SZCZEGÓŁY OFERTY

CYBERBEZPIECZEŃSTWO W BANKU SPÓŁDZIELCZYM – RODO, wymiana danych z dostawcami, szyfrowanie danych, bezpieczeństwo płatności internetowych, bankowość elektroniczna, media społecznościowe, dezinformacja i ochrona poczty elektronicznej

---

Program szkolenia

1. Skuteczna i efektywna ochrona Danych Osobowych:
 Definicja danych osobowych (RODO – art. 4)
 Dane zwykłe vs. dane sensytywne
 Dane finansowe, transakcyjne, behawioralne
 Dane klientów, pracowników, kontrahentów
 Dane objęte tajemnicą bankową
 Metadane, logi systemowe jako dane osobowe
 Błędy klasyfikacyjne i ich konsekwencje
2. Praktyczne zasady działania – Bank, Administracja, Podmioty zewnętrzne:
 Zasady RODO (art. 5)
 Role: administrator, procesor, osoba upoważniona
 Minimalizacja danych w praktyce bankowej
 Rozliczalność i dokumentowanie działań
 Zgody vs. obowiązek prawny
 Wymiana danych z organami publicznymi
 Obowiązki informacyjne

3. Bezpieczne przetwarzanie Danych Osobowych:
 Bezpieczeństwo danych w cyklu życia informacji
 Dostęp do danych a zasada „need to know”
 Uprawnienia, role, autoryzacja
 Praca zdalna i hybrydowa
 Urządzenia prywatne (BYOD)
 Czyste biurko, czysty ekran
 Bezpieczna archiwizacja
 Reagowanie na incydent
4. Szyfrowanie danych osobowych, kanałów komunikacji:
 Szyfrowanie danych „w spoczynku” i „w transmisji”
 Szyfrowanie poczty elektronicznej
 Szyfrowanie dokumentów i nośników danych
 Hasła, klucze kryptograficzne, MFA
 Bezpieczne hasła i menedżery haseł
5. Bezpieczne płatności internetowe:
 Mechanizmy płatności online
 Zagrożenia: phishing, vishing, smishing
 Fałszywe bramki płatnicze

 Malware bankowy
 Przejęcie konta klienta
 Ataki „na BLIK”

6. BEZPIECZNA BANKOWOŚĆ ELEKTRONICZNA:
 Zagrożenia dla systemów bankowości elektronicznej
 Ataki na użytkowników końcowych
 Inżynieria społeczna
 Przejęcie sesji, keyloggery
 MFA
 Monitoring zachowań
 Reakcja na incydent
7. Internet, media społecznościowe:
 Social media jako źródło zagrożeń
 OSINT i profilowanie pracowników
 Fałszywe profile, spear phishing
 Wycieki informacji niejawnych i wewnętrznych
 Zasady publikowania treści
 Prywatność kont
 Separacja życia zawodowego i prywatnego
8. Informacja, dezinformacja, fake news:
 Czym jest dezinformacja?
 Wpływ fake news na sektor finansowy
 Manipulacja informacją
 Deepfake i AI w dezinformacji
 Weryfikacja źródeł
 Reagowanie na fałszywe informacje
9. Bezpieczna poczta elektroniczna:
 Phishing, spear phishing, whaling
 Załączniki i linki
 Spoofing domen
 BEC (Business Email Compromise)
 Jak zgłaszać podejrzane wiadomości?
 Reakcja na kliknięcie w złośliwy link

Warunki uczestnictwa i regulamin

> Warunki uczestnictwa
>
> po otrzymaniu zgłoszenia prześlemy potwierdzenie przyjęcia zgłoszenia, a na około 2 dni przed terminem szkolenia zostaną wysłane wiadomości organizacyjne wraz z linkiem do szkolenia oraz materiałami szkoleniowymi. Płatności po szkoleniu, zwykle w tym samym dniu po szkoleniu prześlemy do Państwa faktury do zapłaty wraz z zaświadczeniem drogą mailową.

> Regulamin
>
> rezygnację przyjmujemy najpóźniej na 3 dni przed szkoleniem w formie pisemnej. Rezygnacja w późniejszym terminie wiąże się z koniecznością pokrycia kosztów w 100%. Nieobecność na szkoleniu nie zwalnia z dokonania opłaty. W przypadku braku możliwości wzięcia udziału w danym terminie jest możliwość przesłania nagrania ze szkolenia online.

Promocja

390 + VAT
za każdą kolejną osobę z firmy

490 + VAT | za osobę

NADCHODZĄCE TERMINY