Możliwość dofinansowania

Cyberbezpieczeństwo w organizacji – aspekty prawne, organizacyjne i techniczne

Numer usługi 2026/07/03/228055/3667798

550,00 PLN brutto
550,00 PLN netto
129,41 PLN brutto/h
129,41 PLN netto/h
128,21 PLN cena rynkowa

STOWARZYSZENIE POLSKA PLATFORMA BEZPIECZEŃSTWA WEWNĘTRZNEGO

Brak ocen dla tego dostawcy

Usługa szkoleniowa
zdalna w czasie rzeczywistym
Zajęcia grupowe
04:15 h
25.11.2026 do 25.11.2026

Informacje podstawowe

Kategoria	Inne / Edukacja
Grupa docelowa usługi	• Pracownicy urzędów administracji publicznej i ich kierownicy • Pracownicy odpowiedzialni za bezpieczeństwo systemów informatycznych • Specjaliści ds. bezpieczeństwa informacji i cyberbezpieczeństwa • Inspektorzy ochrony danych urzędu • Małe i średnie przedsiębiorstwa
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	20-11-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Podstawa uzyskania wpisu do BUR	Standard Usług Szkoleniowo– Rozwojowych PIFS SUS 3.0

Cel

Cel edukacyjny

Celem szkolenia jest wzrost kompetencji kadry w obszarze zagrożeń bezpieczeństwa informacji i cyberbezpieczeństwa.

Główne cele szkolenia to:
- dostarczenie odpowiednich kompetencji uczestnikom kursu,
- podniesienie poziomu bezpieczeństwa w instytucji,
- przygotowanie do wdrażania skutecznych rozwiązań organizacyjnych i zachowań podnoszących cyberbezpieczeństwo w różnego rodzaju organizacjach.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Wzrost świadomości zagrożenia atakiem hackerskim poprzez nabycie umiejętności rozróżniania rodzajów i sposobów ataku oraz rozpoznawanie podejrzanych wiadomości, stron, programów. Szkolenie umożliwi podjęcie działań profilaktycznych, których celem będzie wyeliminowanie ryzyka, które potencjalnie może wystąpić w związku z cyberprzestępczością. Uczestnik szkolenia będzie wiedzieć jak i gdzie zgłaszać próby np. ataku hakerskiego.	Uzyskanie pozytywnego wyniku testu - kryterium 60% poprawnych odpowiedzi.	Test teoretyczny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?

TAK

Pytanie 3. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

I BLOK TEMATYCZNY 9:00-9:45

Wstęp do cyberbezpieczeństwa:

- Jak odróżnić cyberbezpieczeństwo od cyberprzestrzeni?
- Podstawy bezpieczeństwa instytucji – czym jest Polityka Bezpieczeństwa Informacji i SZBI?
- Norma ISO 27001 jako powszechne rozwiązanie i standard bezpieczeństwa.
- Nowe wymagania i obowiązki wdrożeniowe w instytucji w związku z ustawą UKSC 2.0.
- Audyt systemów komputerowych, testy phishingowe i testy penetracyjne.

POKAZ Ataki na „komputery” 9:45-10:45

- Omówienie wraz z demonstracją: Przegląd najczęstszych ataków komputerowych wykorzystywanych przez cyberprzestępców.
- Ataki przez fałszywe maile (kradzież tożsamości, kradzież haseł, tzw. oszustwa nigeryjskie).
- Ataki dokonywane przez telefony komórkowe (fałszywe wiadomości SMS, tzw. SMS Premium, przekierowania rozmów) – przykłady.
- Ataki dokonywane przez sieci bezprzewodowe (WiFi, Bluetooth).
- Malware – złośliwe oprogramowanie instalowane na komputerach, tabletach i smartfonach – przykłady.
- Phishing – podszywanie się pod osoby lub instytucje przykłady.
- Oszustwa inwestycyjne – wykorzystanie zdalnego pulpitu w procederach przestępczych.
- Urządzenia mobilne i komunikatory internetowe podstawy bezpiecznego użytkowania.
- Spoofing telefoniczny – zagrożenia wynikające z możliwości podszywania się pod cudzy numer telefonu.

