kod szkolenia: BS.IT 00 / PL DL 1d NIS2

Bezpieczny pracownik / (AI) Sztuczna inteligencja w służbie oszustów: wykłady Cyber Awareness dla pracowników biurowych

Szkolenie ma na celu zapoznanie uczestników z zagrożeniami wynikającymi z rozwoju sztucznej inteligencji, zwłaszcza w kontekście jej wykorzystywania przez oszustów. Uczestnicy będą mieli okazję poznać praktyczne przykłady zastosowania AI, w tym chatbotów, oraz zrozumieć, jak te technologie mogą zostać użyte do przeprowadzania różnego rodzaju oszustw. Szkolenie pomoże uczestnikom zidentyfikować ryzyka związane z AI w codziennej pracy i wypracować metody obrony przed atakami.

Stawiasz na dalszy rozwój w zakresie bezpieczeństwa - zapoznaj sie z poniższą tematyką:

Sprawdź swoją wiedzę z zakresu:

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

Odbiorcy szkolenia

Szkolenie ma na celu zapoznanie pracowników organizacji z gamą aktualnie stosowanych ataków, głównie o charakterze socjotechnicznym. Poza częścią teoretyczną i praktycznymi przykładami możliwych zagrożeń AI, uczestnicy warsztatów posiądą umiejętność zwiększania bezpieczeństwa swojego środowiska pracy poprzez stosowanie narzędzi takich jak skanery online, menedżer haseł czy bazy wycieków. Przeszkoleni pracownicy będą w stanie skutecznie rozpoznawać popularne typy zagrożeń (m.in. phishing, spear phishing, scam, clickjacking), reagować na nie oraz ustanawiać odpowiednio silne zabezpieczenia własnych kont i danych (hasła, szyfrowanie, uwierzytelnianie dwuskładnikowe). Na warsztatach omówione też zostaną zagadnienia związane z popularnymi typami zagrożeń, jak np. fałszywe sieci wifi, urządzenia szpiegujące, złośliwe oprogramowanie (w tym ransomeware i cryptolockery). Opowiemy też o bezpieczeństwie urządzeń mobilnych i dobrych praktykach dbania o własną prywatność.

Korzyści

- Podniesienie świadomości zagrożeń związanych z działaniami cyberprzestępców,
- Obniżenie poziomu ryzyka kradzieży lub wyłudzenia poufnych danych,
- Obniżenie poziomu ryzyka utraty ciągłości działania procesów biznesowych,
- Ochrona infrastruktury teleinformatycznej organizacji,

Program szkolenia

- Socjotechniki
  - Kto za tym stoi i kto na tym zarabia?
  - Do czego przestępcom nasze dane?
  - Dlaczego celem ataków najczęściej stają się szeregowi pracownicy organizacji?
  - Czym są socjotechniki i z czego wynika ich skuteczność oraz popularność?
  - Metody rozpoznawania ataków socjotechnicznych i sposoby na ich uniknięcie
  - Skutki działań cyberprzestępców dla osób prywatnych i organizacji
  - Ile kosztują nasze dane?
- Bezpieczeństwo Poczty e-mail
  - Zasady weryfikacji załączników
  - Zasady weryfikacji linków
  - Zasady weryfikacji nadawców
  - Czy nadawca musi być tym, za kogo się podaje?
  - Czy łatwo się podszyć pod pracownika firmy?

- Czy łatwo jest wyłudzić duże pieniądze przy pomocy jednego maila?
- Bezpieczeństwo przeglądarek internetowych
  - Czym jest phishing i jak go uniknąć?
  - Czym jest typosquating i domainsquating?
  - Czym są ataki typu clickjacking, camjacking, likejacking?
  - Zasady weryfikacji informacji oraz stron internetowych i URL-i
- Bezpieczeństwo urządzeń i nośników danych
  - Nośniki danych nieznanego pochodzenia jako zagrożenie
  - Popularne socjotechniki typu "na kuriera","na pizzę"
  - Czy lampka USB jest nośnikiem danych?
  - Nowe urządzenia od działu IT
  - Bezpieczne usuwanie danych
- Ataki za pośrednictwem telefonu
  - Wyłudzanie informacji
  - Nakłanianie do określonych działań za pomocą telefonu
  - Czy rozmówca jest tym za kogo się podaje?
- Zagrożenia związane w urządzeniami mobilnymi
  - Bezpieczeństwo aplikacji mobilnych
  - Przydzielanie uprawnień aplikacjom
  - Smartfon – najlepsze narzędzie inwigilacji
- Zagrożenia związane z sieciami WIFI
  - Sieć darmowa
  - Jak się ma nazwa sieci do jej bezpieczeństwa?
  - Czy łatwo stworzyć fałszywą sieć wykradającą dane?
- Bezpieczeństwo haseł
  - Czy nasze hasła są publicznie udostępniane w Internecie?
  - Które z naszych kont zostały już przejęte przez hackerów?
  - Ile trwa złamanie hasła?
  - Co to jest hasło słownikowe?
  - Jak stworzyć silne, bezpieczne i łatwe do zapamiętania hasło?
- 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

- Podstawowa znajomość obsługi komputera

Szkolenie obejmuje

Metoda szkolenia

- wykład

Czas trwania

1 dni / 7 godzin

Język

- Szkolenie: polski
- Materiały: polski