



## Cyberbezpieczeństwo w procesie transformacji cyfrowej przedsiębiorstw z uwzględnieniem zagrożenia militarnego oraz zgodności z prawem krajowym i międzynarodowym - szkolenie

3 375,00 PLN brutto

3 375,00 PLN netto

225,00 PLN brutto/h

225,00 PLN netto/h

K2 CONSULTING  
SPÓŁKA Z  
OGRA NICZONĄ  
ODPOWIEDZIALNOŚĆ  
CIA

Numer usługi 2024/11/03/153767/2393079

📍 Góra Puławska / stacjonarna

🏠 Usługa szkoleniowa

🕒 15 h

📅 16.12.2024 do 17.12.2024



## Informacje podstawowe

<b>Kategoria</b>	Informatyka i telekomunikacja / Bezpieczeństwo IT
<b>Sposób dofinansowania</b>	wsparcie dla osób indywidualnych
<b>Grupa docelowa usługi</b>	Szkolenie dedykowane jest pracownikom, którzy w ramach wykonywania swoich obowiązków służbowych mają styczność z infrastrukturą IT przedsiębiorcy, a w szczególności w swojej pracy codziennej korzystają z narzędzi teleinformatycznych takich jak komputery osobiste, telefony komórkowe czy laptopy i tablety. Osoby te na bazie tych urządzeń mają dostęp do danych firmowych co wpływa na bezpieczeństwo ich przetwarzania w toku transformacji cyfrowej firm wymuszonej przez realia XXI wieku. Wymagalny minimalny staż pracy na danym stanowisku wynoszący co najmniej 1 miesiąc.
<b>Minimalna liczba uczestników</b>	14
<b>Maksymalna liczba uczestników</b>	18
<b>Data zakończenia rekrutacji</b>	15-12-2024
<b>Forma prowadzenia usługi</b>	stacjonarna
<b>Liczba godzin usługi</b>	15
<b>Podstawa uzyskania wpisu do BUR</b>	Certyfikat systemu zarządzania jakością wg. ISO 9001:2015 (PN-EN ISO 9001:2015) - w zakresie usług szkoleniowych

# Cel

## Cel edukacyjny

Szkolenie "Cyberbezpieczeństwo w procesie transformacji cyfrowej przedsiębiorstw z uwzględnieniem zagrożenia militarnego oraz zgodności z prawem krajowym i międzynarodowym" przygotowuje pracownika do bezpiecznego i świadomego przetwarzania danych w toku procesu cyfryzacji przedsiębiorstwa w oparciu o przepisy prawa krajowego i międzynarodowego poprzez poznanie metod ataków, mechanizmów obrony i działań zapobiegawczych przed cyberatakami.

## Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik definiuje podstawowe zagadnienia z zakresu bezpieczeństwa systemów informatycznych	Wyjaśnia pojęcia takie jak IT Security, inżynieria społeczna, oraz Open Source Intelligence	Wywiad swobodny
Uczestnik stosuje i przestrzega polityki hasel jako narzędzia wpływającego na bezpieczeństwo	Potrafi zaplanować politykę hasel w firmie, opierając się na najlepszych praktykach i standardach bezpieczeństwa	Wywiad swobodny
Uczestnik zarządza hasłami od strony formalnej i praktycznej	Stosuje metody zarządzania hasłami, w tym korzystanie z narzędzi IT wspierających zarządzanie hasłami, takich jak menedżery hasel	Wywiad swobodny
Uczestnik ocenia zagrożenia związane z funkcjonowaniem systemów poczty elektronicznej	Identyfikuje zagrożenia związane z pocztą e-mail oraz zna odpowiednie środki zapobiegawcze i zabezpieczenia	Wywiad swobodny
Uczestnik definiuje wpływ cyfryzacji komunikacji na bezpieczeństwo przedsiębiorstwa	Ocena ryzyko związane z cyfryzacją komunikacji, w tym używanie telefonów komórkowych i komunikatorów internetowych, oraz proponuje strategie minimalizacji tego ryzyka	Wywiad swobodny
Uczestnik definiuje podstawowe mechanizmy bezpieczeństwa w kontekście oprogramowania	Wyjaśnia najlepsze praktyki dotyczące kopii zapasowych, aktualizacji oprogramowania oraz korzystania z różnych aplikacji	Wywiad swobodny
Uczestnik identyfikuje zagrożenia związane z urządzeniami mobilnymi i nośnikami zewnętrznymi	Rozpoznaje i określa potencjalne wektory ataków poprzez urządzenia mobilne i zewnętrzne nośniki danych, opisuje odpowiednie środki zaradcze	Wywiad swobodny
Uczestnik definiuje metody ochrony środków pieniężnych w kontekście bankowości internetowej	Opisuje i wie jak zastosować metody ochrony środków pieniężnych, takie jak bezpieczne korzystanie z bankowości internetowej i kart płatniczych	Wywiad swobodny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik identyfikuje wpływ zagrożeń militarnych na cyberbezpieczeństwo przedsiębiorstwa	Omawia podstawowe pojęcia i modele związane z zagrożeniami militarnymi w cyberprzestrzeni oraz przywołać odpowiednie akty prawne regulujące te kwestie	Wywiad swobodny
Uczestnik rozróżnia i klasyfikuje programy złośliwe	Potrafi rozpoznać różne rodzaje programów złośliwych, takie jak wirusy, trojany, ransomware, oraz potrafi zastosować odpowiednie techniki ich neutralizacji i zapobiegania	Wywiad swobodny

## Kwalifikacje

### Kompetencje

Usługa prowadzi do nabycia kompetencji.

