AKADEMIA B&B

PODSTAWY CYBERBEZPIECZEŃSTWA I BEZPIECZEŃSTWA INFORMACJI W ADMINISTRACJI PUBLICZNEJ

Procedury, wytyczne, instrukcje, odpowiedni sprzęt i technologiczne zabezpieczenia to czasem za mało – podczas 95% cyberataków zawodzi po prostu czynnik ludzki.

Dlatego tak ważna jest edukacja i uświadamianie!

Cel szkolenia?

Szkolenie ma na celu podniesienie świadomości zagrożeń, konsekwencji zaistnienia incydentów związanych z naruszeniem bezpieczeństwa informacji, wynikających z niestosowania się do ustalonych norm wewnętrznych i braku świadomości zasad funkcjonujących w organizacji. Najsłabszym ogniwem jest pracownik. Konieczna jest zatem systemowa edukacja i procedury. Zaawansowana technologia i najlepsze systemy zabezpieczeń nie zapewnią kompletnej ochrony, jeśli pracownicy nie znają podstaw cyberbezpieczeństwa, ani umiejętności przeciwdziałania im w cyfrowym świecie

W czasie szkoleń poruszamy realne problemy, z którymi styka się użytkownik, a każdy aspekt jest szeroko poparty przykładami. Omawiamy zagadnienia technologii i Internetu, socjotechnikę oraz zwracamy uwagę na monitorowanie otoczenia i jak być odpornym na fake newsy. Przekazanie w jasny sposób wiedzy teoretycznej i licznych przykładów zagrożeń spowoduje pobudzenie wyobraźni, a co za tym idzie zwiększy czujność i ostrożność.

Skierowane jest do wszystkich pracowników nietechnicznych sektora publicznego.

Jak szkolimy?

Szkolenie realizowane jest w formie mini wykładu. Łączy w sobie wiedzę merytoryczną z praktycznymi przykładami jej wykorzystania w środowisku pracy.

Pozwalamy naszym klientom mieć realny wpływ na kształt i merytoryczną zawartość szkolenia. Na wstępie przeprowadzimy badania ankietowe online z wiedzy o podstawowych aspektach cyberbezpieczeństwa i stosowanych procedurach IT. Wyniki ankietyzacji uwypuklą obszary, na których się skupimy i które omówimy w trakcie szkolenia

Informacje ogólne

Szkolenia mogą być prowadzone w formule otwartej i zamkniętej.

Szkolenie będzie prowadzone w języku polskim.

Szkolenia trwają ok. 4 h.

W przypadku szkoleń trwających do 3 godzin, przewiduje się jedną przerwę trwającą 15 minut. W przypadku szkoleń trwających powyżej 3 godzin, organizowane będą dwie przerwy trwające 15 minut każda.

Dysponujemy potencjałem dydaktycznym i rozbudowanym zapleczem technicznym – mobilna pracownia komputerowa oraz sprzęt komputerowy dla prowadzących umożliwiający przeprowadzenie szkolenia wraz ekran i projektorem.

Mogą się odbywać stacjonarnie, na zamówienie Klienta, w miejscu przez niego wyznaczonym lub w naszej Siedzibie. Szkolenie przeprowadzone powinno być w grupach liczących do 25 pracowników.

Jesteśmy ponadto otwarci i przygotowani na realizację szkolenia w formie online. Liczba uczestników do ustalenia.

Niezależnie od formy, zobowiązujemy się do prowadzenia dokumentacji wszystkich szkoleń w jednakowy sposób – na dokumentację szkolenia składają się:

- lista obecności uczestników szkolenia (w przypadku szkolenia online – raport uczestnictwa i raport końcowy po spotkaniu),
- ankiety satysfakcji sporządzone po każdym szkoleniu wraz z raportem.

Kto prowadzi szkolenia?

Szkolenia prowadzone są przez praktyków, którzy na co dzień mają styczność z szeroko rozumianym bezpieczeństwem informacji i bezpieczeństwem w cyberprzestrzeni. Dostarczają rzetelną wiedzę, która daje uczestnikom przewagę w szybko zmieniającym się świecie cyberbezpieczeństwa i sprawnie wykorzystują swoje doświadczenie zebrane podczas spotkań z pracownikami wszystkich szczebli w administracji publicznej i sektora prywatnego.

