



Ernabo Adrian Flak

★★★★★ 4,6 / 5

789 ocen

Szkolenie: Cyberbezpieczeństwo

Numer usługi 2026/01/03/22948/3237876

📍 zdalna w czasie rzeczywistym

🏠 Usługa szkoleniowa

🕒 10 h

📅 28.03.2026 do 28.03.2026

900,00 PLN brutto

900,00 PLN netto

90,00 PLN brutto/h

90,00 PLN netto/h

Informacje podstawowe

Kategoria

Informatyka i telekomunikacja / Bezpieczeństwo IT

Identyfikatory projektów

Kierunek - Rozwój, Małopolski Pociąg do kariery, Zachodniopomorskie Bony Szkoleniowe

Grupa docelowa usługi

Pracownicy firm i instytucji publicznych, którzy korzystają z komputerów, internetu i poczty elektronicznej w pracy.

Osoby odpowiedzialne za przetwarzanie danych firmowych lub wrażliwych.

Każdy, kto chce zwiększyć świadomość zagrożeń w sieci i nauczyć się podstawowych metod ochrony danych.

- Szkolenie przeznaczone jest również dla uczestników projektu **Kierunek Rozwój** realizowany przez WUP w Toruniu.
- Usługa również adresowana dla Uczestników Projektu **Małopolski Pociąg do Kariery sezon 1**
- Usługa skierowana również dla uczestników projektu "Zachodniopomorskie bony szkoleniowe"
- Oraz dla uczestników projektów dofinansowanych w całej Polsce
- Szkolenie skierowane jest zarówno do **osób indywidualnych, jak i pracodawców i ich pracowników.**

Minimalna liczba uczestników

5

Maksymalna liczba uczestników

10

Forma prowadzenia usługi

zdalna w czasie rzeczywistym

Liczba godzin usługi

10

Podstawa uzyskania wpisu do BUR

Certyfikat systemu zarządzania jakością wg. ISO 9001:2015 (PN-EN ISO 9001:2015) - w zakresie usług szkoleniowych

Cel

Cel edukacyjny

Szkolenie przygotowuje uczestników do rozpoznawania zagrożeń w sieci i stosowania praktycznych metod ochrony danych oraz systemów w codziennej pracy. Uczestnicy nauczą się bezpiecznego korzystania z komputerów, poczty elektronicznej i urządzeń mobilnych oraz reagowania na potencjalne incydenty cyberbezpieczeństwa.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Rozpoznaje zagrożenia w sieci (phishing, malware, ransomware, socjotechnika)	Nazwać co najmniej 3 rodzaje ataków cybernetycznych.	Test teoretyczny z wynikiem generowanym automatycznie
	Analizuje przykładowe e-maile lub strony internetowe i określa, które są potencjalnie niebezpieczne.	Test teoretyczny z wynikiem generowanym automatycznie
	Wyjaśnia różnice między phishingiem, malware a ransomware na podstawie realnych przykładów.	Test teoretyczny z wynikiem generowanym automatycznie
: Stosuje zasady bezpieczeństwa w codziennej pracy z komputerem i urządzeniami mobilnymi	Tworzy silne hasła	Test teoretyczny z wynikiem generowanym automatycznie
	Wdraża zasady bezpiecznego korzystania z poczty elektronicznej i Internetu.	Test teoretyczny z wynikiem generowanym automatycznie
Chroni dane osobowe i firmowe zgodnie z RODO i dobrymi praktykami cyberbezpieczeństwa	Identyfikuje dane osobowe w dokumentach i wiadomościach elektronicznych	Test teoretyczny z wynikiem generowanym automatycznie
	Stosuje podstawowe zasady szyfrowania danych i komunikacji.	Test teoretyczny z wynikiem generowanym automatycznie
	Opisuje procedurę odzyskiwania danych w razie awarii.	Test teoretyczny z wynikiem generowanym automatycznie
	Wskazuje kroki postępowania w przypadku wykrycia phishingu lub ransomware.	Test teoretyczny z wynikiem generowanym automatycznie
	Przeprowadza symulację zgłoszenia incydentu do działu IT lub odpowiednich służb.	Test teoretyczny z wynikiem generowanym automatycznie
Reaguje na incydenty cybernetyczne, minimalizując ich skutki	Ocenia stopień ryzyka i podejmuje odpowiednie działania minimalizujące skutki incydentu.	Test teoretyczny z wynikiem generowanym automatycznie

