Możliwość dofinansowania

TC Kochan Rafał

4,8 / 5

1 446 ocen

Cyberbezpieczeństwo i ochrona danych osobowych w przedsiębiorstwie.

Numer usługi 2025/06/26/16765/2838598

Olecko / stacjonarna

Usługa szkoleniowa

20 h

04.09.2025 do 05.09.2025

3 600,00 PLN brutto

3 600,00 PLN netto

180,00 PLN brutto/h

180,00 PLN netto/h

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie przeznaczone dla przedsiębiorców i ich pracowników, którzy chcą poznać zasady ochrony przed cyberprzestępczością, oraz z uwagi na fakt zarządzania danymi osobowymi, ochrony tych danych przed atakami hakerów.
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	10
Data zakończenia rekrutacji	03-09-2025
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	20
Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Szkolenie przygotowuje do identyfikacji i unikania cyberataków, stosowania polityk bezpieczeństwa w organizacji oraz przestrzegania przepisów prawnych. Potwierdza przygotowanie do skutecznego chronienia wrażliwych informacji i minimalizowania ryzyka naruszeń bezpieczeństwa w firmie.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Weryfikuje wirusy, szpiegowanie oraz rodzaje i sposoby hakowania systemu operacyjnego.	Rozróżnia narzędzia do ochrony przed atakami cyberprzestępców.	Prezentacja
	Rozróżnia narzędzia do ochrony przed złośliwym oprogramowaniem.	Prezentacja
	Charakteryzuje zagrożenie płynące z sieci aby skutecznie je zneutralizować.	Debata swobodna
	Definiuje zasady funkcjonowania metod socjotechnicznych w celu wyłudzenia danych (m.in. phishing).	Debata swobodna
Monitoruje zachowania w sieci, zna tryb bezpieczny i korzysta z trybu incognito.	Rozróżnia niebezpieczne zachowania w sieci.	Debata swobodna
Wdraża procedury zapewniające bezpieczeństwo w sieci.	Tworzy i korzysta z kopii bezpieczeństwa, zabezpiecza komputer przed ryzykiem wykradnięcia danych.	Prezentacja
	Definiuje i wdraża ochronę firmowych systemów.	Prezentacja

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

Szkolenie "Cyberbezpieczeństwo i ochrona danych osobowych w przedsiębiorstwie" ma na celu zwiększenie świadomości kursanta na temat zagrożeń cybernetycznych oraz nauczenie go skutecznych metod ochrony danych firmowych i osobowych. Uczestnik zdobędzie praktyczną wiedzę na temat identyfikacji i unikania cyberataków, stosowania polityk bezpieczeństwa w organizacji oraz przestrzegania przepisów prawnych. Szkolenie wyposaży go w umiejętności związane z bezpiecznym korzystaniem z sieci, zarządzaniem dostępem do informacji oraz stosowaniem odpowiednich narzędzi zabezpieczających dane przed wyciekiem lub kradzieżą. Dzięki temu kursant będzie w stanie skutecznie chronić wrażliwe informacje i minimalizować ryzyko naruszeń bezpieczeństwa w firmie.

Szczegółowy program szkolenia:

Dzień 1

- Największe zagrożenia i skutki cyberataków.
- Narzędzia do ochrony przed atakami cyberprzestępców.
- Narzędzia do ochrony przed złośliwym oprogramowaniem.
- Poznanie zagrożeń płynących z sieci aby skutecznie je zneutralizować.

Dzień 2

- Jakie znamy zasady funkcjonowania metod socjotechnicznych w celu wyłudzenia danych (m.in. phishing).
- Najczęstsze niebezpieczne zachowania w sieci.
- Tworzenie kopii bezpieczeństwa jako podstawowe zabezpieczenie komputera przed ryzykiem wykradnięcia danych.
- Jakie mamy narzędzia do ochrony firmowych systemów.
- Inspiracja i motywowanie innych pracowników do wdrażania procedur podnoszących bezpieczeństwo w sieci.
- Walidacja.

Poniżej przedstawiamy metody i narzędzia dzięki którym Uczestnik może przed rozpoczęciem usługi uzupełnić i uporządkować dotychczasową wiedzę, celem lepszego przyswojenia programu szkoleń oraz czy jest on dobrany adekwatnie do tematyki usługi:

- **Przegląd materiałów:** Przeczytaj lub obejrzyj materiały, które będą omawiane na szkoleniu. To pozwoli Ci na lepsze zrozumienie tematu.
- **Testy i quizy:** Wykonaj testy i quizy online, aby sprawdzić swoją wiedzę. Można korzystać z platform takich jak Quizlet lub Kahoot.
- **Mind map (mapa myśli):** Stwórz mapę myśli, która pomoże zobrazować związki między różnymi tematami. Można użyć narzędzi online, takich jak MindMeister lub XMind.

