Bezpieczeństwo systemów i sieci komputerowych.

Czas trwania: 13 godzin/2 dni
Miejsce: szkolenie on-line lub forma stacjonarna w siedzibie klienta lub organizatora ul. Ks. Bp. W. Tymienieckiego 22G, parter budynku, sala K2.
Cena: 1200 zł netto/osoba

Uczestnicy szkolenia otrzymają materiały merytoryczne oraz certyfikat uczestnictwa w szkoleniu.

O szkoleniu

Celem szkolenia jest przekazanie wiedzy z zakresu projektowania, wdrażania i utrzymania systemów i sieci komputerowych ze szczególnym naciskiem na aspekty związane z bezpieczeństwem przechowywania, przesyłania i przetwarzania danych. Uczestnicy szkolenia nabędą także wiedzę dotyczącą projektowania i zarządzania systemami oraz sieciami komputerowymi.

Program szkolenia

Bezpieczeństwo informacji:

- ✓ Bezpieczeństwo informacji w organizacji.
- ✓ Prawne aspekty związane z bezpieczeństwem informacji, np. wymagania RODO, aktualne akty prawne.
- ✓ Tworzenie kultury ochrony informacji.

Zagrożenia bezpieczeństwa informacji:

- ✓ Cyberzagrożenia - przykłady kradzieży i wycieku danych.
- ✓ Zagrożenia przy korzystaniu z internetu: poczta e-mail, strony www, serwisy społecznościowe.

Bezpieczne hasło:

- ✓ Weryfikacja haseł do systemów informatycznych.
- ✓ Tworzenie silnego hasła.
- ✓ Ochrona haseł.

Ataki hackerskie / socjotechniczne:

- ✓ Podejrzane e-maile, czyli przykłady realnych zagrożeń np. ransomware.
- ✓ Czy pendrive od znajomego może być niebezpieczny?
- ✓ Skuteczne metody ochrony przed atakami.

Polityka bezpieczeństwa:

- ✓ Polityka Bezpieczeństwa Informacji jako skuteczne narzędzie ochrony informacji.
- ✓ Skuteczne procedury ochrony danych.

Harmonogram dzień 1

L.p.	**Przedmiot/Temat zajęć**	**Godzina rozpoczęcia**	**Godzina zakończenia**	**Liczba godzin**
1.	**Bezpieczeństwo informacji** • Bezpieczeństwo informacji w organizacji. • Prawne aspekty związane z bezpieczeństwem informacji, np. wymagania RODO, aktualne akty prawne. • Tworzenie kultury ochrony informacji.	08:00	10:00	2:00
2.	**Przerwa**	10:15	10:30	0:15
3.	**Zagrożenia bezpieczeństwa informacji** • Cyberzagrożenia. • Przykłady kradzieży i wycieku danych. • Zagrożenia przy korzystaniu z internetu: poczta e-mail, strony www, serwisy społecznościowe.	10:30	12:00	1:30
4.	**Przerwa**	12:00	12:30	0:30
5.	**Bezpieczne hasło** • Weryfikacja haseł do systemów informatycznych. • Tworzenie silnego hasła. • Ochrona haseł.	12:30	14:30	2:00

Harmonogram dzień 2

L.p.	**Przedmiot/Temat zajęć**	**Godzina rozpoczęcia**	**Godzina zakończenia**	**Liczba godzin**
1.	**Ataki hakerskie/socjotechniczne:** • Podejrzane e-maile, czyli przykłady czyli przykłady realnych zagrożeń np. ransomware. • Czy pendrive od znajomego może być niebezpieczny?	8:00	10:00	2:00
2.	**Przerwa**	10:15	10:30	0:15
3.	**Skuteczne metody ochrony przed atakami.**	10:30	12:00	1:30
4.	**Przerwa**	12:00	12:30	0:30
5.	**Polityka bezpieczeństwa** • Polityka bezpieczeństwa Informacji jako skuteczne narzędzie ochrony informacji. • Skuteczne procedury ochrony danych	12:30	14:30	2:00

Efekty szkolenia

Uczestnik nabędzie umiejętność samokształcenia się w zakresie cyberbezpieczeństwa i jego kluczowych pojęć, zagrożeń, ataków, regulacji i technik cyberobrony. Wzrost kompetencji kadry w obszarze zagrożeń bezpieczeństwa informacji/cyberbezpieczeństwa – podniesienie poziomu bezpieczeństwa w instytucji. Przygotowanie do wdrażania skutecznych rozwiązań organizacyjnych i zachowań podnoszących cyberbezpieczeństwo w urzędzie/instytucji. Uczestnik rozumie znaczenie bezpieczeństwa podczas korzystania z internetu oraz potrafi prawidłowo identyfikować i rozstrzygać dylematy związane z siecią.

Dla kogo?

Szkolenie skierowane do osób na co dzień wykorzystujących systemy informatyczne w organizacji, osób odpowiedzialnych za bezpieczeństwo systemów, w tym przygotowanie dokumentów i wytycznych dla pracowników dotyczących cyberbezpieczeństwa.