### Warunki uznania kompetencji

**Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?**

Tak. Zaświadczenia wydawane uczestnikom po odbytych szkoleniach zawierają opis efektów uczenia się.

**Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?**

Tak. Zaświadczenie o ukończeniu szkolenia potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane kryteria weryfikacji.

**Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?**

Tak. Zaświadczeniu o ukończeniu szkolenia potwierdza, że zarówno proces szkolenia, jak i jego weryfikacja zostały przeprowadzone z uwzględnieniem środków zapewniających niezależność tych etapów.

## Program

### Moduł I - wprowadzenie do bezpieczeństwa systemów Informatycznych

- Wprowadzenie do zagadnień z zakresu IT Security
- Polityka haseł jako narzędzie wpływające na bezpieczeństwo
- Metodyka zarządzania hasłami od strony formalnej
- Narzędzia IT wspierające zarządzanie hasłami
- Wprowadzenie do zagadnienia - Inżynieria społeczna
- Wprowadzenie do zagadnienia - Open Source Intelligence tzw. "biały wywiad"
- Warsztaty praktyczne

### Moduł II - sieć Internet jako zagrożenie dla przedsiębiorstwa

- Bezpieczeństwo związane z funkcjonowaniem systemów poczty elektronicznej
- Prawo krajowe i międzynarodowe w odniesieniu do cyfryzacji komunikacji w przedsiębiorstwie

- Uwarunkowania korzystania z usług hostingu stron www w odniesieniu do prawa krajowego i międzynarodowego
- Case study: poczta e-mail jako wektor ataku
- Case study: strona www przedsiębiorstwa jako wektor ataku
- Cyfryzacja komunikacji w przedsiębiorstwie jako wektor ataku w odniesieniu do telefonów komórkowych oraz komunikatorów internetowych
- Warsztaty praktyczne

### Moduł III - oprogramowanie wykorzystywane w firmie jako wektor ataku

- Kopie zapasowe danych jako podstawowy mechanizm bezpieczeństwa Informatycznego przedsiębiorstwa
- Case study: najczęściej popełniane błędy w odniesieniu do logiki funkcjonowania systemu kopii bezpieczeństwa
- Niewykonanie aktualizacji oprogramowania jako wektor ataku na przedsiębiorstwo
- Bezpieczeństwo IT w odniesieniu do oprogramowania Microsoft Office 2021
- Bezpieczeństwo IT w odniesieniu do oprogramowania Mozilla Thunderbird
- Bezpieczeństwo IT w odniesieniu do przeglądarek internetowych
- Warsztaty praktyczne

### Moduł IV - ochrona informacji oraz środków pieniężnych

- Urządzenia mobilne takie jak telefony, tablety, laptopy jako wektor ataku na przedsiębiorstwo
- Case study: sieci WiFi jako wektor ataku na przedsiębiorstwo
- Bezpieczeństwo danych w odniesieniu do zewnętrznych nośników danych takich jak pamięci pendrive oraz zewnętrzne dyski twarde
- Metody ochrony środków pieniężnych w odniesieniu do bankowości internetowej oraz kart płatniczych
- Warsztaty praktyczne

### Moduł V - Zagrożenie militarne a cyberbezpieczeństwo przedsiębiorstwa.

- podstawowe pojęcia i modele
- przegląd aktów prawnych regulujących funkcjonowanie cyberprzestrzeni
- klasyfikacja programów złośliwych

