



K2 GROUP SPÓŁKA  
Z OGRANICZONĄ  
ODPOWIEDZIALNOŚ  
CIĄ

★★★★★ 4,6 / 5

86 ocen

## Cyberbezpieczeństwo w organizacji – ochrona danych i bezpieczna praca w środowisku cyfrowym - szkolenie.

Numer usługi 2026/07/13/179479/3685266

📍 Puławy

🏢 Usługa szkoleniowa

📅 stacjonarna

👤 Zajęcia indywidualne

🕒 15:00 h

📅 20.08.2026 do 21.08.2026

4 280,40 PLN brutto

3 480,00 PLN netto

285,36 PLN brutto/h

232,00 PLN netto/h

261,33 PLN cena rynkowa ⓘ

## Informacje podstawowe

### Kategoria

Informatyka i telekomunikacja / Bezpieczeństwo IT

### Grupa docelowa usługi

Szkolenie skierowane do właściciela przedsiębiorstwa, który w ramach prowadzonej działalności gospodarczej korzysta z narzędzi teleinformatycznych, takich jak komputer, laptop, smartfon, poczta elektroniczna, systemy informatyczne oraz usługi internetowe i chmurowe. Uczestnik posiada dostęp do danych firmowych, dokumentacji elektronicznej oraz informacji dotyczących klientów, kontrahentów i procesów biznesowych, przez co odpowiada za bezpieczeństwo ich przetwarzania i ochronę przed zagrożeniami cybernetycznymi.

Usługa jest przeznaczona dla osoby zarządzającej przedsiębiorstwem, która chce podnieść swoje kompetencje w zakresie ochrony danych, bezpiecznego korzystania z technologii cyfrowych, rozpoznawania cyberzagrożeń oraz wdrażania dobrych praktyk cyberbezpieczeństwa wspierających bezpieczne funkcjonowanie firmy w środowisku cyfrowym.

### Minimalna liczba uczestników

1

### Maksymalna liczba uczestników

1

### Data zakończenia rekrutacji

19-08-2026

### Forma prowadzenia usługi

stacjonarna

### Podstawa uzyskania wpisu do BUR

Certyfikat ISO 21001: 2018 Organizacje edukacyjne – „Systemy zarządzania dla organizacji edukacyjnych – wymagania ze wskazówkami dotyczącymi użytkowania”

# Cel

## Cel edukacyjny

Szkolenie przygotowuje uczestnika do bezpiecznego funkcjonowania w środowisku cyfrowym poprzez rozwinięcie wiedzy i umiejętności związanych z identyfikacją zagrożeń cybernetycznych, ochroną danych, bezpiecznym korzystaniem z narzędzi informatycznych oraz stosowaniem zasad cyberhigieny w codziennej pracy. Uczestnik po zakończeniu szkolenia potrafi rozpoznawać zagrożenia występujące w środowisku cyfrowym, właściwie reagować na próby ataków oraz stosować rozwiązania zwiększające poziom bezpieczeństwa

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

| Efekty uczenia się                                                                         | Kryteria weryfikacji                                                                                                                                              | Metoda walidacji        |
|--------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| Uczestnik identyfikuje podstawowe zagrożenia cyberbezpieczeństwa występujące w organizacji | rozdziela rodzaje cyberzagrożeń; wskazuje skutki ich wystąpienia dla organizacji; omawia najczęstsze metody działania cyberprzestępców                            | Wywiad swobodny         |
| Uczestnik rozpoznaje próby ataków socjotechnicznych                                        | identyfikuje cechy wiadomości phishingowych; rozdziela phishing, smishing i vishing; wskazuje właściwe działania po wykryciu próby oszustwa                       | Wywiad swobodny         |
| Uczestnik stosuje zasady bezpiecznego zarządzania dostępem do zasobów cyfrowych            | tworzy hasła zgodne z dobrymi praktykami; wyjaśnia zasady stosowania MFA; wskazuje narzędzia wspierające bezpieczne uwierzytelnianie                              | Wywiad swobodny         |
| Uczestnik stosuje zasady ochrony danych i informacji w środowisku prac                     | klasyfikuje informacje pod kątem poziomu poufności; wskazuje sposoby zabezpieczania danych; opisuje zasady bezpiecznego udostępniania informacji                  | Wywiad ustrukturyzowany |
| Uczestnik bezpiecznie korzysta z poczty elektronicznej, Internetu i usług chmurowych       | identyfikuje ryzyka związane z korzystaniem z usług online; wskazuje zasady bezpiecznej komunikacji elektronicznej; opisuje metody ograniczania zagrożeń          | Wywiad swobodny         |
| Uczestnik stosuje zasady cyberhigieny podczas pracy z urządzeniami służbowymi i prywatnymi | wskazuje znaczenie aktualizacji systemów; omawia zasady bezpiecznej pracy z urządzeniami mobilnymi; opisuje sposoby zabezpieczania nośników danych                | Wywiad swobodny         |
| Uczestnik organizuje bezpieczną pracę zdalną                                               | wskazuje zagrożenia związane z pracą poza siedzibą firmy; opisuje zasady korzystania z sieci Wi-Fi; dobiera rozwiązania zwiększające bezpieczeństwo pracy zdalnej | Wywiad swobodny         |

# Kwalifikacje

## Kompetencje

Usługa prowadzi do nabycia kompetencji.

### Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyrażnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyrażnie 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 wyrażnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

## Program

### Moduł I. Wprowadzenie do cyberbezpieczeństwa w organizacji

- aktualne zagrożenia cybernetyczne,
- cyberbezpieczeństwo jako element bezpieczeństwa organizacji,
- skutki incydentów bezpieczeństwa dla przedsiębiorstwa,
- odpowiedzialność pracownika za bezpieczeństwo informacji.

### Moduł II. Ataki socjotechniczne i manipulacja użytkownikiem

- phishing, spear phishing, smishing, vishing,
- wyłudzenie danych i podszywanie się pod instytucje,
- analiza przykładów rzeczywistych ataków,
- warsztaty identyfikacji zagrożeń.

### Moduł III. Bezpieczne uwierzytelnianie i zarządzanie dostępem

- polityka haseł,
- menedżery haseł,
- uwierzytelnianie wieloskładnikowe,
- kontrola dostępu do zasobów.

### Moduł IV. Ochrona danych i informacji

- rodzaje informacji w organizacji,
- bezpieczne przechowywanie danych,
- zasady udostępniania informacji,
- ochrona danych osobowych w codziennej pracy.

### Moduł V. Bezpieczeństwo poczty elektronicznej, Internetu i usług chmurowych

- zagrożenia związane z pocztą elektroniczną,
- bezpieczne korzystanie z Internetu,
- bezpieczeństwo pracy w chmurze,
- analiza przypadków naruszeń bezpieczeństwa.

**Moduł VI. Cyberhigiena i bezpieczeństwo urządzeń**

- aktualizacje systemów i aplikacji,
- złośliwe oprogramowanie,
- bezpieczeństwo urządzeń mobilnych,
- bezpieczne korzystanie z nośników danych.

**Moduł VII. Bezpieczna praca zdalna**

- organizacja bezpiecznego stanowiska pracy,
- bezpieczeństwo sieci bezprzewodowych,
- korzystanie z VPN,
- dobre praktyki pracy poza biurem.

**Walidacja**

- 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 skierowane do właściciela przedsiębiorstwa, który w ramach prowadzonej działalności gospodarczej korzysta z narzędzi teleinformatycznych, takich jak komputer, laptop, smartfon, poczta elektroniczna, systemy informatyczne oraz usługi internetowe i chmurowe. Uczestnik posiada dostęp do danych firmowych, dokumentacji elektronicznej oraz informacji dotyczących klientów, kontrahentów i procesów biznesowych, przez co odpowiada za bezpieczeństwo ich przetwarzania i ochronę przed zagrożeniami cybernetycznymi. Usługa jest przeznaczona dla osoby zarządzającej przedsiębiorstwem, która chce podnieść swoje kompetencje w zakresie ochrony danych, bezpiecznego korzystania z technologii cyfrowych, rozpoznawania cyberzagrożeń oraz wdrażania dobrych praktyk cyberbezpieczeństwa wspierających bezpieczne funkcjonowanie firmy w środowisku cyfrowym.
- 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 uczestnik otrzyma materiały merytoryczne w formie prezentacji. Materiały wysyłane są na adres mailowy uczestnika szkolenia.
- Usługa realizowana jest w godzinach zegarowych (1 godzina zegarowa = 60 minut).
- Przerwy i walidacja wliczone są w czas trwania szkolenia.

# Harmonogram

Liczba pozycji harmonogramu: 12

| Przedmiot / temat                                                               | Typ aktywności | Prowadzący   | Data realizacji zajęć | Godzina rozpoczęcia | Godzina zakończenia | Liczba godzin |
|---------------------------------------------------------------------------------|----------------|--------------|-----------------------|---------------------|---------------------|---------------|
| <div>1 z 12</div> Moduł I.<br>Wprowadzenie do cyberbezpieczeństwa w organizacji | Zajęcia        | Kamil Kamola | 20-08-2026            | 08:00               | 09:00               | 01:00         |
| <div>2 z 12</div> Moduł II. Ataki socjotechniczne i manipulacja użytkownikami   | Zajęcia        | Kamil Kamola | 20-08-2026            | 09:00               | 10:30               | 01:30         |

