Bezpieczny pracownik – wykłady Cyber Awareness dla pracowników biurowych

PRZEZNACZENIE 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, 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 WYNIKAJĄCE Z UKOŃCZENIA SZKOLENIA

- 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

OCZEKIWANE PRZYGOTOWANIE SŁUCHACZY

Podstawowa znajomość obsługi komputera

PRZYGOTOWANIE DO SZKOLENIA

Wirtualna Klasa

- Poznanie trenera i grupy
- Sprawdzanie wiedzy - testy i quizy
- Wprowadzenie w temat zajęć

WYKŁADY I WARSZTATY

Sala szkoleniowa

1. 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

2. 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?
3. 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
4. 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
5. Ataki za pośrednictwem telefonu
    - Wyłudzanie informacji
    - Nakłanianie do określonych działań za pomocą telefonu
    - Czy rozmówca jest tym za kogo się podaje?
6. Zagrożenia związane w urządzeniami mobilnymi
    - Bezpieczeństwo aplikacji mobilnych
    - Przydzielanie uprawnień aplikacjom
    - Smartfon - najlepsze narzędzie inwigilacji
7. Zagrożenia związane z sieciami WIFI
    - Sieć darmowa
    - Jak się ma nazwa sieci do jej bezpieczeństwa
    - Czy łatwo stworzyć fałszywą sieć wykradającą dane
8. 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?
9. Sztuczna inteligencja w służbie oszustów
    - Fałszywe tożsamości
    - Wykorzystanie AI do generowania wizerunku
    - Wykorzystanie AI do fałszowania obrazu
    - Wykorzystanie AI do podrabiania głosu

WSPARCIE I ROZWÓJ PO SZKOLENIU

Portal Altkom Akademii

- Dostęp do materiałów szkoleniowych i uzupełniających
- Opieka trenera
- Kontakt ze społecznością

Kod szkolenia	BS.IT 00 / PL AA 1d
Czas trwania	1 dni
Poziom	Podstawowy
Autoryzacja	Altkom