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

Program szkolenia jest dostosowany do potrzeb uczestników usługi oraz głównego celu usługi i jej charakteru oraz obejmuje zakres tematyczny usługi. Uczestnik nie musi spełniać dodatkowych wymagań dot. poziomu zaawansowania.

Usługa prowadzona jest w godzinach dydaktycznych. Przerwy nie są wliczone w ogólny czas usługi rozwojowej. Harmonogram usługi może ulec nieznacznemu przesunięciu, ponieważ ilość przerw oraz długość ich trwania zostanie dostosowana indywidualnie do potrzeb uczestników szkolenia. Łączna długość przerw podczas szkolenia nie będzie dłuższa aniżeli zawarta w harmonogramie.

Zajęcia zostaną przeprowadzone przez ekspertów z wieloletnim doświadczeniem, którzy przekazują nie tylko wiedzę teoretyczną, ale także praktyczne wskazówki i najlepsze praktyki. Uczestnicy mają możliwość czerpania z jego wiedzy i doświadczeń.

Szkolenie będzie realizowane **zdalnie w czasie rzeczywistym** za pomocą platformy **ClickMeeting**, co umożliwi aktywny udział uczestników w warsztatach i ćwiczeniach grupowych.

Szkolenie realizowane jest przez platformę umożliwiającą:

- udostępnianie ekranu,
- czat, komunikację audio-wideo,
- współdzielenie materiałów i plików,
- interaktywną prezentację kodu i analiz danych.

Każdy uczestnik pracuje indywidualnie na swoim komputerze z bieżącym wsparciem trenera.

Przed dokonaniem zapisu i złożeniem karty uczestnictwa do Operatora, zachęcamy do **kontaktowania się z nami telefonicznie, SMS-em lub e-mailem** pod adresem/numerem wskazanym w zakładce „**Kontakt**”.

Pozwoli to **potwierdzić dostępność miejsca** w grupie szkoleniowej oraz rozwiązać ewentualne wątpliwości.

Program szkolenia:

Moduł 1: Wprowadzenie do cyberbezpieczeństwa (1 godz. dydaktyczna)

- Definicja cyberbezpieczeństwa.
- Podstawowe pojęcia: hacker, malware, ransomware, phishing.
- Przykłady realnych incydentów cybernetycznych.

- Znaczenie świadomości użytkownika w ochronie danych.

Metody: prezentacja, dyskusja, quiz wprowadzający.

Moduł 2: Zagrożenia i ataki w sieci (2 godz. dydaktyczne)

- Rodzaje zagrożeń:
 - Wirusy, trojany, ransomware.
 - Phishing i spear phishing.
 - Ataki typu Man-in-the-Middle, DDoS.
 - Socjotechnika.
- Analiza przykładów ataków.
- Jak rozpoznawać podejrzane działania.

Metody: case study, analiza przykładowych wiadomości e-mail i stron internetowych, ćwiczenia praktyczne.

Moduł 3: Bezpieczeństwo urządzeń i systemów (2 godz. dydaktyczne)

- Aktualizacje systemów i oprogramowania.
- Oprogramowanie antywirusowe i firewall.
- Bezpieczne konfiguracje urządzeń.
- Zabezpieczenie urządzeń mobilnych i zdalnej pracy.

Metody: prezentacja, , dyskusja.

Moduł 4: Bezpieczne korzystanie z internetu i e-maila (1,5 godz. dydaktyczna)

- Silne hasła i zarządzanie nimi (menedżery haseł).
- Autoryzacja dwuskładnikowa (2FA).
- Rozpoznawanie podejrzanych linków i załączników.
- Bezpieczne korzystanie z mediów społecznościowych.