KATARZYNA GLIB

Inspektor Ochrony Danych, Certyfikowany Audytor Wiodący normy ISO 27001, szkoleniowiec
Odpowiedzialna za tworzenie i wdrażanie Systemów Zarządzania Bezpieczeństwem Informacji, z uwzględnieniem zasad ochrony danych osobowych oraz audytowanie w/w obszarów w podmiotach publicznych i prywatnych. Wykonuje opracowania z zakresu bezpieczeństwa informacji, badania zgodności z normami, przepisami prawa i ładu korporacyjnego.
Realizuje audyty z zakresu ochrony danych osobowych, bezpieczeństwa informacji oraz KRI, KSC.

ADRIAN KAMIZELA

Certyfikowany Audytor Wiodący normy ISO 27001, szkoleniowiec
Wyspecjalizowany w zakresie szeroko pojętej technologii IT, w tym sieci komputerowych i bezpieczeństwa systemów komputerowych oraz komputerowych systemach zarządzania i sterowania. Realizuje audyty bezpieczeństwa danych w systemach informatycznych i sieci ICT oraz KRI i KSC. Bierze pod lupę aspekty techniczne analizując oprogramowanie, serwisy WWW i pocztowe. Weryfikuje wszelkie ustanowione zabezpieczenia informacji przed nieuprawnionym dostępem.

Trenerzy pracujący w Akademii BB są pasjonatami symulacji biznesowych jako narzędzi do praktycznej nauki oraz angażowania uczestników szkoleń, dzięki którym zdobywają oni wyłącznie umiejętności przydatne w życiu, tym zawodowym, jak i prywatnym. Posiadają wszechstronną wiedzę, wielokierunkowe wykształcenie, praktyczne doświadczenie. Kładą nacisk na praktyczne podejście dostosowując je do aktualnej grupy odbiorców jego szkoleń.
Trenerzy w pełni odpowiadają za zawartość merytoryczną szkoleń, ich zakres i dobór materiałów.

Agenda szkolenia**:

1	Główne założenia i wymagania prawne związane z bezpieczeństwem informacji w Urzędzie
2	System Zarządzania Bezpieczeństwem Informacji (SZBI). Polityka bezpieczeństwa w organizacji.
3	Bezpieczeństwo fizyczne i środowiskowe. Zasady czystości w bezpieczeństwie danych i informacji.
4	Zabezpieczenie informatycznych nośników danych.
5	Zdalny dostęp do zasobów jednostki, korzystanie z urządzeń prywatnych przez pracowników oraz związane z tym potencjalne zagrożenia.
6	Zasady korzystania ze służbowego sprzętu do celów prywatnych
7	Czym jest incydent bezpieczeństwa i jak na niego reagować?
8	Czym jest cyberbezpieczeństwa i dlaczego jest istotne?
9	Wyjaśnienie podstawowych pojęć związanych z cyberbezpieczeństwem tj. https, AES-256, IP, TCP, UDP, DOMENA, URL, komunikator i inne.
10	Ataki sieciowe i komputerowe. Omówienie zagrożeń takich jak phishing, ransomware, malware, socjotechnika, atak telefoniczny, spoofing,
11	Bezpiecznie przetwarzanie danych: szyfrowanie, przechowywanie, udostępnianie, komunikacja
12	Metody nieautoryzowanego pozyskania danych + przykłady
13	Zasady korzystania z poczty elektronicznej.
14	Bezpieczeństwo podczas korzystania z przeglądarek internetowych.
15	Bezpieczne korzystanie z mediów społecznościowych
16	Bezpieczeństwo zakupów oraz płatności w Internecie.
17	Bezpieczeństwo danych w chmurze.

18	Prywatność w sieci czyli: trackery, ciastka, tryb incognito.
19	Bezpieczne hasła, menedżer haseł, autoryzacja dwuetapowa, klucze sprzętowe
20	Fake news – identyfikacja i walka z fałszywymi wiadomościami.

**

Zakres szkolenia może być dowolnie konfigurowany w zależności od rodzaju działalności i procesów w niej zachodzących.

Co po szkoleniu?

Szkolenie zakończone testem zdobytej wiedzy – test przeprowadzony z wykorzystaniem urządzeń mobilnych (każdy uczestnik szkolenia otrzyma link).

Uczestnik szkolenia otrzyma pakiet materiałów szkoleniowych w formie elektronicznej.

Szkolenie jest certyfikowane. Uczestnik po zakończeniu szkolenia otrzyma zaświadczenie ukończenia szkolenia. W przypadku przeszkolenia wszystkich pracowników, certyfikat uzyska dana Instytucja.

Jesteś zainteresowany ofertą?

Jeśli masz dodatkowe pytania lub chcesz zapoznać się z naszą ofertą zapraszamy do kontaktu z opiekunami handlowymi.