

Cyberbezpieczeństwo dla członków Zarządu i kadry kierowniczej (kod: CYBERSEC-MGMT)

Opis i cel szkolenia

Cyberbezpieczeństwo stało się jednym z kluczowych obszarów zarządzania organizacją – obok operacji, finansów, czy compliance. Zarządy i kadra kierownicza potrzebują jasnego obrazu, jakie istnieją różne typy incydentów (ransomware, wycieki danych, oszustwa finansowe, nadużycia z wykorzystaniem AI...), scenariusze ataków - i jak wpływają one na ciągłość działania, odpowiedzialność prawną, czy reputację firmy. Dopiero na tej podstawie można świadomie podejmować decyzje dotyczące ryzyka, budżetów i priorytetów w obszarze bezpieczeństwa.

Nasze jednodniowe szkolenie pokazuje cyberbezpieczeństwo z perspektywy zarządczej: skupiamy się na socjotechnikach, atakach przez pocztę elektroniczną, przeglądarki, urządzenia mobilne, hasła i sieci WiFi, a także na nowych możliwościach oszustów wynikających z wykorzystania sztucznej inteligencji (deepfake głosu i wizerunku, zaawansowany phishing...). Uczestnicy poznają najczęstsze scenariusze ataków na organizacje, ich konsekwencje dla biznesu oraz proste, ale skuteczne zasady, które można egzekwować od pracowników i menedżerów - bez wchodzenia w szczegóły techniczne.

Szkolenie prowadzone jest przez renomowanego wykładowcę i praktyka bezpieczeństwa IT, który na co dzień pracuje w branży security oraz regularnie szkoli i występuje jako prelegent na konferencjach. Zajęcia mają formę wykładowo-warsztatową, z przykładami z realnych incydentów i przestrzenią na pytania uczestników, tak aby słuchacze mogli przełożyć wiedzę na konkretne decyzje, procedury i wymagania wobec swoich zespołów. Realizujemy je zarówno w formule otwartej – w terminach publikowanych na stronie i dostępnych dla pojedynczych uczestników – jak i na zamówienie dla grup z firm oraz instytucji.

Czas trwania

1 dzień

Program

- Ogólny kontekst zagrożeń. 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 organizacji i dla osób prywatnych
 - Ile kosztują nasze dane?
 - Dyrektywa NIS2
 - Wymagania regulu 24/7/30, czyli co robi firma po ataku wg ustawy
 - Obowiązki pracowników i pracodawcy wynikające z NIS2
 - System S46
 - Stopnie alarmowe CRP
- Bezpieczeństwo poczty e-mail
 - Zasady weryfikacji załączników

Zapytaj o szczegóły

tel. 22 63 64 164

akademia@alx.pl

Najbliższe terminy

2026-05-27 (Zdalnie)

2026-05-27 (Warszawa)

2026-06-24 (Zdalnie)

2026-06-24 (Warszawa)

- 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?
- 4. Przeglądarki internetowe i strony WWW
 - Bezpieczeństwo przeglądarek internetowych
 - Czym jest phishing i jak go uniknąć?
 - Czym jest typosquatting i domainsquatting?
 - Czym są ataki typu clickjacking, camjacking, likejacking?
 - Zasady weryfikacji informacji oraz stron internetowych i URL-i
- 5. Urządzenia i nośniki danych
 - 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
- 6. Ataki za pośrednictwem telefonu
 - Wyłudzenie informacji
 - Nakłanianie do określonych działań za pomocą telefonu
 - Czy rozmówca jest tym za kogo się podaje?
- 7. Urządzenia mobilne i aplikacje
 - Zagrożenia związane w urządzeniami mobilnymi
 - Bezpieczeństwo aplikacji mobilnych
 - Przydzielanie uprawnień aplikacjom
 - Smartfon – najlepsze narzędzie inwigilacji
- 8. Sieci bezprzewodowe, WiFi
 - Zagrożenia związane z sieciami WiFi
 - Sieć darmowa
 - Jak się ma nazwa sieci do jej bezpieczeństwa?
 - Czy łatwo stworzyć fałszywą sieć wykradającą dane?
- 9. Hasła i dostęp do kont
 - 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?
- 10. AI – Sztuczna inteligencja w służbie oszustów
 - Definicja i pokaz praktyczny chatbotów (np. ChatGPT)
 - Wykorzystanie chatbotów do pomocy w codziennej pracy – pokaz praktyczny
 - Zagrożenia związane z chatbotami
 - Phishing związany z AI
 - Wyciek danych / hackowanie ChatGPT
 - Fałszywe tożsamości
 - Wykorzystanie AI do generowania wizerunku
 - Wykorzystanie AI do fałszowania obrazu
 - Wykorzystanie AI do podrabiania głosu
 - Generowanie fałszywych danych

Zapytaj o szczegóły

tel. 22 63 64 164

akademia@alx.pl

Najbliższe terminy

2026-05-27 (Zdalnie)

2026-05-27 (Warszawa)

2026-06-24 (Zdalnie)

2026-06-24 (Warszawa)

Przeznaczenie i wymagania

Szkolenie stworzone zostało przede wszystkim pod kątem członków zarządu, właścicieli firm, dyrektorów i menedżerów - oraz osób nadzorujących obszary IT, ryzyka, czy też bezpieczeństwa informacji.

Ponieważ zajęcia kierowane są do kadry kierowniczej, nie oczekujemy żadnej szczególnej wiedzy technicznej, ani z zakresu cyberbezpieczeństwa. Ze względu na tematykę i kontekst szkolenia, przydatne będzie doświadczenie w zarządzaniu firmą lub zespołami oraz typowa znajomość codziennej obsługi komputera, internetu.

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

999 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

2026-05-27 (Zdalnie)

2026-05-27 (Warszawa)

2026-06-24 (Zdalnie)

2026-06-24 (Warszawa)