Cyberbezpieczeństwo w firmach i instytucjach JST

Data i miejsce szkolenia: 1 października 2024r., godz. 9:00 – 13:00, webinarium.

Prowadzący: Gabriela Rychły - Szkolenie prowadzone jest przez doświadczonego praktyka – czynny IOD, audytor ISO 27001, mediator sądowy, ekspert w dziedzinie bezpieczeństwa informacji, wykładowca RODO w Akademia Humanitas , ekspert Infor w zakresie ochrony danych osobowych, wieloletni praktyk, oraz prelegent na licznych seminariach (w tym w debatach z udziałem UODO), szkoleniach otwartych i zamkniętych z zakresu ochrony danych osobowych i bezpieczeństwa informacji. Konsultant wiodących kancelarii prawnych, specjalista z zakresu ochrony danych osobowych świadczący usługi kompleksowej obsługi prawnej podmiotów gospodarczych, jak i jednostek sektora administracji publicznej, trener z wieloletnim doświadczeniem, które przekłada się na umiejętność przystępnego przekazywania i wyjaśniania skomplikowanych zagadnień. W ramach obsługi firm opracowuje oraz wdraża systemy ochrony danych osobowych w różnych podmiotach. Jest cenionym konsultantem ds. ochrony danych osobowych w uczelniach, jednostkach administracji placówkach oświatowych i medycznych. Posiada wieloletnie doświadczenie w zakresie wdrażania polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym oraz systemów zarządzania bezpieczeństwem informacji.

Szkolenie z zakresu cyberbezpieczeństwa dla pracowników firm i instytucji, to wiedza, jak chronić najważniejsze zasoby na komputerach służbowych, świadomość skali zagrożeń związanych z cyberprzestrzenią oraz umiejętności m.in. wdrażania dobrych praktyki ochrony informacji. Pracownicy po przejściu szkolenia poznają zagrożenia płynące ze złośliwego oprogramowania. Dowiedzą się, jak bezpiecznie korzystać z poczty elektronicznej. Nauczą się chronić przed spamem. Poznają zasady bezpiecznego korzystania ze sprzętu elektronicznego. Dowiedzą się, jak bezpiecznie tworzyć i przechowywać hasła. Nauczą się chronić przed phishingiem oraz dowiedzą się jak bezpiecznego korzystać z mediów społecznościowych.

Odbiorcy szkolenia:

Właściciele małej i średniej firmy, pracownicy JST, pracownicy takich działów jak marketing, sprzedaż, księgowość, HR, wszystkie osoby które chcą zwiększyć swoją wiedzę i świadomość jak chronić firmę, urząd swoje miejsce pracy oraz swoje prywatne zasoby przed atakami, czym jest cyberbezpieczeństwo , jak nie narazić się na straty wizerunkowe i finansowe.

Co zyskujesz, szkoląc pracowników lub siebie z cyberbezpieczeństwa?

Przede wszystkim wiedzę i świadomość - pamiętaj o tym że system bezpieczeństwa firmy jest tak mocny, jak świadomy zagrożeń jest pracownik.

Uczestnicy szkolenia dowiedzą się:

- jak rozpoznać fałszywe maile – phishing – pokazane i omówione przykłady
- jak zapobiec oszustwom
- jak bezpiecznie korzystać z portali społecznościowych, co chroni zarówno ich prywatne dane, jak i dane firmy.
- jak wygląda bezpieczna praca w hybrydzie
- jak sprawdzić, czy ich dane wyciekły, co pozwoli na szybką reakcję i ochronę poufnych informacji.
- jak bezpiecznie pracować zdalnie, aby nie narażać firmy i klientów na wyciek danych.

Poznają najnowsze metody ataków i jak się przed nimi bronić

Uczestnicy po szkoleniu będą świadomi popularnych metod ataków cyberprzestępców z wykorzystaniem AI, co pozwoli im lepiej chronić firmę przed nowymi zagrożeniami

Udział w szkoleniu to również spełnienie norm i obowiązków

- Biorąc udział w szkoleniu spełnisz obowiązki wynikające z przepisów, w tym KSC, RODO i Krajowych Ram Interoperacyjności.
- Przygotujesz się do spełnienia wymagań dla certyfikatu ISO 27001.

Program szkolenia:

1. **Czym jest cyberbezpieczeństwo.**
2. **Obowiązki JST w zakresie cyberbezpieczeństwa.**
3. **Wymagania dla pracowników wynikające z KRI, ustawy o KSC oraz RODO.**
4. **Rodzaje cyberzagrożeń m.in.:**
   - 4.1. Złośliwe oprogramowania (malware);
   - 4.2. Ataki z wykorzystaniem złośliwego kodu na stronach internetowych;
   - 4.3. Phishing, czyli bezpośrednie wyłudzanie poufnych informacji lub za pomocą złośliwego oprogramowania;
   - 4.4. Ataki na aplikacje internetowe;
   - 4.5. SPAM – niechciana korespondencja;
   - 4.6. Ataki DDoS – czyli blokowanie dostępu do usług poprzez sztuczne generowanie wzmożonego ruchu;
   - 4.7. Kradzież tożsamości;
   - 4.8. Naruszenie poufności, integralności lub dostępności danych;
   - 4.9. Zagrożenia wewnętrzne powodowane przez pracowników;
   - 4.10. Wyciek danych;

