



BLU PROFESSIONAL
SKILLS INSTITUTE
SPÓŁKA Z
OGRANICZONĄ
ODPOWIEDZIALNOŚ
CIĄ

Brak ocen dla tego dostawcy

Cyberbezpieczeństwo sieci teleinformatycznych w przedsiębiorstwach

Numer usługi 2024/08/22/171618/2274904

📍 Bydgoszcz / stacjonarna
🏠 Usługa szkoleniowa
🕒 8 h
📅 16.12.2024 do 16.12.2024

960,00 PLN brutto
780,49 PLN netto
120,00 PLN brutto/h
97,56 PLN netto/h

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Administracja IT i systemy komputerowe
Identyfikator projektu	Kierunek - Rozwój
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	• Administratorzy IT: Specjaliści zajmujący się zarządzaniem i ochroną infrastruktury sieciowej, którzy muszą znać protokoły sieciowe, systemy operacyjne oraz narzędzia do monitorowania sieci. • Specjaliści ds. bezpieczeństwa informacji: Profesjonaliści, których zadaniem jest identyfikacja i przeciwdziałanie zagrożeniom cybernetycznym oraz wdrażanie polityk bezpieczeństwa. • Menedżerowie IT: Decydenci odpowiedzialni za nadzorowanie polityk IT i koordynację zespołów technicznych w celu minimalizacji ryzyka cyberzagrożeń. • Pracownicy techniczni: Osoby, które na co dzień pracują z sieciami teleinformatycznymi i potrzebują umiejętności technicznych związanych z bezpieczeństwem sieci. • Przedstawiciele firm i organizacji: Pracownicy firm, którzy mają na celu podniesienie poziomu cyberbezpieczeństwa w swoich organizacjach
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	15-12-2024

Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	8
Podstawa uzyskania wpisu do BUR	Certyfikat ICVC - SURE (Standard Usług Rozwojowych w Edukacji): Norma zarządzania jakością w zakresie świadczenia usług rozwojowych

Cel

Cel edukacyjny

Szkolenie „Cyberbezpieczeństwo sieci teleinformatycznych w przedsiębiorstwach” przygotowuje uczestników do podejmowania działań związanych z projektowaniem, zabezpieczaniem i zarządzaniem sieciami teleinformatycznymi w organizacjach. Uczestnicy po zakończeniu szkolenia będą zdolni do samodzielnego identyfikowania zagrożeń, wdrażania procedur bezpieczeństwa oraz skutecznego reagowania na incydenty sieciowe, minimalizując tym samym ryzyko dla bezpieczeństwa firmowych danych.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Charakteryzuje podstawowe zasady bezpieczeństwa sieci teleinformatycznych	Wymienia główne zagrożenia sieciowe i opisuje sposoby ich minimalizacji	Test teoretyczny
	Definiuje podstawowe protokoły sieciowe oraz wyjaśnia ich rolę w zapewnieniu bezpieczeństwa	Test teoretyczny
Identyfikuje i stosuje procedury zabezpieczania infrastruktury sieciowej	Opisuje procesy wdrożenia firewalla i systemów IDS/IPS w sieci firmowej	Test teoretyczny
	Wyjaśnia znaczenie aktualizacji i zarządzania łatkami w kontekście bezpieczeństwa sieci	Test teoretyczny
Rozpoznaje i reaguje na incydenty bezpieczeństwa w sieciach teleinformatycznych	Wymienia kroki do podjęcia w przypadku wykrycia naruszenia bezpieczeństwa	Test teoretyczny
	Opisuje metody raportowania incydentów i sugeruje odpowiednie środki zaradcze	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

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

Wprowadzenie do bezpieczeństwa sieci teleinformatycznych:

Cel i znaczenie bezpieczeństwa sieci w przedsiębiorstwie. Rodzaje zagrożeń sieciowych. Ogólne zasady bezpieczeństwa sieci.

Fundamenty sieci teleinformatycznych:

Struktura sieci i protokoły. Model OSI i TCP/IP. Podstawy technologii sieci bezprzewodowych.

Praktyczne aspekty bezpieczeństwa sieci:

Kontrola dostępu i uwierzytelnianie. Zarządzanie hasłami. Bezpieczeństwo poczty elektronicznej i przeglądarek internetowych.

Twarde i miękkie zagrożenia dla bezpieczeństwa sieci:

Malware: wirusy, trojany, ransomware. Phishing i inne ataki socjotechniczne. Bezpieczeństwo fizyczne i zagrożenia środowiskowe.

Zabezpieczanie sieci teleinformatycznych:

Zasady projektowania bezpiecznej sieci. Wdrożenie zasad bezpieczeństwa: Firewall, IDS/IPS. Bezpieczeństwo sieci bezprzewodowych.

Szyfrowanie i bezpieczeństwo sieci VPN:

Podstawy kryptografii. Zastosowanie VPN do ochrony danych. Zagrożenia dla bezpieczeństwa VPN.

Bezpieczeństwo chmury i zasobów zdalnych:

Bezpieczeństwo infrastruktury chmurowej. Bezpieczeństwo danych w chmurze. Bezpieczeństwo zdalnych pracowników i mobilnych urządzeń.

