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

Opis i cel szkolenia

Szkolenie „Bezpieczeństwo teleinformatyczne dla specjalistów IT" to 3-dniowy, praktyczny warsztat dla administratorów, inżynierów sieci, specjalistów wsparcia oraz dla wszystkich specjalistów IT i osób odpowiedzialnych za infrastrukturę IT. Celem jest kompleksowe wprowadzenie w tematykę cybersecurity, uporządkowanie wiedzy o zagrożeniach i ich identyfikacji - oraz pokazanie, jak realnie wzmacniać bezpieczeństwo środowiska w organizacji, od konfiguracji usług, po codzienną administrację i zarządzanie.

Podczas zajęć uczestnicy analizują typowe scenariusze ataków na systemy i sieci (włamania, wycieki danych, ransomware, nadużycia uprawnień... jak również socjotechnika...), sposoby działania atakujących oraz błędy konfiguracyjne, które te ataki umożliwiają. Na tej podstawie omawiane są konkretne środki ochrony (implementacja środków bezpieczeństwa), na przykład: segmentacja sieci, zabezpieczenia usług, mechanizmy uwierzytelniania i autoryzacji, rejestrowanie i analiza logów, kopie zapasowe. Jak również podstawy reagowania na incydenty. Odnosimy się też do aktualnych trendów i nowych klas ataków hackerskich oraz metod obrony przed nimi.

Szkolenie ma charakter warsztatowy: studia realnych przypadków, przykładowe konfiguracje, najlepsze praktyki bezpieczeństwa, krótkie ćwiczenia i checklisty, które można od razu przenieść do własnej organizacji. Uczestnicy konfrontują swoje obecne rozwiązania z dobrymi praktykami, mają możliwość skonsultowania się z trenerem-praktykiem, jak również wymiany doświadczeń z innymi specjalistami z branży IT - i upewniają się, czy ich środowisko spełnia podstawowe wymagania bezpieczeństwa. Poruszamy również kwestie zapewniania zgodności z przepisami prawnymi, w tym w obszarze regulacji dotyczących ochrony danych.

Czas trwania

3 dni, 9:00 - 17:00

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.
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

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

Najbliższe terminy
2026-12-16 (Zdalnie)
2026-12-16 (Warszawa)

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
2026-12-16 (Zdalnie)
2026-12-16 (Warszawa)

Przeznaczenie i wymagania

Szkolenie stworzone zostało z myślą o specjalistach IT, w szczególności - dla administratorów systemów i sieci, inżynierów wsparcia, ale też dla programistów, jak również i dla ról odpowiedzialnych za infrastrukturę i bezpieczeństwo systemów w firmie lub instytucji.

Oczekujemy podstawowej znajomości administracji systemami lub sieciami (Windows lub Linux, usługi sieciowe, konta użytkowników). Przydatne będzie jakiekolwiek doświadczenie w pracy w IT.

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
— 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

2390 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
2026-12-16 (Zdalnie)
2026-12-16 (Warszawa)