Możliwość dofinansowania

Cyberbezpieczeństwo oraz ochrona informacji w działalności handlowej

Numer usługi 2026/03/27/42004/3442570

3 321,00 PLN brutto
2 700,00 PLN netto
369,00 PLN brutto/h
300,00 PLN netto/h
261,33 PLN cena rynkowa

Pro-Invest AG
Michał Żmija

4,6 / 5
263 oceny

Warszawa
Usługa szkoleniowa
stacjonarna
09:00 h
10.06.2026 do 11.06.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie skierowane jest do pracowników firm handlowych, w szczególności osób odpowiedzialnych za sprzedaż, obsługę klientów i kontrahentów, przygotowanie ofert oraz udział w postępowaniach przetargowych. Odbiorcami są również osoby mające dostęp do danych biznesowych i komunikacji elektronicznej w organizacji, a także kadra zarządzająca nadzorująca procesy handlowe i bezpieczeństwo informacji.
Minimalna liczba uczestników	6
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	01-06-2026
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	9
Podstawa uzyskania wpisu do BUR	Certyfikat systemu zarządzania jakością wg. ISO 9001:2015 (PN-EN ISO 9001:2015) - w zakresie usług szkoleniowych

Cel

Cel edukacyjny

Usługa przygotowuje uczestników do identyfikowania zagrożeń cybernetycznych i ataków socjotechnicznych w działalności handlowej, stosowania zasad bezpiecznej pracy z pocztą elektroniczną, danymi i urządzeniami,

rozpoznawania zagrożeń w komunikacji z kontrahentami oraz podejmowania właściwych działań w przypadku incydentu cyberbezpieczeństwa zgodnie z przyjętymi procedurami organizacyjnymi.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik identyfikuje zagrożenia cybernetyczne oraz ataki socjotechniczne w działalności handlowej.	rozróżnia rodzaje ataków (phishing, vishing, podszywanie się)	Test teoretyczny z wynikiem generowanym automatycznie
	wskazuje charakterystyczne cechy podejrzanych wiadomości i działań	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik wskazuje właściwe działania w przypadku incydentu cyberbezpieczeństwa.	Rozróżnia etapy reagowania na incydent cyberbezpieczeństwa oraz zasady zgłaszania zagrożenia w organizacji.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik stosuje zasady bezpiecznej pracy z pocztą elektroniczną, danymi i urządzeniami.	wskazuje zasady tworzenia i zarządzania hasłami,	Test teoretyczny z wynikiem generowanym automatycznie
	rozpoznaje bezpieczne i niebezpieczne załączniki oraz linki,	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik identyfikuje zagrożenia w komunikacji z kontrahentami oraz w obiegu dokumentów.	Identyfikuje zagrożenia związane z komunikacją z kontrahentami, fałszywymi fakturami oraz zmianą danych do płatności.	Test teoretyczny z wynikiem generowanym automatycznie

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

TAK

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Ramowy program szkolenia :

Program szkolenia:

Dzień 1:

Zagrożenia cybernetyczne i socjotechnika w biznesie

1. Współczesne zagrożenia cybernetyczne dla firm

• najczęstsze typy ataków na firmy handlowe

• dlaczego działy sprzedaży i obsługi przetargów są atrakcyjnym celem dla cyberprzestępców

• przykłady rzeczywistych incydentów w organizacjach

2. Ataki socjotechniczne

• phishing i spear-phishing

• vishing i próby wyłudzeń telefonicznych

• podszywanie się pod kontrahentów i pracowników firmy

• analiza przykładów rzeczywistych wiadomości e-mail

3. Cyberoszustwa w relacjach z kontrahentami

• oszustwa związane ze zmianą numerów rachunków bankowych

• fałszywe faktury

• przejęcie skrzynek e-mail i podszywanie się pod pracowników

• przykłady rzeczywistych incydentów biznesowych

4. Bezpieczeństwo dokumentów i danych biznesowych

• bezpieczeństwo dokumentów przetargowych

• ochrona ofert handlowych

• zagrożenia związane z przesyłaniem plików i korzystaniem z chmury

Dzień 2:

Praktyczne zasady bezpieczeństwa w pracy

5. Bezpieczeństwo poczty elektronicznej i pracy w sieci

• identyfikacja niebezpiecznych załączników i linków

• bezpieczna praca z dokumentami elektronicznymi

• higiena cyfrowa pracownika

6. Ochrona informacji w organizacji

• silne hasła i zarządzanie hasłami

• uwierzytelnianie wieloskładnikowe (MFA)

• bezpieczeństwo urządzeń służbowych

• podstawowe zasady OPSEC w działalności biznesowej

7. Reagowanie na incydenty cyberbezpieczeństwa

• jak rozpoznać incydent

• procedura reagowania w firmie

• ograniczanie skutków ataku

• współpraca z działem IT lub zewnętrznymi specjalistami

8. Warsztat – analiza scenariuszy

• analiza przykładowych ataków phishingowych

• symulacja sytuacji: fałszywy kontrahent

• dyskusja nad procedurami bezpieczeństwa w organizacji

Forma szkolenia:

Szkolenie prowadzone jest w formie warsztatowej i obejmuje:

• analizę rzeczywistych przykładów ataków cybernetycznych

• omówienie scenariuszy zagrożeń w działalności firm handlowych

• dyskusję nad praktycznymi zasadami bezpieczeństwa w organizacji

Szkolenia prowadzone są przez praktyków bezpieczeństwa posiadających doświadczenie w obszarze ochrony informacji, zarządzania ryzykiem oraz reagowania na incydenty bezpieczeństwa.

Na początku szkolenia przeprowadzany jest pre-test, natomiast na zakończeniu szkolenia realizowany jest post-test w celu weryfikacji osiągnięcia efektów uczenia się.

Warsztat obejmuje 9 h dydaktycznych .

Godzina dydaktyczna trwa 45 minut.

Harmonogram

Liczba pozycji harmonogramu: 2

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 2 dzien 1	-	10-06-2026	12:20	15:40	03:20
2 z 2 dzien 2	-	11-06-2026	08:00	12:00	04:00

Cennik

Jeżeli korzystasz z dofinansowania w wysokości co najmniej 70% przysługuje Tobie zwolnienie z podatku VAT

Cennik

Rodzaj ceny	Cena

Koszt przypadający na 1 uczestnika brutto	3 321,00 PLN
Koszt przypadający na 1 uczestnika netto	2 700,00 PLN
Koszt osobogodziny brutto	369,00 PLN
Koszt osobogodziny netto	300,00 PLN

Prowadzący

Liczba prowadzących: 0

Brak wyników.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy szkolenia otrzymają materiały dydaktyczne w formie elektronicznej, obejmujące opis omawianych zagadnień oraz zestawzadań ćwiczeniowych. Szkolenie prowadzone jest w formie warsztatów z wykorzystaniem komputera. Każdy uczestnik ma możliwość zadawania pytań i konsultacji indywidualnych z trenerem.

Uczestnicy otrzymają certyfikat i zaświadczenie.

Adres

Warszawa 9
Warszawa
woj. mazowieckie

Kontakt

ANNA WIŚNIEWSKA

E-mail a.wisniewska@proinvestag.pl
Telefon (+48) 606 757 757