Bezpieczeństwo teleinformatyczne dla specjalistów IT (kod: CYBERSECURITY-IT)

Opis i cel szkolenia

Nasz warsztat "bezpieczeństwo teleinformatyczne" został zaprojektowany jako kompleksowe wprowadzenie w tematykę cybersecurity - z myślą o pracownikach działów IT, którzy codziennie stają przed wyzwaniami związanymi z zapewnieniem bezpieczeństwa informacji w swoich organizacjach. Celem warsztatów jest podniesienie świadomości i umiejętności uczestników w zakresie identyfikacji i zarządzania zagrożeniami cyfrowymi, które mogą wpłynąć na bezpieczeństwo organizacji.

Podczas szkolenia uczestnicy będą mieli okazję zgłębić tematykę implementacji środków bezpieczeństwa, a także zrozumieć kluczowe problemy, które mogą pojawić się podczas wprowadzania tych środków w życie. Poruszone zostaną zagadnienia związane z najnowszymi trendami w cyberbezpieczeństwie oraz metodami obrony przed (coraz bardziej wyrafinowanymi) atakami hakerskimi.

Szkolenie będzie zawierało również sesje dotyczące tzw. najlepszych praktyk bezpieczeństwa. Uczestnicy nauczą się, jak efektywnie stosować te praktyki w celu optymalizacji infrastruktury firmowej. Będzie to obejmowało analizę przypadków użycia, dyskusje grupowe oraz praktyczne ćwiczenia, dzięki którym uczestnicy będą mogli zastosować zdobytą wiedzę w realnych scenariuszach firmowych.

Ponadto, warsztaty będą okazją do wymiany doświadczeń z innymi profesjonalistami z branży IT, co umożliwi uczestnikom poszerzenie swoich horyzontów i zdobycie nowych perspektyw na temat zarządzania bezpieczeństwem informacji. Zostaną omówione również wyzwania związane z zapewnieniem zgodności z przepisami prawnymi i regulacjami dotyczącymi ochrony danych.

Podsumowując, kompleksowe szkolenie, które ma na celu wyposażenie pracowników IT w niezbędne narzędzia i wiedzę, aby efektywnie chronić swoje organizacje przed zagrożeniami cyfrowymi, jednocześnie optymalizując ich infrastrukturę technologiczną.

Czas trwania

3 dni

Program

1. **Studium przypadków ataków na dane**
   — Wyjaśnienie podstawowych pojęć w branży IT. Każde pojęcie będzie dodatkowo omawiane indywidualnie, gdy pojawi się w dalszej części szkolenia. Zapoznanie uczestników z przykładami największych wycieków danych w historii i ich konsekwencje finansowe dla firmy.
2. **Zdobywanie informacji**
   — OSINT (tzw. biały wywiad, rozpoznanie z ogólnodostępnych źródeł): portale społecznościowe, wycieki danych, analiza danych celem przygotowania ataku socjotechnicznego.
3. **Anatomia ataku**
   — W tej części szkolenia zostanie wykonany pokaz praktycznego ataku – od pozyskania informacji, wykorzystania socjotechniki, poprzez przejęcie kontroli nad komputerem, telefonem i kontem bankowym. Realne pokazanie powiązań wpływu lekceważenia zasad bezpieczeństwa i działania w stresie – do utraty tożsamości cyfrowej.

Zapytaj o szczegóły
tel. 22 63 64 164
akademia@alx.pl

Najbliższe terminy
2025-03-19 (Zdalnie)
2025-03-19 (Warszawa)
2025-05-21 (Zdalnie)
2025-05-21 (Warszawa)

4. **Phishing i spoofing, czyli dlaczego jesteśmy podatni**
   — Studium przypadków realizacji ataków socjotechnicznych – przykłady z polskich urzędów i instytucji państwowych. Metody diagnozy ataku i jego neutralizacji.
5. **Zabezpieczenie urządzeń końcowych i użytkownika**
   — Dobre praktyki dla użytkowników końcowych: jak powinni zabezpieczyć sieć WiFi, telefon, komputer, konta internetowe, urządzenia służbowe. Bezpieczne korzystanie z Internetu. W ramach szkolenia zostanie pokazany sposób wykorzystania sieci do bezpiecznego przechowywania danych oraz wysyłania szyfrowanych wiadomości przez komunikatory oraz sieci VPN.
6. **Dokumentacja bezpieczeństwa firmy**
   — Analiza ryzyka. Polityka bezpieczeństwa firmy PBE. Polityka bezpiecznej eksploatacji systemu SWB. Szczególne wymagania bezpieczeństwa systemu IT.
7. **Wymogi prawne SZBI**
   — Omówienie aktualnych wymogów prawnych europejskich i krajowych, standardy zarządzania bezpieczeństwem informacji.
8. **Audyt systemów IT**
   — Proces audytowania systemów IT.
9. **Projektowanie mechanizmów kontrolnych bezpieczeństwa systemu**
   — Mechanizmy kontrolne bezpieczeństwa systemu: wskazówki, jak projektować bezpieczny system wg międzynarodowego instytutu ISECOM.
10. **Incydenty komputerowe**
    — Sposoby reagowania na incydenty komputerowe: jak sprawnie reagować na incydenty i włamania.

Zapytaj o szczegóły
tel. 22 63 64 164
akademia@alx.pl

Najbliższe terminy
2025-03-19 (Zdalnie)
2025-03-19 (Warszawa)
2025-05-21 (Zdalnie)
2025-05-21 (Warszawa)

Przeznaczenie i wymagania

Brak szczegółowych wymagań wobec uczestników szkolenia.

Certyfikaty

Uczestnicy szkolenia otrzymują imienne certyfikaty sygnowane przez ALX.

Lokalizacje

— Warszawa – ul. Jasna 14/16A
— Zdalnie – zajęcia realizowane poprzez platformę Zoom
— Kraków – ul. św. Filipa 23
— Katowice – ul. Stawowa 10
— Wrocław – ul. Rynek 35
— Gdańsk – ul. Toruńska 12
— Warsaw (English) – Jasna 14/16A
— Online (English) – your home, office or wherever you want
— na życzenie dowolne miejsce w Polsce, lub UE (zajęcia prowadzone w języku angielskim)

Cena szkolenia

2490 PLN netto (VAT 23%)

W cenę szkoleń organizowanych w naszej siedzibie wliczone są:

— autorskie materiały szkoleniowe,
— indywidualne stanowisko komputerowe do pracy podczas zajęć,
— certyfikaty ukończenia szkolenia,

— drobny poczęstunek oraz ciepłe i zimne napoje,
— możliwość jednorazowego kontaktu z instruktorem (instruktorami) po szkoleniu i zadawania pytań dotyczących materiału szkolenia.

Cena szkolenia nie zawiera obiadów. Można je dokupić w cenie 35 zł netto za obiad.

Zapytaj o szczegóły
tel. 22 63 64 164
akademia@alx.pl

Najbliższe terminy
2025-03-19 (Zdalnie)
2025-03-19 (Warszawa)
2025-05-21 (Zdalnie)
2025-05-21 (Warszawa)