Metody: warsztat praktyczny, ćwiczenia w tworzeniu bezpiecznych haseł.

Moduł 5: Ochrona danych osobowych i firmowych (1,5 godz. dydaktyczna)

- Podstawy RODO i prawa w cyberbezpieczeństwie.
- Szyfrowanie danych i komunikacji.
- Backup i odzyskiwanie danych.
- Polityki bezpieczeństwa w firmie.

Metody: prezentacja, dyskusja, krótkie ćwiczenia.

Moduł 6: Reagowanie na incydenty i plan awaryjny (1 godz. dydaktyczna)

- Co zrobić w przypadku ataku (phishing, ransomware, utrata danych).
- Zgłaszanie incydentów.
- Tworzenie planu awaryjnego dla danych i systemów.
- Podstawy cyberhigieny w codziennej pracy.

Metody: scenariusze praktyczne, symulacja incyduentu, dyskusja.

Moduł 7: Podsumowanie i test wiedzy (1 godz. dydaktyczna)

Omówienie najważniejszych zasad.

Test wiedzy

Harmonogram

Liczba przedmiotów/zajęć: 1

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 1 DZIEŃ 1// 10 godzin dyd + 30 min przerwy/ Szczegółowy harmonogram z podziałem godz. zostanie udostępniony maksymalnie na 7 dni przed rozpoczęciem usługi	Marcin Rał	28-03-2026	08:00	16:00	08:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	900,00 PLN
Koszt przypadający na 1 uczestnika netto	900,00 PLN
Koszt osobogodziny brutto	90,00 PLN
Koszt osobogodziny netto	90,00 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

Marcin Rał

Praktyk i szkoleniowiec w zakresie technologii chmurowych oraz programowania. Uczy, jak skutecznie wykorzystać chmurę do optymalizacji procesów oraz efektywnego zarządzania infrastrukturą IT w sposób sprzyjający zrównoważonemu rozwojowi. Jako wykładowca na Uczelni Wyższej prowadzi zajęcia z programowania klienckiego, zarządzania usługami chmurowymi oraz baz danych dla aplikacji internetowych. Posiada ponad kilkunastoletnie doświadczenie w branży IT i zrealizował liczne kursy oraz warsztaty, skierowane zarówno do początkujących, jak i zaawansowanych. Jego szkolenia podkreślają, że technologie chmurowe odgrywają kluczową rolę w transformacji ekologicznej. Dzięki elastyczności i wydajności, jakie oferują chmury, organizacje mają możliwość zmniejszenia zużycia energii i zasobów, co ma pozytywny wpływ na ochronę środowiska. W 2023 roku zdobył certyfikat " Zielone kompetencje IT".

W ostatnich 24 miesiącach przeprowadził ponad 200 godzin szkoleń związanych z tematyką IT, w tym Cyberbezpieczeństwa.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdy z uczestników otrzyma materiały dydaktyczne- prezentację w formie e-mail.

Trener prowadzący szkolenie na bieżąco będzie przysyłał zadania oraz ćwiczenia.

Warunki uczestnictwa

Warunkiem zdobycia certyfikatu potwierdzającego zdobyte kompetencje jest przystąpienie do Egzaminu . Na egzamin uczestnik nie musi dokonywać osobnego zapisu oraz jest w koszt usługi.

Wymagana jest obecność min 80% lub zgodna ze wskazaniami Operatora. Obecność na usłudze weryfikowana będzie na podstawie raportu logowań wygenerowanego z platformy.

Uczestnicy przyjmują do wiadomości, że usługa może być poddana monitoringowi z ramienia Operatora lub PARP i wyrażają na to zgodę.

Uczestnik ma obowiązek zapisania się na usługę przez BUR co najmniej w dniu zakończenia rekrutacji.