| Przedmiot / temat                                                                  | Typ aktywności | Prowadzący   | Data realizacji zajęć | Godzina rozpoczęcia | Godzina zakończenia | Liczba godzin |
|------------------------------------------------------------------------------------|----------------|--------------|-----------------------|---------------------|---------------------|---------------|
| 3 z 12 -                                                                           | Przerwa        | -            | 20-08-2026            | 10:30               | 11:00               | 00:30         |
| 4 z 12 Moduł III. Bezpieczne uwierzytelnianie i zarządzanie dostępem               | Zajęcia        | Kamil Kamola | 20-08-2026            | 11:00               | 13:00               | 02:00         |
| 5 z 12 -                                                                           | Przerwa        | -            | 20-08-2026            | 13:00               | 13:30               | 00:30         |
| 6 z 12 Moduł IV. Ochrona danych i informacji                                       | Zajęcia        | Kamil Kamola | 20-08-2026            | 13:30               | 15:00               | 01:30         |
| 7 z 12 Moduł V. Bezpieczeństwo poczty elektronicznej, Internetu i usług chmurowych | Zajęcia        | Kamil Kamola | 21-08-2026            | 08:00               | 10:00               | 02:00         |
| 8 z 12 -                                                                           | Przerwa        | -            | 21-08-2026            | 10:00               | 10:30               | 00:30         |
| 9 z 12 Moduł VI. Cyberhigiena i bezpieczeństwo urządzeń wo urzędzeń                | Zajęcia        | Kamil Kamola | 21-08-2026            | 10:30               | 13:00               | 02:30         |
| 10 z 12 -                                                                          | Przerwa        | -            | 21-08-2026            | 13:00               | 13:30               | 00:30         |
| 11 z 12 Moduł VII. Bezpieczna praca zdalna                                         | Zajęcia        | Kamil Kamola | 21-08-2026            | 13:30               | 15:30               | 02:00         |
| 12 z 12 -                                                                          | Walidacja      | -            | 21-08-2026            | 15:30               | 16:00               | 00:30         |

## Podsumowanie

| Rodzaj godzin                 | Liczba godzin |
|-------------------------------|---------------|
| Suma godzin zegarowych usługi | 15:00         |
| w tym suma godzin zajęć       | 12:30         |

| Rodzaj godzin                        | Liczba godzin |
|--------------------------------------|---------------|
| w tym suma godzin walidacji          | 00:30         |
| w tym suma przerw                    | 02:00         |
| Suma godzin dydaktycznych bez przerw | 17:15         |

## Cennik

Jeżeli korzystasz z dofinansowania i usługa stanowi usługę kształcenia zawodowego lub przekwalifikowania zawodowego wraz z usługą lub dostawą towarów ściśle związaną z usługami kształcenia zawodowego lub przekwalifikowania zawodowego to możesz mieć możliwość skorzystania ze zwolnienia z podatku VAT na podstawie art. 43 ust. 1 pkt 29 lit. c ustawy z dnia 11 marca 2024 r. o podatku od towarów i usług, jeśli usługa w całości jest finansowana ze środków publicznych lub § 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, gdy usługa jest finansowana w co najmniej 70% ze środków publicznych.

### Cennik

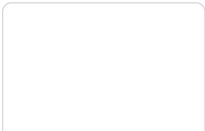
| Rodzaj ceny                               | Cena         |
|-------------------------------------------|--------------|
| Koszt przypadający na 1 uczestnika brutto | 4 280,40 PLN |
| Koszt przypadający na 1 uczestnika netto  | 3 480,00 PLN |
| Koszt osobogodziny brutto                 | 285,36 PLN   |
| Koszt osobogodziny netto                  | 232,00 PLN   |

### Liczba godzin usługi

| Rodzaj godzin                   | Liczba godzin |
|---------------------------------|---------------|
| Liczba godzin zegarowych usługi | 15:00         |

## 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 uczestnik otrzyma materiały merytoryczne w formie prezentacji. Materiały wysyłane są na adres mailowy uczestnika szkolenia.

### Warunki uczestnictwa

Szkolenie skierowane do właściciela przedsiębiorstwa, który w ramach prowadzonej działalności gospodarczej korzysta z narzędzi teleinformatycznych, takich jak komputer, laptop, smartfon, poczta elektroniczna, systemy informatyczne oraz usługi internetowe i chmurowe. Uczestnik posiada dostęp do danych firmowych, dokumentacji elektronicznej oraz informacji dotyczących klientów, kontrahentów i procesów biznesowych, przez co odpowiada za bezpieczeństwo ich przetwarzania i ochronę przed zagrożeniami cybernetycznymi.

Usługa jest przeznaczona dla osoby zarządzającej przedsiębiorstwem, która chce podnieść swoje kompetencje w zakresie ochrony danych, bezpiecznego korzystania z technologii cyfrowych, rozpoznawania cyberzagrożeń oraz wdrażania dobrych praktyk cyberbezpieczeństwa wspierających bezpieczne funkcjonowanie firmy w środowisku cyfrowym.

### Informacje dodatkowe

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

## Adres

ul. Dęblińska 18  
24-100 Puławy  
woj. lubelskie

Szkolenie odbędzie się w siedzibie firmy K2 Group sp. z o.o. w sali konferencyjnej.

## Kontakt



**ANDŻELIKA IWANICZ**

**E-mail** [a.iwanicz@k2g.com.pl](mailto:a.iwanicz@k2g.com.pl)

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

