kod szkolenia: BS.IT VR / PL AA 1d

Company (un)hacked - Szkolenie z cyberbezpieczeństwa w oparciu o technologię VR

Czy zastanawiałeś się, jak skutecznie zwiększyć poziom zabezpieczeń swojej firmy, jednocześnie angażując swoich pracowników w nowoczesny sposób? Teraz masz szansę zobaczyć to na własne oczy! Zapraszamy na wyjątkowe wydarzenie, które otworzy przed Tobą drzwi do świata innowacyjnych szkoleń z cyberbezpieczeństwa w technologii VR.

Oferujemy szkolenie w nowej odsłonie.

Przełam bariery tradycyjnych metod szkoleniowych i zwiększ skuteczność nauczania o cyberbezpieczeństwie dzięki aplikacji VR. Odkryj naukę poprzez praktykę. Zanurzenie w realnych zadaniach i praktyczna aplikacja umiejętności wykazują znacznie większą skuteczność w nauczaniu niż metody takie jak czytanie, słuchanie czy obserwacja.

Szkolenie realizowane wyłącznie w formule stacjonarnej.

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 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

- Umiejętność sprecyzowania i charakteryzacji podstawowych zasad zachowania bezpieczeństwa informacji, zagrożenia i ryzyko ich naruszenia z zewnątrz.
- Umiejętność identyfikacji rodzajów zabezpieczeń stosowanych na używanym przez siebie sprzęcie i oprogramowaniu oraz zgłaszanie potencjalnych luk w zabezpieczeniach.
- Umiejętność stosowania wytycznych dotyczących sposobu pracy w sieci i w trybie zdalnym z zachowaniem zasad bezpieczeństwa informacji i cyberbezpieczeństwa.
- Umiejętność reakcji na podejrzane incydenty, zgłaszając ich wystąpienie przełożonemu i eliminuje zagrożenia zgodnie z otrzymanymi poleceniami.
- Nauka przez praktykę.

Program szkolenia

1. Wstęp.
   - Co to jest cyberbezpieczeństwo – definicja cyberprzestrzeni i cyberbezpieczeństwa, dlaczego to jest ważne, aktualne trendy na świecie.
   - 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.
   - Studia przypadków oraz wpływ cyberataków na organizację.
   - Współczesne strategie bezpieczeństwa.
2. Typy ataków hackerskich – demonstracje wraz z objaśnieniem metod ochrony.
   - Przegląd aktualnych ataków komputerowych wykorzystywanych przez cyberprzestępców, typowe błędy zabezpieczeń wykorzystywane przez atakujących.
   - Ścieżka ataku (kill-chain) zasady- rozpoznanie i zasady postępowania.
   - 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.
3. Dobre praktyki, formy obrony przed atakami.
4. Rozwój Kompetencji z zakresu bezpieczeństwa.
5. Dlaczego bezpieczeństwo to nie tylko Departament Bezpieczeństwa.

Oczekiwane przygotowanie uczestnika

Ogólna znajomosć obsługi komputera

Szkolenie obejmuje

- Dzień pracy z trenerem
- Nadzór trenera
- Kontakt ze społecznością
- Podręcznik w wersji elektronicznej

Czas trwania

1 dni / 7 godzin

Język

- Szkolenie: polski
- Materiały: polski