Walidacja usługi jest wliczona do procesu kształcenia w czasie trwania usługi.

- Aby zaliczyć walidację wymagane jest zaliczenie 90% poprawnych odpowiedzi.
- Walidacja będzie poprowadzona w formie dyskusji, swobodnej debaty na temat realnych zagrożeń - weryfikacja rozumienia ryzyka przez uczestników oraz analizy incydentu bezpieczeństwa – opis sytuacji, w której doszło do naruszenia danych, a uczestnicy mają za zadanie wskazać, co poszło nie tak i jakie kroki należy podjąć.
- Walidacja metodą prezentacji polegać będzie na tym, że każdy uczestnik przygotowuje krótką prezentację (ok. 10 minut). Walidator ocenia poprawność merytoryczną oraz sposób przekazania informacji.

Warunki organizacyjne:

- Każdy uczestnik ma do dyspozycji samodzielne stanowisko komputerowe.
- Każdy uczestnik otrzymuje indywidualne konto na platformie testowej.
- Dostęp do symulowanych środowisk zagrożeń.
- Dokumentacja oraz materiały edukacyjne w formie cyfrowej.
- Wsparcie instruktora w czasie rzeczywistym.

Szkolenie prowadzone jest w godzinach dydaktycznych.

Przerwy są wliczone w czas trwania usługi.

Harmonogram

Liczba przedmiotów/zajęć: 15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 15 Największe zagrożenia i skutki cyberataków.	Paweł Romaniuk	04-09-2025	07:30	08:15	00:45
2 z 15 Narzędzia do ochrony przed atakami cyberprzestępców.	Paweł Romaniuk	04-09-2025	08:15	09:45	01:30
3 z 15 Przerwa	Paweł Romaniuk	04-09-2025	09:45	10:00	00:15
4 z 15 Narzędzia do ochrony przed złośliwym oprogramowaniem.	Paweł Romaniuk	04-09-2025	10:00	12:15	02:15
5 z 15 Przerwa	Paweł Romaniuk	04-09-2025	12:15	12:30	00:15
6 z 15 Poznanie zagrożeń płynących z sieci aby skutecznie je zneutralizować.	Paweł Romaniuk	04-09-2025	12:30	15:30	03:00
7 z 15 Jakie znamy zasady funkcjonowania metod socjotechnicznych w celu wyłudzenia danych (m.in. phishing).	Paweł Romaniuk	05-09-2025	07:30	08:15	00:45
8 z 15 Najczęstsze niebezpieczne zachowania w sieci.	Paweł Romaniuk	05-09-2025	08:15	09:45	01:30
9 z 15 Przerwa	Paweł Romaniuk	05-09-2025	09:45	10:00	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
10 z 15 Tworzenie kopii bezpieczeństwa jako podstawowe zabezpieczenie komputera przed ryzykiem wykradnięcia danych.	Paweł Romaniuk	05-09-2025	10:00	10:45	00:45
11 z 15 Jakie mamy narzędzia do ochrony firmowych systemów.	Paweł Romaniuk	05-09-2025	10:45	12:15	01:30
12 z 15 Przerwa	Paweł Romaniuk	05-09-2025	12:15	12:30	00:15
13 z 15 Jakie mamy narzędzia do ochrony firmowych systemów.	Paweł Romaniuk	05-09-2025	12:30	13:15	00:45
14 z 15 Inspiracja i motywowanie innych pracowników do wdrażania procedur podnoszących bezpieczeństwo w sieci.	Paweł Romaniuk	05-09-2025	13:15	14:00	00:45
15 z 15 Walidacja	-	05-09-2025	14:00	14:30	00:30

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	3 600,00 PLN
Koszt przypadający na 1 uczestnika netto	3 600,00 PLN
Koszt osobogodziny brutto	180,00 PLN

Koszt osobogodziny netto	180,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Paweł Romaniuk

