TYTUŁ SZKOLENIA:
„PODSTAWY CYBERBEZPIECZEŃSTWA W TWOJEJ FIRMIE”

GRUPA DOCELOWA USŁUG
Firmy MSP, które chcą poznać aktualne cyberzagrożenia oraz skuteczne metody ochrony danych w swojej organizacji;
Kierownicy, grupy pracownicze, komórki organizacyjne, zespoły projektowe oraz pracownicy organizacji.

PROGRAM USŁUGI

CZĘŚĆ I – PODSTAWY CYBERBEZPIECZEŃSTWA W FIRMIE

- Cyberbezpieczeństwo w firmie – założenia skutecznego wdrożenia
- Prawne aspekty związane z cyberbezpieczeństwem
- Budowanie świadomości dotyczącej cyberzagrożeń wśród pracowników
- Bezpieczna praca zdalna
- Pytania/Odpowiedzi

CZĘŚĆ II – CYBERZAGROŻENIA
- Przykłady kradzieży i wycieku danych z firm i instytucji
- Zagrożenia przy korzystaniu z Internetu: poczta e-mail, strony www, serwisy społecznościowe
- Dezinformacja i fakenewsy
- Czy pendrive od znajomego może być niebezpieczny?
- Pytania/Odpowiedzi

CZĘŚĆ III – TWOJE HASŁO DO SYSTEMÓW
- Czy Twoje hasło do systemów jest bezpieczne?
- Jak stworzyć silne hasło i łatwo je zapamiętać?
- Czy należy często zmieniać hasło?
- Jak bezpiecznie chronić hasła?
- Używanie menedżera haseł
- Podwójne uwierzytelnienie (2FA) jako skuteczny sposób zabezpieczenia konta w systemie
- Pytania/Odpowiedzi

CZĘŚĆ IV – ATAKI HACKERSKIE I SOCJOTECHNICZNE

- Przykłady ataków hackerskich i socjotechnicznych wykorzystujących np. spoofing i phishing
- Ransomware jako największe zagrożenie
- Podejrzane e-maile i smsy - jak je odróżnić w codziennej pracy
- Jak się chronić przed phishingiem i ransomware?
- Pytania/Odpowiedzi

CEL EDUKACYJNY

Celem szkolenia jest podniesienie kompetencji uczestników w zakresie ochrony informacji gromadzonych i przetwarzanych w firmie, wiedzy o aktualnych cyberzagrożeniach oraz stosowania aktualnych obowiązków wynikających np. z RODO. Uczestnicy zdobędą wiedzę niezbędną do skutecznej ochrony informacji i bezpiecznego ich przetwarzania w firmie oraz nabędą umiejętności pozwalające im przeciwstawić się podstawowym próbom cyberataków (phishing, ransomware).

W trakcie szkolenia uczestnicy zapoznają się także - na licznych przykładach - z podstawowymi zasadami tzw. cyberhigieny.

Szkolenie oprócz wykładu jest prowadzone także w formie warsztatowej z licznymi case studies, co przyczyni się pośrednio także do rozwinięcia kompetencji społecznych w zakresie komunikacji poprzez wspólną analizę przypadków, współpracę w grupie.

EFEKTY UCZENIA

Uczestnik po zakończonym szkoleniu:

- posiada praktyczną wiedzę dotyczącą aktualnych cyberzagrożeń;
- ma świadomość wartości i znaczenia posiadanych informacji przez firmę oraz jej pracowników oraz konsekwencji wystąpienia incydentów bezpieczeństwa;
- zna podstawowe, skuteczne metody zabezpieczania dokumentacji i systemów informatycznych;
- zna metody poprawy cyberbezpieczeństwa poprzez wprowadzenie lub udoskonalenie standardów ochrony informacji.

CZAS TRWANIA SZKOLENIA

1 dzień / 6-8 godzin

ZAJĘCIA POPROWADZĄ

Arkadiusz Stawczyk
Bezpieczeństwo informacji i cyberbezpieczeństwo

Specjalista w dziedzinie bezpieczeństwa informacji.
Audytor Wiodący ISO/IEC 27001:2017. Kierownik i koordynator projektów (certyfikat zarządzania projektami: TenStep Fn-TSPM).
Specjalista IT Security – CISS (Certified IT Security Specialist). Trener i egzaminator ECDL.
Członek Polskiego Towarzystwa Informatycznego (PTI)
Prowadzi szkolenia oraz consulting w obszarach ICT w biznesie i administracji. Ma za sobą również kilkuletnie doświadczenie wykładowcy wyższej uczelni.
Absolwent Wyższej Szkoły Inżynierskiej w Zielonej Górze, kierunek matematyka.
Poprzednio kierownik Wydziału Informatyki w dużej jednostce administracji samorządowej. Był odpowiedzialny za kluczowe projekty informatyczne realizowane w urzędzie oraz skuteczne wdrażanie Polityki Bezpieczeństwa Informacji.