- 
- Szkolenie ma charakter praktyczny i aktywizujący w celu wypracowania najkorzystniejszego podejścia oraz rozwiązań dla organizacji.
  - Warunki niezbędne do spełnienia, aby realizacja usługi pozwoliła na osiągnięcie głównego celu: Aby osiągnąć główny cel usługi, uczestnicy muszą wziąć udział w całym szkoleniu (100% frekwencji), aktywnie uczestniczyć w szkoleniu.
  - Szkolenie dedykowane jest pracownikom, którzy w ramach wykonywania swoich obowiązków służbowych mają styczność z infrastrukturą IT przedsiębiorcy, a w szczególności w swojej pracy codziennej korzystają z narzędzi teleinformatycznych takich jak komputery osobiste, telefony komórkowe czy laptopy i tablety. Osoby te na bazie tych urządzeń mają dostęp do danych firmowych co wpływa na bezpieczeństwo ich przetwarzania w toku transformacji cyfrowej firm wymuszonej przez realia XXI wieku. Wymagany minimalny staż pracy 1 miesiąc.
  - Trener na bieżąco - w trakcie trwania usługi weryfikuje postępy i ocenia efekty uczenia. Po zakończonej usłudze zostaje przeprowadzona walidacja, oparta o założone kryteria weryfikacji efektów uczenia się, realizowana jest z zachowaniem rozdzielności funkcji.
  - W ramach realizacji szkolenia uczestnicy otrzymują materiały merytoryczne w formie prezentacji. Materiały wysyłane są na adresy mailowe uczestników szkolenia.
  - Usługa realizowana jest w godzinach zegarowych (1 godzina zegarowa = 60 minut).
  - Przerwy wliczone są w czas trwania szkolenia.

## Harmonogram

Liczba przedmiotów/zajęć: 9

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<b>1 z 9</b> Moduł I - wprowadzenie do bezpieczeństwa systemów Informatycznych	Kamil Kamola	16-12-2024	08:00	11:00	03:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<b>2 z 9</b> Moduł II - sieć Internet jako zagrożenie dla przedsiębiorstwa	Kamil Kamola	16-12-2024	11:00	13:00	02:00
<b>3 z 9</b> Przerwa	Kamil Kamola	16-12-2024	13:00	13:15	00:15
<b>4 z 9</b> Moduł II - sieć Internet jako zagrożenie dla przedsiębiorstwa c.d	Kamil Kamola	16-12-2024	13:15	15:00	01:45
<b>5 z 9</b> Moduł III - oprogramowanie wykorzystywane w firmie jako wektor ataku	Kamil Kamola	16-12-2024	15:00	16:00	01:00
<b>6 z 9</b> Moduł III - oprogramowanie wykorzystywane w firmie jako wektor ataku c.d	Kamil Kamola	17-12-2024	08:00	10:00	02:00
<b>7 z 9</b> Moduł IV - ochrona informacji oraz środków pieniężnych	Kamil Kamola	17-12-2024	10:00	13:00	03:00
<b>8 z 9</b> Przerwa	Kamil Kamola	17-12-2024	13:00	13:15	00:15
<b>9 z 9</b> Moduł V - Zagrożenie militarne a cyberbezpieczeństwo przedsiębiorstwa	Kamil Kamola	17-12-2024	13:15	15:00	01:45

## Cennik

### Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	3 375,00 PLN

<b>Koszt przypadający na 1 uczestnika netto</b>	3 375,00 PLN
<b>Koszt osobogodziny brutto</b>	225,00 PLN
<b>Koszt osobogodziny netto</b>	225,00 PLN

## Prowadzący

Liczba prowadzących: 1



1 z 1

### Kamil Kamola

Przedsiębiorca posiadający 13-letnie doświadczenie zawodowe w branży IT. W trakcie swojej pracy zawodowej kładzie nacisk na rozwój praktycznych umiejętności w zakresie bezpieczeństwa systemów informatycznych pod kątem zgodności z obecnie obowiązującymi przepisami prawa międzynarodowego oraz krajowego. W swojej codziennej pracy koordynuje działania związane z funkcjonowaniem sektora IT przedsiębiorstw prywatnych jak i podmiotów publicznych, świadczy usługi z zakresu m.in. modelowania procesów biznesowych, audytów oraz analiz przedwdrożeniowych. W przeszłości zdobywał doświadczenie zawodowe na stanowisku programisty aplikacji webowych. Osoba posiadająca bogate doświadczenie zawodowe zbudowane na praktyce, a nie jedynie samej teorii. Posiada średnie wykształcenie. Posiada co najmniej 250 godzin doświadczenia w realizacji szkoleń w podobnej tematyce zrealizowanych w ostatnich pięciu latach (60 miesiącach) wstecz od dnia rozpoczęcia szkolenia.

## Informacje dodatkowe

### Informacje o materiałach dla uczestników usługi

W ramach realizacji szkolenia uczestnicy otrzymują materiały merytoryczne w formie prezentacji. Materiały wysyłane są na adresy mailowe uczestników szkolenia.

### Warunki uczestnictwa

Koszt szkolenia nie zawiera kosztów dojazdu, zakwaterowania oraz wyżywienia, a także kosztów środków trwałych.

### Informacje dodatkowe

Usługa zwolniona z VAT na podstawie §3 ust.1 pkt 14 rozporządzenia Ministra Finansów z dnia 20.12.2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień (Dz.U. z 2015 r., poz.736)

## Adres

ul. Radomska 52C  
24-100 Góra Puławska

woj. lubelskie

Szkolenie odbędzie się w siedzibie IMTech.

## Kontakt



**Kamil Kamola**

**E-mail** [bur@k2c.com.pl](mailto:bur@k2c.com.pl)

**Telefon** (+48) 533 552 510