3. Techniki manipulacji, wyłudzenie informacji oraz przestępczość przeciwko godności osobistej
4. Rodzaje informacji i ustalenie stopnia istotności
5. Zarządzanie bezpieczeństwem informacji
6. Rodzaje zagrożeń dla Bezpieczeństwa Informacji
 - cyberataki (Malware, Phishing, ataki typu DDoS, pendrive i inne nośniki danych)
 - przestępczość ekonomiczna
7. Sposoby wykrywania złośliwego oprogramowania
8. Ataki socjotechniczne - odróżnianie fałszywej korespondencji, wykorzystywanie mediów społecznościowych, ataki typu APT
9. Zarządzanie hasłami dostępu
10. Analiza wybranych studiów przypadku, ocena zachowań, metod działania analiza wybranych rozwiązań wykorzystywanych w urzędzie
 - świadomość zagrożeń i konieczność przeciwdziałania im
 - tworzenie, wdrażanie, utrzymanie oraz rozwój polityki bezpieczeństwa
 - audyt systemów komputerowych w tym testy penetracyjne
11. Bezpieczeństwo urzędu a bezpieczeństwo narodowe



PeDaGo

Rynek Główny 28

31-010 Kraków

tel: 12 341 61 77

fax: 12 341 61 76

kom: 534 301 352

biuro@pedago.pl

www.pedago.pl