



Szkolenie CYBERBEZPIECZEŃSTWO JAKO STRATEGIA ORGANIZACJI

ZAKRES SZKOLENIA



Wprowadzenie do cyberbezpieczeństwa

- poddomeiny
- krajobraz cyberzagrożeń
- najczęstsze cyberzagrożenia
- definicje
- specyfika cyberzagrożeń w sieciach przemysłowych



Omówienie 3 filarów cyberbezpieczeństwa

- Ludzie (zasoby eksperckie, zakresy odpowiedzialności, budowanie zespołów, skuteczna komunikacja)
- Procesy (sposoby zarządzania)
- Technologie (środki zabezpieczające)



Kluczowe wymogi prawne

- Dyrektywa NIS2
- Dyrektywa CER
- Ustawa o Krajowym Systemie Cyberbezpieczeństwa (UKSC)
- SEC



Kluczowe standardy oraz dobre praktyki

- ISO 27001
- NIST
- IEC 62443
- Metodyki zarządzania ryzykiem
- Koncepcje wartę uwagi



Omówienie przykładowych cyberataków

- DoS
- MITM
- Brute Force
- Ransomware
- Spoofing
- Phishing



Rola zarządu w obszarze cyberbezpieczeństwa

- Procesy, ludzie, technologie
- Budżet cyberbezpieczeństwa
- GRC



Systemy Zarządzania Bezpieczeństwem Informacji

- SOC/SIEM/SOAR
- Budowa dokumentacji wewnętrznej
- Audyty
- Systemy Informatyczne



Case Study

- Harvard Business Review
- SolarWinds
- Pokaz laboratoryjny

O Szkoleniu

Celem szkolenia jest przedstawienie cyberbezpieczeństwa z perspektywy osób zarządzających organizacją oraz przygotowanie do wdrażania strategicznego podejścia w obszarze cyberbezpieczeństwa.



Materiały:

- ✓ standardy i przepisy
- ✓ raporty branżowe
- ✓ case study
- ✓ komentarze eksperckie



Forma:

- ✓ wykład
- ✓ zadania indywidualne
- ✓ ćwiczenia w grupach



Organizacja:

- ✓ 20 godzin
- ✓ 4 dni
- ✓ możliwość zajęć hybrydowych



**Politechnika
Krakowska**
Jubileusz 80-lecia



**Wydział Inżynierii
Elektrycznej i Komputerowej**
Jubileusz 50-lecia



SZKOLENIE ZAKOŃCZONE CERTYFIKATEM



Cena szkolenia: 1900 PLN (Netto)

TEMATY SZKOLENIA

I

Wprowadzenie do Cyberbezpieczeństwa w Organizacji

Ilość godzin: 6

Forma zajęć: Wykład

Tematyka: Podstawowe definicje i pojęcia; Podejście strategiczne w cyberbezpieczeństwie

II

Ochrona Sieci OT dla Zarządów Jednostek Samorządowych

Ilość godzin: 4 (3+1)

Forma zajęć: Wykład + Laboratorium Sprzętowe

Tematyka: Ochrona Sieci OT w kontekście Dyrektywy NIS2/UKSC; Studium Cyberataku

III

Prawne aspekty Cyberbezpieczeństwa

Ilość godzin: 6

Forma zajęć: Wykład

Tematyka: Obowiązujące regulacje; Cyberbezpieczeństwo w umowach; Odpowiedzialność prawna

IV

Zarządzenie Bezpieczeństwem Informacji

Ilość godzin: 2

Forma zajęć: Wykład

Tematyka: Struktura Dokumentacji Wewnętrznej; Zasady nadzoru, rozwoju i audytów wewnętrznych

V

Informatyczne Systemy Zarządzania Bezpieczeństwem

Ilość godzin: 2

Forma zajęć: Wykład

Tematyka: SOC/SIEM/SOAR - omówienie; Budowa zespołu SOC; Zabezpieczenia Informatyczne

Zapisy na szkolenie

Rekrutacja na szkolenie ma charakter ciągły.

Informacja o uruchomieniu szkolenia zostanie wysłana do zainteresowanych po uzyskaniu minimalnej liczby zgłoszeń - 8.



**FORMULARZ
ZGŁOSZENIOWY**

Kontakt

Kierownik Szkolenia

dr hab. inż. Piotr Małka, prof. PK
piotr.malka@pk.edu.pl

Rejestracja

lic. Grażyna Skuza
grazyna.skuza@pk.edu.pl

Obsługa finansowa

mgr inż. Anna Łukasik
anna.lukasik@pk.edu.pl

