Możliwość dofinansowania

Cyberbezpieczeństwo w organizacji – aspekty prawne, organizacyjne i techniczne - szkolenie

Numer usługi 2026/06/29/228055/3656111

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
- 22.09.2026 do 22.09.2026

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	16-09-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Podstawa uzyskania wpisu do BUR	Standard Usług Szkoleniowo– Rozwojowych PIFS SUS 3.0

Cel

Cel edukacyjny

Szkolenie przygotowuje do skutecznego rozpoznawania ataków cyfrowych i socjotechnicznych, przestrzegania procedur bezpieczeństwa oraz prawidłowego reagowania na incydenty w pracy stacjonarnej i zdalnej.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Rozróżnia rodzaje, mechanizmy i sposoby cyberataków ukierunkowanych na organizację.	Charakteryzuje metody działania cyberprzestępców (phishing, smishing, vishing).	Test teoretyczny
	Identyfikuje cechy charakterystyczne podejrzanych wiadomości e-mail oraz fałszywych stron.	Test teoretyczny
	Wskazuje różnice pomiędzy złośliwym oprogramowaniem a atakiem socjotechnicznym.	Test teoretyczny
Stosuje zasady profilaktyki i bezpiecznej pracy z systemami teleinformatycznymi w codziennych obowiązkach służbowych.	Tworzy bezpieczne hasła oraz konfiguruje uwierzytelnianie dwuskładnikowe (MFA).	Test teoretyczny
	Dobiera bezpieczne metody przesyłania i zabezpieczania dokumentów elektronicznych.	Test teoretyczny
	Wykorzystuje zasady bezpiecznego korzystania z Internetu i poczty w pracy stacjonarnej oraz zdalnej.	Test teoretyczny
Organizuje procedurę reagowania na próby ataku oraz incydenty cyberbezpieczeństwa w instytucji.	Kwalifikuje zdarzenie komputerowe jako incydent bezpieczeństwa informacji.	Test teoretyczny
	Wyznacza właściwe osoby i podmioty w instytucji do zgłoszenia zdarzenia.	Test teoretyczny
	Zabezpiecza materiał dowodowy po wykryciu próby cyberataku.	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

Warunki organizacyjne:

- **Forma realizacji:** Szkolenie odbywa się w formule zdalnej w czasie rzeczywistym za pośrednictwem platformy Microsoft Teams. Szkolenie prowadzone jest dla jednej grupy, bez podziału na podgrupy.
- **Stanowisko uczestnika:** Każdy uczestnik pracuje na samodzielnym stanowisku komputerowym z dostępem do stabilnego łącza internetowego, głośników/słuchawek oraz mikrofonu.
- **Materiały:** Uczestnicy otrzymują prezentację oraz materiały szkoleniowe w formie elektronicznej (PDF) w dniu szkolenia.
- **Wsparcie techniczne:** Wykładowca oraz organizator zapewniają bieżącą opiekę techniczną oraz moderatora czatu podczas trwania transmisji.

Sposób organizacji walidacji:

- **Forma walidacji:** Walidacja odbywa się w formie cyfrowego testu wiedzy (post-testu) jednokrotnego lub wielokrotnego wyboru, udostępnianego uczestnikom online po zakończeniu części merytorycznej.
- **Czas trwania:** Na wykonanie testu przewidziano osobny blok czasowy na koniec usługi (ok. 15 minut).
- **Przebieg i ocena:** Każdy uczestnik wypełnia test samodzielnie. Weryfikacja następuje automatycznie lub bezpośrednio przez walidatora. Warunkiem pozytywnego zaliczenia walidacji i uzyskania zaświadczenia jest uzyskanie **minimum 60% poprawnych odpowiedzi**.