Zarządzanie incydentami i reagowanie na nie:

Planowanie reagowania na incydenty. Zasady raportowania incydentów. Recuperacja po incydentach.

Aktualizacje i patch management:

Znaczenie aktualizacji i łatek. Zarządzanie procesem aktualizacji. Wykorzystanie narzędzi do zarządzania patchami.

Sesja Q&A

Sesja pytań od uczestników oraz dyskusja moderowana.

Harmonogram

Liczba przedmiotów/zajęć: 10

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 10 Wprowadzenie do bezpieczeństwa sieci teleinformatycznych	Jacek Kapelski	16-12-2024	08:00	08:30	00:30
2 z 10 Fundamenty sieci teleinformatycznych	Jacek Kapelski	16-12-2024	08:30	09:15	00:45
3 z 10 Praktyczne aspekty bezpieczeństwa sieci	Jacek Kapelski	16-12-2024	09:30	10:15	00:45
4 z 10 Twarde i miękkie zagrożenia dla bezpieczeństwa sieci	Jacek Kapelski	16-12-2024	10:15	11:00	00:45
5 z 10 Zabezpieczanie sieci teleinformatycznych	Jacek Kapelski	16-12-2024	11:15	12:00	00:45
6 z 10 Szyfrowanie i bezpieczeństwo sieci VPN	Jacek Kapelski	16-12-2024	12:00	12:45	00:45
7 z 10 Bezpieczeństwo chmury i zasobów zdalnych	Jacek Kapelski	16-12-2024	13:30	14:15	00:45
8 z 10 Zarządzanie incydentami i reagowanie na nie	Jacek Kapelski	16-12-2024	14:30	15:15	00:45

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
9 z 10 Aktualizacje i patch management	Jacek Kapelski	16-12-2024	15:15	15:45	00:30
10 z 10 Sesja Q&A	Jacek Kapelski	16-12-2024	15:45	16:00	00:15

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	960,00 PLN
Koszt przypadający na 1 uczestnika netto	780,49 PLN
Koszt osobogodziny brutto	120,00 PLN
Koszt osobogodziny netto	97,56 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

Jacek Kapelski

Jacek Kapelski to doświadczony ekspert w dziedzinie cyberbezpieczeństwa, z pasją do technologii informatycznych, którą rozwijał przez wiele lat pracy w różnych sektorach IT. Jego kariera zawodowa rozpoczęła się w dużej korporacji, gdzie pełnił rolę administratora IT, zdobywając bezcenne doświadczenie w zarządzaniu rozbudowanymi infrastrukturami sieciowymi i serwerowymi. Dzięki swojej wiedzy i zaangażowaniu, Jacek szybko stał się nieocenionym członkiem zespołu odpowiedzialnego za bezpieczeństwo i stabilność systemów informatycznych firmy. Jacek jest certyfikowanym specjalistą Windows Server, co potwierdza jego głęboką znajomość technologii Microsoft oraz umiejętność zarządzania serwerami na najwyższym poziomie. Jego podejście do cyberbezpieczeństwa cechuje się precyzją i dbałością o najmniejsze detale, co sprawia, że potrafi przewidzieć potencjalne zagrożenia i skutecznie im przeciwdziałać. Jacek wierzy, że kluczem do sukcesu w dzisiejszym cyfrowym świecie jest ciągłe doskonalenie umiejętności oraz poszerzanie wiedzy, co przekłada na swoje szkolenia, które prowadzi z pełnym zaangażowaniem i profesjonalizmem. Prywatnie Jacek jest entuzjastą nowinek technologicznych i chętnie dzieli się swoją wiedzą z innymi, pomagając im lepiej zrozumieć skomplikowane zagadnienia związane z cyberbezpieczeństwem. Na jego szkoleniach uczestnicy mogą liczyć nie tylko na solidną dawkę

wiedzy teoretycznej, ale także na praktyczne wskazówki i rozwiązania, które mogą od razu wdrożyć w swoich firmach.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy otrzymują: skrypt szkoleniowy, prezentację multimedialną, indywidualne długopisy, kartki i inne jednorazowe pomoce dydaktyczne a także certyfikat ukończenia szkolenia

Warunki uczestnictwa

- Uczestnikiem szkolenia może być każda osoba, która spełnia wymagania wiekowe oraz posiada podstawową wiedzę na temat systemów Windows oraz klientów pocztowych.
- Uczestnik powinien posiadać własny komputer przenośny z systemem Windows, który umożliwi mu praktyczne wykonywanie ćwiczeń podczas szkolenia.
- Organizator zapewnia oprogramowanie i środowisko testowe do przeprowadzania praktycznych ćwiczeń.
- Uczestnicy powinni zachować odpowiedni poziom kultury i szacunku wobec prowadzącego oraz innych uczestników szkolenia.
- Uczestnik zobowiązany jest do aktywnego uczestnictwa w szkoleniu i wykonywania zadań praktycznych, które są częścią programu szkolenia.

Adres

ul. Kijowska 44
85-703 Bydgoszcz
woj. kujawsko-pomorskie

Udogodnienia w miejscu realizacji usługi

- Wi-fi

Kontakt



Michał Majcherek

E-mail szkolenia@bps.edu.pl

Telefon (+48) 537 770 040