Organizator zapewnia dostępność osobom ze szczególnymi potrzebami podczas realizacji usług rozwojowych zgodnie z Ustawą z dnia 19 lipca 2019 r. o zapewnianiu dostępności osobom ze szczególnymi potrzebami (Dz.U. 2022 poz. 2240) oraz „Standardami dostępności dla polityki spójności 2021-2027”. **W przypadku potrzeby zapewnienia specjalnych udogodnień prosimy o kontakt przed zapisem na usługę!**

Informacje dodatkowe

- **Zapis BUR nie jest jednoznaczny z zarezerwowaniem miejsca.** W celu potwierdzenia miejsca prosimy o dodatkowy kontakt telefoniczny/sms lub mailowy na adres/numer wskazany w zakładce " kontakt"
- zawarto umowę z WUP w Toruniu w ramach projektu Kierunek Rozwój
- zawarto umowę z WUP w Krakowie w ramach projektu Małopolski Pociąg do Kariery
- zawarto umowę z WUP w Szczecinie w ramach projektu Zachodniopomorskie Bony Szkoleniowe
- usługi dedykowane również uczestnikom innych programów dofinansowań

Podstawa zwolnienia z VAT:

1) art. 43 ust. 1 pkt 29 lit. c Ustawy z dnia 11 marca 2024 o podatku od towarów i usług - w przypadku dofinansowania w wysokości 100%

2) § 3 ust. 1 pkt. 14 Rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień - w przypadku dofinansowania w co najmniej 70%

3) W przypadku braku uzyskania dofinansowania lub uzyskania dofinansowania poniżej 70%, do ceny usługi należy doliczyć 23% VAT

Warunki techniczne

1. Sprzęt uczestnika:

- **komputer lub laptop** z systemem operacyjnym Windows 10 / 11, macOS lub Linux,
- **procesorem** co najmniej **Intel i5 / Ryzen 5** lub równoważnym,
- **pamięcią RAM: minimum 8 GB** (zalecane 16 GB dla płynnej pracy z dużymi zbiorami danych),
- **wolną przestrzenią dyskową: minimum 10 GB,**
- **stabilne łącze internetowe (min. 10 Mbps)** – w przypadku zajęć zdalnych,
- **aktualna przeglądarką internetową (Chrome, Edge, Firefox),**

Obowiązkowe:

- **Kamera:** Uczestnik powinien posiadać działającą kamerę (wbudowaną w laptop/komputer lub zewnętrzną). Kamera umożliwia aktywny udział w sesjach, prezentację ćwiczeń grupowych oraz interakcję z prowadzącym.
- **Mikrofon:** Niezbędny jest sprawny mikrofon (wbudowany lub zewnętrzny, np. w zestawie słuchawkowym). Umożliwia zadawanie pytań, udział w dyskusjach i ćwiczeniach grupowych.
- Zalecane użycie słuchawek z mikrofonem, aby zredukować echo i poprawić jakość dźwięku.

2. Oprogramowanie:

Nie jest wymagane wcześniejsze przygotowanie środowiska programistycznego. Wszystkie niezbędne programy, dane i narzędzia zostaną przekazane przez trenera w trakcie trwania szkolenia.

3. Łącze internetowe:

- Minimum 10 Mbps download / 5 Mbps upload
- Stabilne połączenie bez dużych przerw i opóźnień

4. Środowisko pracy:

- Ciche miejsce do pracy i nauki
- Dostęp do powierzchni roboczej umożliwiającej komfortowe używanie komputera
- Możliwość dzielenia ekranu w trakcie sesji praktycznych i konsultacji

5. Środowisko szkoleniowe

Szkolenie realizowane jest przez platformę umożliwiającą:

- udostępnianie ekranu,
- czat, komunikację audio-wideo,
- współdzielenie materiałów i plików,
- interaktywną prezentację kodu i analiz danych.

Kontakt



NIKOL WATOŁA

E-mail nikol.watola@ernabo.com

Telefon (+48) 530 642 270