



## Cyberbezpieczeństwo – zagrożenia w sieci

Numer usługi 2024/06/10/8117/2178229

1 045,50 PLN brutto

850,00 PLN netto

130,69 PLN brutto/h

106,25 PLN netto/h

ZETO Lublin

SPÓŁKA Z

OGRANICZONĄ

ODPOWIEDZIALNOŚĆ

CIA



Lublin / stacjonarna

Usługa szkoleniowa

8 h

29.01.2025 do 29.01.2025

## Informacje podstawowe

<b>Kategoria</b>	Informatyka i telekomunikacja / Bezpieczeństwo IT
<b>Sposób dofinansowania</b>	wsparcie dla pracodawców i ich pracowników wsparcie dla osób indywidualnych
<b>Grupa docelowa usługi</b>	<ul style="list-style-type: none"><li>pracownicy i/lub właściciele pracujących z komputerem, Internetem oraz urządzeniami mobilnymi</li><li>pracownicy z sektora MSP</li></ul>
<b>Minimalna liczba uczestników</b>	4
<b>Maksymalna liczba uczestników</b>	15
<b>Forma prowadzenia usługi</b>	stacjonarna
<b>Liczba godzin usługi</b>	8
<b>Podstawa uzyskania wpisu do BUR</b>	Certyfikat systemu zarządzania jakością wg. ISO 9001:2015 (PN-EN ISO 9001:2015) - w zakresie usług szkoleniowych

## Cel

### Cel edukacyjny

Celem szkolenia jest dostarczenie specjalistycznej wiedzy i umiejętności z zakresu identyfikowania i zrozumienia zróżnicowanych źródeł zagrożeń ataków cyfrowych oraz do zwiększenia świadomości pracowników w firmie w obszarze cyberbezpieczeństwa.

Uczestnik pozna procedury, które należy wdrożyć w celu zapewnienia bezpieczeństwa infrastruktury cyfrowej. Uczestnik uzyska wiedzę jak analizować i zgłaszać incydenty.

## Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik pozna rodzaje ataków socjotechnicznych i na infrastrukturę	potrafi rozpoznać zagrożenie płynące z sieci i skutecznie je zneutralizować, zna zasady funkcjonowania metod socjotechnicznych w celu wyłudzenia danych (m.in. phishing)	Test teoretyczny
Uczestnik zna zasady bezpiecznego korzystania z Internetu, poczty e-mail oraz mediów społecznościowych i chmury	potrafi rozpoznać fałszywy adres e-mail, aplikację, link, zna metody wyłudzenia danych i umie je zidentyfikować i opisać	Test teoretyczny
Uczestnik stosuje najlepsze praktyki bezpieczeństwa danych i skutecznie reaguje na incydenty cyberbezpieczeństwa.	Potrafi stosować techniki zapobiegania atakom.	Test teoretyczny
	Prawidłowo reaguje na incydenty związane z atakami. Promuje kulturę bezpieczeństwa cyfrowego w organizacji.	Test teoretyczny

## Kwalifikacje

### Kompetencje

Usługa prowadzi do nabycia kompetencji.

### Warunki uznania kompetencji

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

Tak, dokument potwierdza opis efektów uczenia się

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

tak, dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji

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

tak, dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od wal

## Program

1. Pre test
2. Cyberbezpieczeństwo co to jest i czy nas dotyczy?
3. Ataki socjotechniczne

- Czym są ataki socjotechniczne
  - Omówienie przykładów ataków socjotechnicznych
  - Wykrywanie ataków socjotechnicznych
  - Prawidłowa reakcja na ataki socjotechniczne
4. Ataki na infrastrukturę
- Aplikacje i urządzenia mobilne
  - Niebezpieczeństwa związane z pocztą e-mail i załącznikami
  - Strony WWW
  - Ataki przez telefony
  - Ataki typu ransomware
  - Oszustwa phishingowe – rodzaje i charakter ataków
5. Zapewnienie bezpieczeństwa
- Bezpieczeństwo poczty e-mail
  - Polityka zarządzania hasłami
  - Podpisywanie i szyfrowanie dokumentów
  - Bezpieczeństwo fizyczne – polityka czystego biurka oraz czystego ekranu.
6. Post test

## Harmonogram

Liczba przedmiotów/zajęć: 0

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
Brak wyników.					

## Cennik

### Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	1 045,50 PLN
Koszt przypadający na 1 uczestnika netto	850,00 PLN
Koszt osobogodziny brutto	130,69 PLN
Koszt osobogodziny netto	106,25 PLN

## Prowadzący

Liczba prowadzących: 1



## Katarzyna Żółkiewska-Malicka

Dyrektor ds. bezpieczeństwa informacji w ZETO sp. z o.o. w Lublinie. Audytor wewnętrzny, specjalista ds. bezpieczeństwa informacji z 20 letnim stażem pracy, w zakresie przeprowadzania audytów cyberbezpieczeństwa, bezpieczeństwa informacji, ochrony danych osobowych oraz audytów śledczych. Auditor Wiodący systemu zarządzania bezpieczeństwem informacji wg ISO/IEC 27001. Posiada tytuł Executive Master of Business Administration.

Wykładowca w Wyższej Szkole Przedsiębiorczości i Administracji w Lublinie (zajęcia z zakresu ochrony danych osobowych oraz audytu na studiach podyplomowych na kierunku Inspektor Ochrony Danych). Trener prowadzący szkolenia z zakresu bezpieczeństwa informacji, ochrony danych osobowych oraz cyberbezpieczeństwa.

## Informacje dodatkowe

### Informacje o materiałach dla uczestników usługi

Prezentacja zawierająca główne tematy szkolenia.

### Informacje dodatkowe

Szkolenie realizowane jest w godzinach dydaktycznych (45 min). Łącznie realizowanych jest 8 godzin dydaktycznych i 30 minut przerw każdego dnia (przerwy nie wliczane do czasu szkolenia).

Istnieje możliwość zastosowania zwolnienia z podatku VAT dla szkoleń mających charakter kształcenia zawodowego lub służących przekwalifikowaniu zawodowemu pracowników, których poziom dofinansowania ze środków publicznych wynosi co najmniej 70% (na podstawie § 3 ust. 1 pkt 14 Rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. zmieniające rozporządzenie w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień (Dz. U. z 2013 r. poz. 1722 ze zm.)

**Prosimy o kontakt telefoniczny lub mailowy w celu rezerwacji miejsca i uzgodnienia szczegółów szkolenia.**

Warunkiem uzyskania zaświadczenia jest uczestnictwo w co najmniej 80% zajęć usługi rozwojowej oraz zaliczenie zajęć w formie testu wykonywanego na zakończenie szkolenia.

## Adres

ul. Diamentowa 2  
20-447 Lublin  
woj. lubelskie

### Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi
- Laboratorium komputerowe

## Kontakt

Ewa Fronczyk - Kowalczyk

**E-mail** ewa.kowalczyk@zeto.lublin.pl



**Telefon** (+48) 81 7184 250