

kod szkolenia: BS.IT CS / PL DL 2d

Security/Warsztaty z Cyberbezpieczeństwa (AI)

Zobacz film: https://youtu.be/QvD-S_XordQ

Dyrektywa NIS2

Unijne przepisy rozszerzają zakres przepisów dotyczących cyberbezpieczeństwa. Przedsiębiorcy objęci regulacją NIS2, wynikającą z ustawy o krajowym systemie bezpieczeństwa, będą objęci obowiązkiem stosowania produktów, usług bądź procesów, objętych tymi schematami certyfikacyjnymi.

Sprawdź, czy Twoja firma będzie objęta dyrektywą NIS2

Sprawdź swoją wiedzę z zakresu:

- [CompTIA CySA+](#)
- [CompTIA Security+](#)
- [CompTIA Network+](#)
- [OSINT - Biały Wywiad, czyli jak dotrzeć do cennych informacji](#)
- [CEH - Certified Ethical Hacker](#)
- [ECIH - Certified Incident Handler](#)
- [Testy penetracyjne](#)



Odbiorcy szkolenia

Szkolenie skierowane do kadry zarządzającej oraz pracowników administracyjnych, użytkowników komputerów i innych urządzeń z dostępem do Internetu, nie będących specjalistami z zakresu bezpieczeństwa IT.



Korzyści

Poszerzenie wiedzy pracowników na temat bezpiecznego korzystania z cyberprzestrzeni w miejscu pracy i poza nim.

Uczestnicy nauczą się:

- definiować i charakteryzować najważniejsze techniki cyberataków,
- rozpoznawać i zapobiegać zagrożeniom związanym z cyberprzestępczością,
- podejmować odpowiednie działania (zabezpieczenia) w przypadku usiłowania cyberataku,
- rozpoznawać socjotechniki wykorzystywane przez „ cyberprzestępców”,
- docelowo także popularyzować wiedzę nabytą na szkoleniu w organizacji.



Program szkolenia

1. Wstęp

- Co to jest cyberbezpieczeństwo – definicja cyberprzestrzeni i cyberbezpieczeństwa, dlaczego to jest ważne
- Ryzyko i zarządzanie ryzykiem – co to jest ryzyko, podstawowe pojęcia i zasady zarządzania ryzykiem
- Polityka bezpieczeństwa – czym jest w organizacji polityka bezpieczeństwa i jaka jest jej rola
- Incydenty bezpieczeństwa – co należy rozumieć jako incydent bezpieczeństwa i jak z nim postępować
- Normy i standardy bezpieczeństwa – powszechnie stosowane rozwiązania, norma ISO27001
- – AI Act – Normy dotyczące AI
- NIS2 i DORA oraz ECSF/NICE

2. Ataki „na człowieka” tzw. SOCJOTECHNIKA (stosowane techniki manipulacji)

- Ataki socjotechniczne – techniki manipulacji wykorzystywane przez cyberprzestępców
- Sposoby – pod jakimi pretekstami wyłudza się firmowe dokumenty
- Wykrywanie – jak rozpoznać, że jest się celem ataku socjotechnicznego
- Reakcja – jak prawidłowo reagować na ataki socjotechniczne
- Jak i skąd atakujący zbierają dane na twój temat
- Miejsca, w których zostawiamy swoje dane świadomie i nieświadomie – jak świadomie udostępniać informacji w sieci

3. Atak „na komputery” – demonstracje wraz z objaśnieniem metod ochrony

- Przegląd aktualnych ataków komputerowych wykorzystywanych przez cyberprzestępców, typowe błędy zabezpieczeń wykorzystywane przez atakujących
- Ataki przez sieci bezprzewodowe (WiFi, Bluetooth, NFC)
- Ataki przez pocztę e-mail (fałszywe e-maile)
- Ataki przez strony WWW – jak nie dać się zainfekować, fałszywe strony

- Ataki przez komunikatory (Skype, Facebook)
 - Ataki przez telefon (fałszywe SMS-y, przekierowania rozmów, itp.)
 - Ataki APT, phishing, smishing, spear-phishing, pharming, spoofing, spam, spim, scam
4. Dobre praktyki związane z bezpiecznym wykorzystaniem firmowych zasobów
- Polityka haseł, zarządzanie dostępem i tożsamością – jakie hasło jest bezpieczne, jak nim zarządzać, zasady udzielania dostępu do zasobów informacyjnych
 - Bezpieczeństwo fizyczne – urządzenia, nośniki danych, dokumenty, „czyste biurko”
 - Bezpieczna praca z urządzeniami mobilnymi (smartfon, tablet, laptop)
 - Problem aktualnego oprogramowania i kopii zapasowych
 - Bezpieczna praca z pakietem biurowym Microsoft Office
 - Bezpieczna praca z programem pocztowym
 - Bezpieczna praca z przeglądarką internetową
 - Zastosowanie technik kryptograficznych (szyfrowanie, certyfikaty)
5. Aspekty prawne
- Odpowiedzialność pracownika przed pracodawcą za ujawnienie informacji
 - Nieautoryzowane użycie systemów komputerowych
 - Rażące zaniedbania związane z wykorzystywaniem sprzętu komputerowego
 - Dane osobowe i dane wrażliwe
6. AI – Sztuczna inteligencja w służbie oszustów:
- Definicja i pokaz praktyczny chatbotów (np. ChatGPT)
 - Wykorzystanie chatbotów do pomocy w codziennej pracy – pokaz praktyczny
 - Zagrożenia związane z chatbotami
 - Phishing związany z AI
 - Wyciek danych / hackowanie ChatGPT
 - Fałszywe tożsamości
 - Wykorzystanie AI do generowania wizerunku
 - Wykorzystanie AI do fałszowania obrazu
 - Wykorzystanie AI do podrabiania głosu
 - Generowanie fałszywych danych
 - Podsumowanie w formie konkretnych rad metod obrony i detekcji



Oczekiwane przygotowanie uczestnika

Wymagana ogólna wiedza informatyczna z zakresu systemów operacyjnych i zagadnień sieciowych.

Jako uzupełnienie rekomendujemy:

Praktyczny trening zasad bezpieczeństwa informacji w firmie – Symulacja biznesowa „Ambasada”.



Szkolenie obejmuje

- 2 dni pracy z trenerem
- Nadzór trenera
- Kontakt ze społecznością
- Podręcznik w wersji elektronicznej
- Środowisko laboratoryjne

Metoda szkolenia

- wykład
- warsztaty



Czas trwania

2 dni / 14 godzin

Język

- Szkolenie: polski
- Materiały: polski