SECURITUM

SZKOLENIE

Cyber Awareness

Grupa docelowa

Pracownicy biurowi | Kadra zarządzająca

Poziom zaawansowania

★ ★ ★

TRENER

Artur Czyż

- Rocznie realizuje przeszło 100 projektów związanych z bezpieczeństwem IT (audyty, pentesty, szkolenia)
- Aktywnie uczestniczy w programach typu bug bounty, przykłady zgłoszonych błędów: IBM InfoSphere (CVE-2016-0250 / CVE-2016-0280) oraz Swagger UI (CVE-2016-7559 i CVE-2016-7918)
- Prelegent na konferencji: Advanced Threat Summit (2014)
- Autor tekstów w serwisie sekurak.pl oraz w magazynie „Programista”
- Posiada certyfikat Offensive Security Certified Professional
- Konsultant d/s bezpieczeństwa IT w firmie Securitum

PUBLIKACJE

- *Odczytywanie danych zapisanych na zbliżeniowych kartach płatniczych*
- *Automatyczna analiza złośliwego oprogramowania z wykorzystaniem SysAnalyzer*
- *Nietypowe metody wykorzystywane w atakach phishingowych*

ZAPISZ SIĘ

ZAMÓWIENIE SZKOLENIA

DODATKOWE INFORMACJE

< SZKOLENIA@SECURITUM.PL >

O SZKOLENIU

- szkolenie prowadzone przez doświadczonego eksperta do spraw bezpieczeństwa IT
- od 2 do 4 godzin konkretnej wiedzy znacząco podnoszącej świadomość uczestników w dziedzinie bezpieczeństwa teleinformatycznego
- możliwość dostosowania agendy do potrzeb Klienta
- prezentacja realnych technik wykorzystywanych przez przestępców przedstawiona w sposób zrozumiały dla osób nietechnicznych
- trafne przykłady z życia zwiększające umiejętność rozpoznawania i reagowania na rzeczywiste zagrożenia
- poznawanie sekretów hackerów

DODATKOWE INFORMACJE

ZAMÓWIENIE SZKOLENIA

UCZESTNICY O SZKOLENIU

- *Praktyczne przykłady z życia.*
- *Fachowość wykładowcy, ciekawe tematy, praktyczne porady.*
- *Przedstawienie konkretnych przykładów ataków.*
- *Jasność i klarowność przekazywanych informacji.*
- *Trener otwarty na współpracę z uczestnikami szkolenia w przyszłości (pomoc i porady).*
- *Zaangażowany, duża wiedza merytoryczna.*

RAMOWY PROGRAM SZKOLENIA

Podstawy bezpieczeństwa

- zasada „czystego biurka”, „czystego ekranu” i inne

Pakiet biurowy i (nie)bezpieczne dokumenty

- bezpieczna konfiguracja pakietu, złośliwe makra, kradzież danych logowania i inne potencjalne ataki

Socjotechnika

- strategie atakującego wraz z planem działania
  - podszywanie się pod pracownika biurowego (różne warianty), służby ochrony, współpracownika lub firmę współpracującą, interesanta i wiele innych
- profilowanie, zbieranie informacji o ofierze i planowanie najlepszego momentu do ataku

Polityka haseł i kodów dostępu

- zasady tworzenia i ich bezpieczna wymiana
- bezpieczne przechowywanie haseł
- odzyskiwanie hasła i dostępu do systemu operacyjnego

Bezpieczne korzystanie z Internetu

- przeglądarka internetowa (m.in. zasady bezpiecznego korzystania, ważne opcje i rozszerzenia)
- bezprzewodowy dostęp (m.in. zasady bezpiecznego korzystania)
- programy pocztowe

Phishing

Bezpieczna bankowość

- karty zbliżeniowe (odczytywanie zapisanych danych)
- bankowość internetowa (zasady bezpiecznego korzystania)
- bankomat (zasady bezpiecznego korzystania oraz przegląd popularnych metod działania przestępców)

Bezpieczeństwo plików

- zasady bezpieczeństwa, BadUSB

Złośliwe oprogramowanie

- weryfikacja i instalacja oprogramowania
- złośliwy dokument PDF – widok z perspektywy atakującego
- ukrywanie prawdziwego rozszerzenia pliku

Bezpieczeństwo usług mobilnych i stacjonarnych

- instalacja aplikacji na smartfonach
- podsłuchiwanie rozmów
- podszywanie się pod nadawcę wiadomości SMS i rozmówcę telefonicznego
- bramki odbioru SMS i SMS Premium

Bezpieczeństwo w domu

- konfiguracja routera i zabezpieczanie domowej sieci

Bezpieczeństwo w firmie

- zdalny dostęp oraz zgłaszanie incydentów

Pytania i odpowiedzi

SZKOLENIE POLECAJĄ

ROSWALTO

sekurak.pl

programista