4.11. Ataki ransomware w celu wyłudzenia okupu za odszyfrowanie lub nieujawnianie wykradzionych danych.

5. **W skrócie czym jest:**
   5.1. Inwentaryzacja zasobów informatycznych;
   5.2. Audyt bezpieczeństwa;
   5.3. Skanowanie podatności;
   5.4. Zapobieganie utracie informacji (kopie zapasowe, system DLP);
   5.5. Zabezpieczenie sieci;
   5.6. Oprogramowanie antywirusowe;
   5.7. Szyfrowanie danych;
   5.8. Wykrywanie i zapobieganie włamaniom do zasobów informatycznych.
6. **Jak rozpoznać cyberzagrożenia.**
7. **Jak zachować się bezpiecznie online.**
8. **Jak pandemia, cyfryzacja oraz praca zdalna wpłynęły na bezpieczeństwo organizacji.**
9. **Zarządzanie uprawnieniami użytkowników do systemów informatycznych.**
10. **Dobre praktyki cyberbezpieczeństwa w samorządach.**
11. **Jak bezpiecznie korzystać z internetu.**
12. **Przykłady ataków cyberprzestępców.**

Informacje organizacyjne:

- szkolenie będzie zorganizowane jako webinarium **w formule online** na platformie ClickMeeting. Aby wziąć udział w szkoleniu wystarczy korzystać z komputera (smartfona) z dostępem do internetu oraz z aktualną przeglądarką internetową;
- dzień przed szkoleniem otrzymają Państwo od nas emaila wysłanego z platformy ClickMeeting z niezbędnymi informacjami do zalogowania się na platformę szkoleniową oraz linkami do materiałów szkoleniowych;
- w trakcie szkolenia można na czacie zadawać pytania prowadzącemu, obsługa jest łatwa (intuicyjna).

Cena szkolenia: 390 zł + 23% VAT. Cena obejmuje: dostęp do platformy e-lernigowej w czasie rzeczywistym, autorskie materiały szkoleniowe, certyfikat uczestnictwa w szkoleniu dla każdego uczestnika.
(Faktury „zw" dla sektora finansów publicznych po przesłaniu oświadczenia o zwolnieniu z VAT)
Zgłoszenia można dokonać poprzez stronę internetową www.totalexpert.pl ewentualnie wysyłając kartę zgłoszenia na adres: **biuro@totalexpert.pl**

KARTA ZGŁOSZENIA

Prosimy o odesłanie mailem na adres: biuro@totalexpert.pl

PRZEDMIOT ZGŁOSZENIA					
Nazwa szkolenia/kursu:	***Cyberbezpieczeństwo w firmach i instytucjach JST***				
Termin szkolenia:	**1.10.2024r.**	**Miasto szkolenia:**	**Online**	**Cena:**	

DANE UCZESTNIKA SZKOLENIA		
Imię i nazwisko uczestników, stanowisko	**Kontakt do uczestnika**	
	Telefon	**Adres email**
1.		
2.		
3.		
4.		

DANE FIRMY DO FAKTURY (NABYWCA)			
Nazwa:			
Adres (ulica i miasto):			
NIP:		**UWAGI (ODBIORCA):**	
☐ **Wysłanie faktury pocztą tradycyjną**		☐ **Wysłanie faktury mailem na adres:**	

OSOBA ZGŁASZAJĄCA			
Imię i nazwisko;		**Pełniona funkcja:**	
E-mail:		**Telefon kontaktowy:**	

Warunki uczestnictwa:

Wypełniona karta zgłoszenia jest warunkiem uczestnictwa w szkoleniu i podstawą do wystawienia faktury VAT za szkolenie bez podpisu odbiorcy. Faktury wysyłamy pocztą email lub na życzenie pocztą tradycyjną, płatność do 14 dni po szkoleniu.

Oświadczenie dla finansujących szkolenie ze środków publicznych:

Niniejszym oświadczamy, że nabyta w/w usługa szkoleniowa w zakresie kształcenia zawodowego jest finansowana:

- ☐ w całości ze środków publicznych (art. 43 ust. 1 pkt 29c ustawy z dn. 11.03.2004r. o podatku od towarów i usług Dz. U. 2011 nr 177, poz. 1054 z późn. zm.)
- ☐ w co najmniej 70% ze środków publicznych (§ 3 ust. 1 pkt 14 Rozp. MF z dn. 20.12.2013r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień - Dz. U. 2013, poz. 1722)

Warunki rezygnacji:

Rezygnacja musi nastąpić w formie pisemnej najpóźniej na 2 dni przed rozpoczęciem szkolenia. Rezygnacja w terminie późniejszym lub niezgłoszenie się na szkolenie/kurs nie zwalnia od dokonania opłaty w pełnej wysokości.

Zgody:

☐ *Wyrażam zgodę na przetwarzanie moich danych osobowych przez Total Expert Jan Howaniec ul. Wysoka 5, 41-209 Sosnowiec w zakresie prowadzonej przez nią działalności gospodarczej na podstawie Ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. (RODO). Wiem, że mam pełne prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;

☐ Wyrażam zgodę na otrzymywanie informacji handlowych od Total Expert Jan Howaniec ul. Wysoka 5, 41-209 Sosnowiec na podany adres e-mail-na podstawie Ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. (RODO). W każdym momencie przysługuje mi prawo do odwołania powyższej zgody.

Informujemy, że administratorem danych osobowych, w rozumieniu przepisów Ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. (RODO) jest Total Expert Jan Howaniec ul. Wysoka 5, 41-209 Sosnowiec. Pani/Pana dane nie będą przetwarzane w sposób zautomatyzowany w tym również w formie profilowania.

Przesłanie karty zgłoszenia stanowi potwierdzenie przyjęcia oferty oraz potwierdzenie zapoznania się z regulaminem świadczenia usług szkoleniowych.

	.....	.....
Pieczątka firmowa	**Miejscowość, data**	**Podpis osoby upoważnionej**