Od 20 lat, trener, specjalista od zabezpieczeń, integracji technologii w procesach sprzedaży orazkonsultant biznesu. Praktyk w obszarach cyberbezpieczeństwa, zarządzania projektami,optymalizacji procesów sprzedaży przy użyciu najnowszej technologii, komunikacji marketingowej,przedsiębiorczości, organizowaniu i prowadzeniu programów wymiany wiedzy i doświadczeń orazzarządzaniu zespołami o zróżnicowanych kompetencjach i specjalizacjach.
Ze szkoleniami związany jest od 2003r. gdzie prowadził szkolenia dla pracowników sektora:zabezpieczeń IT, HR, fi nansowego, bankowego, ubezpieczeniowego.
Posiada wieloletnie doświadczenie praktyczne w zarządzaniu projektami związanymi z wdrażaniem polityk ochrony danych oraz strategii cyberbezpieczeństwa w różnych typach organizacji gdzie wdraża rozwiązania IT, które chronią przed atakami hackerskimi, malwarem i innymi zagrożeniami związanymi z bezpieczeństwem danych. (300h przeprowadzonych strategii). Od 2023 specjalizuje się w transformacji cyfrowej przedsiębiorstw np. w szkoleniu zespołów sprzedażowych w zakresie wykorzystywania nowych technologii w sprzedaży, co pozwala na efektywniejsze zarządzanie procesami sprzedażowymi. Aktualnie bierze udział w projektach implementacji systemów SIEM (Security Information and Event Management), firewall klasy enterprise, monitorowania anomalii sieciowych oraz testów penetracyjnych w celu oceny podatności systemów.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnik otrzyma materiały na każdy z modułów. Będą one składać się z części merytorycznej jak i praktycznej czyli ćwiczeń, zadań domowych, testów. Uczestnik będzie otrzymywał materiały szkoleniowe według potrzeb i wprost proporcjonalnie do przerobionego materiału nauczania. Uczestnicy w ramach usługi otrzymają: skrypty, prezentacje, narzędzia do ćwiczeń etc. w wersji papierowej (istnieje możliwość otrzymania materiałów w formie elektronicznej po uprzednim poinformowaniu firmy szkoleniowej).

Na szkoleniu w celu lepszego zaangażowania uczestników będą wykorzystywane poniższe metody interaktywne:

- Burza mózgów - gdzie Uczestnicy dzielą się swoimi pomysłami, rozwiązaniami lub opiniami na temat konkretnego zagadnienia.
- Dyskusje grupowe - gdzie Uczestnicy dzielą się na małe grupy, które omawiają konkretne pytanie, problem lub temat związany z treścią szkolenia
- Symulacje i gry fabularne - gdzie Uczestnicy wcielają się w role i wykonują zadania, które imitują realne sytuacje związane z tematem szkolenia
- Quizy i ankiety na żywo - Wykorzystanie narzędzi online do przeprowadzenia quizów lub ankiet (np. Mentimeter)

Po zakończonym szkoleniu uczestnik otrzyma zaświadczenie ukończenia szkolenia po potwierdzeniu co najmniej 80% obecności oraz możliwość indywidualnej konsultacji z trenerem po zakończeniu szkolenia.

Warunki uczestnictwa

Warunkiem uczestnictwa w usłudze z dofinansowaniem jest posiadanie ID wsparcia nadanego przez operatora oraz aktywnego konta w Bazie Usług Rozwojowych.

Zapis na szkolenie za pośrednictwem Bazy powinno odbyć się po spełnieniu wszystkich warunków określonych przez Operatora, do którego składają Państwo dokumenty o dofinansowanie.

Przed podpisaniem umowy o dofinansowanie szkolenia z Operatorem, skontaktuj się z nami w celu potwierdzenia terminu szkolenia i dostępności wolnych miejsc.

Informujemy, że w trakcie szkolenia możliwa jest wizyta kontrolna z udziałem PARP, Operatora lub innej jednostki wyznaczonej w celu sprawdzenia poprawności realizacji szkolenia.

Informacje dodatkowe

Godziny szkolenia mogą ulec pewnym przesunięciom ze względu na tempo pracy. W celu zapewnienia pełnej satysfakcji uczestników, staramy się dostosować harmonogram do indywidualnych potrzeb i wymagań uczestników.

Usługa jest zwolniona z podatku VAT w przypadku, kiedy przedsiębiorstwo zwolnione jest z podatku VAT lub dofinansowanie wynosi co najmniej 70%. Podstawa: §3 ust. 1 pkt. 14 rozporządzenia Ministra Finansów z dnia 20.12.2013 r. w sprawie zwolnień od podatku od towarów i usług oraz szczegółowych warunków stosowania tych zwolnień (tekst jednolity Dz.U. z 2020 r., poz. 1983).

Adres

pl. Plac Wolności 7a
19-400 Olecko
woj. warmińsko-mazurskie

Szkolenie odbędzie się w siedzibie firmy BIURO RACHUNKOWE RĘKAWEK Elżbieta Rękawek

Udogodnienia w miejscu realizacji usługi

- Wi-fi
- Klimatyzacja

Kontakt

Marcin Kierdelewicz

E-mail marcin.kierdelewicz84@gmail.com
Telefon (+48) 510 225 135