I BLOK TEMATYCZNY 9:00-9:45 (Sposób realizacji zajęć: wykład na żywo, prezentacja multimedialna, współdzielenie ekranu, rozmowa na żywo, chat)

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 (Sposób realizacji zajęć: pokaz/pokaz praktyczny na żywo, współdzielenie ekranu, rozmowa na żywo, dyskusja na czacie)

- 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 (Sposób realizacji zajęć: omówienie na żywo, ćwiczenia interaktywne, pokaz/demonstracja na żywo, współdzielenie ekranu, chat, rozmowa na żywo)

- 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 (Sposób realizacji zajęć: wykład na żywo, analiza przypadków, dyskusja, rozmowa na żywo, chat, cyfrowy test wiedzy online)

- 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 Cyberbezpieczeństwo w organizacji – aspekty prawne, organizacyjne i techniczne	Zajęcia	Dawid Rachmajda	22-09-2026	09:00	10:45	01:45
2 z 4 -	Przerwa	-	22-09-2026	10:45	11:00	00:15
3 z 4 Cyberbezpieczeństwo w organizacji – aspekty prawne, organizacyjne i techniczne	Zajęcia	Dawid Rachmajda	22-09-2026	11:00	13:00	02:00
4 z 4 -	Walidacja	-	22-09-2026	13:00	13:15	00:15

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	04:15
w tym suma godzin zajęć	03:45

Rodzaj godzin	Liczba godzin
w tym suma godzin walidacji	00:15
w tym suma przerw	00:15
Suma godzin dydaktycznych bez przerw	05:15

Cennik

Cennik

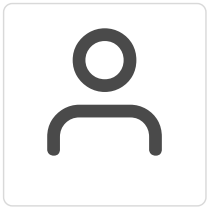
Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	550,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	
Koszt przypadający na 1 uczestnika netto	550,00 PLN
Koszt osobogodziny brutto	129,41 PLN
Koszt osobogodziny netto	129,41 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	04:15

Prowadzący

Liczba prowadzących: 1



1 z 1

Dawid Rachmajda

Doświadczenie i kwalifikacje:

Wykształcenie wyższe (Wyższa Szkoła Bezpieczeństwa – specjalność: cyberterroryzm, cyberbezpieczeństwo i bezpieczeństwo publiczne). Ekspert PPBW z zakresu cyberbezpieczeństwa, analityk kryminalny i certyfikowany ekspert w dziedzinie białego wywiadu (OSINT), od ponad 15 lat związany z organami ścigania.

Doświadczenie z ostatnich 5 lat (2021–2026):

Specjalizuje się w zwalczaniu zaawansowanej przestępczości cyfrowej, identyfikowaniu schematów oszustw gospodarczych oraz prowadzeniu dochodzeń w środowiskach trudno dostępnych (Darknet). W tym okresie zdobył certyfikaty z zakresu analizy śledczej i bezpieczeństwa IT (w tym United States Secret Service) oraz uprawnienia pełnomocnika ds. cyberbezpieczeństwa (UKSC 2.0 / NIS2). W latach 2021–2026 aktywny prelegent na konferencjach technologicznych (m.in. Oh My Hack) oraz trener prowadzący szkolenia i audyty z zakresu cyberbezpieczeństwa dla sektora publicznego i prywatnego.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały dla uczestników usługi:

Każdy uczestnik szkolenia otrzymuje pakiet materiałów dydaktycznych w formie elektronicznej (pliki w formacie PDF), udostępniany przed rozpoczęciem zajęć:

1. **Prezentacja szkoleniowa.**
2. **Instrukcja techniczna:** Praktyczna instrukcja krok po kroku dotycząca procedury szyfrowania dysków.
3. **Poradnik / Instrukcja wdrażania zabezpieczeń:** Instrukcja konfiguracji uwierzytelniania dwuskładnikowego (2FA) oraz wykorzystania fizycznych kluczy bezpieczeństwa dla kont użytkowników (np. Google).
4. **Post-test (arkusz walidacyjny):** Cyfrowy test wiedzy służący do weryfikacji i oceny osiągnięcia efektów uczenia się.

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