10:45-11:00 PRZERWA

II BLOK TEMATYCZNY 11:00-12:00

- Socjotechnika, czyli ataki na „człowieka” – omówienie wraz z demonstracją: Jak rozpoznać, że jest się celem ataku socjotechnicznego?
- Przykłady ataków socjotechnicznych: Ataki dokonywane z użyciem social media (Facebook, Instagram), w tym przez komunikatory (Messenger, Skype).
- Miejsca, gdzie zostawiamy swoje dane – działania świadome i nieświadome.
- Sztuczna Inteligencja (AI) – najnowsze zagrożenia: Zagrożenia wynikające z możliwości generowania obrazów i wizerunków.
- Generowanie głosu przez AI: Możliwości złośliwego wykorzystania technologii deepfake.
- Tworzenie złośliwego oprogramowania i skryptów obchodzących zabezpieczenia systemów przy użyciu AI.
- Wykorzystanie sztucznej inteligencji przez oszustów w praktyce.
- Działania ochronne i sposoby wykrywania ataków wspieranych przez AI.

III BLOK TEMATYCZNY 12:00-13:00

- Reagowanie w przypadku rozpoznania cyberprzestępstwa: Gdy instytucja pada ofiarą cyberataku lub cyberprzestępstwa – kogo i jak poinformować (zgodnie z wymogami UKSC 2.0).
- Sposób postępowania w przypadku zgłaszania popełnienia przestępstwa organom ścigania.
- Współdziałanie z organami ścigania w zakresie rozpoznawania i zwalczania cyberprzestępczości.
- Jak skutecznie zabezpieczyć dowody cyberprzestępstwa?
- Podsumowanie i dyskusja.

Harmonogram

Liczba pozycji harmonogramu: 4

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 4 Wstęp do cyberbezpieczeństwa/Ataki na „komputery” – omówienie wraz z demonstracją	Zajęcia	Dawid Rachmajda	25-11-2026	09:00	10:45	01:45
2 z 4 -	Przerwa	-	25-11-2026	10:45	11:00	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
3 z 4 Socjotechnika, czyli ataki na „człowieka”/ Reagowanie w przypadku rozpoznania cyberprzestępstwa	Zajęcia	Dawid Rachmajda	25-11-2026	11:00	13:00	02:00
4 z 4 -	Walidacja	-	25-11-2026	13:00	13:15	00:15

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	04:15
w tym suma godzin zajęć	03:45
w tym suma godzin walidacji	00:15
w tym suma przerw	00:15
Suma godzin dydaktycznych bez przerw	05:15

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	550,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	
Koszt przypadający na 1 uczestnika netto	550,00 PLN
Koszt osobogodziny brutto	129,41 PLN
Koszt osobogodziny netto	129,41 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	04:15

Prowadzący

Liczba prowadzących: 1

1 z 1

Dawid Rachmajda

Ekspert PPBW z zakresu cyberbezpieczeństwa, analityk kryminalny i certyfikowany ekspert w dziedzinie białego wywiadu (OSINT), od ponad 15 lat związany z organami ścigania. Specjalizuje się w zwalczaniu zaawansowanej przestępczości cyfrowej, identyfikowaniu schematów oszustw gospodarczych oraz prowadzeniu dochodzeń w środowiskach trudno dostępnych, takich jak sieć Darknet. Jego kompetencje potwierdzają liczne certyfikaty z zakresu analizy śledczej i bezpieczeństwa IT, w tym specjalistyczne szkolenia organizowane przez United States Secret Service. Posiada formalne uprawnienia pełnomocnika ds. cyberbezpieczeństwa zgodne z nowelizacją ustawy UKSC 2.0 (dyrektywa NIS2). Prelegent na największych wydarzeniach technologicznych, m. in. na konferencji Oh My Hack. Wykształcenie zdobył na Wyższej Szkole Bezpieczeństwa, gdzie ukończył specjalność z zakresu cyberterroryzmu, cyberbezpieczeństwa i bezpieczeństwa publicznego.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały dydaktyczne zostaną udostępnione w formie elektronicznej w dniu szkolenia, przed rozpoczęciem zajęć.

Warunki techniczne

Spotkanie będzie przeprowadzone za pośrednictwem aplikacji Microsoft Teams. Link do spotkania uczestniczy otrzymają na 5 dni przed szkoleniem.

Uczestnik musi posiadać:

- dostęp do komputera ze sprawnym systemem operacyjnym i kamerą internetową, mikrofon
- stabilne łącze internetowe
- dostęp do przeglądarki internetowej lub zainstalowaną aplikację Microsoft Teams
- zaleca się zalogowanie do platformy Microsoft Teams na 10-15 minut przed rozpoczęciem zajęć w celu przetestowania warunków technicznych połączenia

Kontakt

Aneta Jabłońska

E-mail aneta.jablonska@ppbw.pl
Telefon (+48) 695 386 963