Webinar: Cyberbezpieczeństwo w praktyce - jak chronić firmę i pracowników przed cyberzagrożeniami?

Bezpieczna praca z narzędziami cyfrowymi i AI z zachowaniem cyberhigieny pracownika - codzienne dobre praktyki.

21 stycznia 2027 r. - Online

Wprowadzenie do cyberbezpieczeństwa firmy:
- Czym jest cyberbezpieczeństwo i dlaczego dotyczy każdego pracownika?
- Jakie zasoby firmy wymagają ochrony: dane, dokumenty, systemy, urządzenia i komunikacja?
- Najczęstsze zagrożenia cybernetyczne dla przedsiębiorstw.
- Rola pracownika w systemie bezpieczeństwa organizacji.
- Konsekwencje incydentów: finansowe, prawne, organizacyjne i wizerunkowe.
- Przykłady rzeczywistych ataków na przedsiębiorstwa.

Najpopularniejsze zagrożenia cybernetyczne:
- Phishing;
- Ransomware i złośliwe oprogramowanie.
- Zagrożenia związane z siecią i urządzeniami.

Cyberhigiena pracownika - codzienne dobre praktyki:
- Tworzenie silnych i unikalnych haseł.
- Uwierzytelnianie wieloskładnikowe (MFA).
- Blokowanie komputera podczas nieobecności.
- Bezpieczne korzystanie z poczty elektronicznej.
- Ochrona danych firmowych przed nieuprawnionym dostępem.
- Bezpieczne korzystanie z urządzeń mobilnych.
- Zasady bezpiecznego przechowywania i przesyłania dokumentów.
- Ochrona prywatności i danych osobowych.

Bezpieczna praca z narzędziami cyfrowymi i AI:
- Korzystanie z narzędzi chmurowych.
- Ryzyka związane z korzystaniem z publicznych narzędzi AI.
- Jakich danych firmowych nie wolno wprowadzać do chatbotów i publicznych modeli AI?
- Weryfikacja informacji i dokumentów generowanych przez AI.
- Bezpieczne udostępnianie plików i nadawanie uprawnień.

Ochrona informacji i danych firmowych:
- Klasyfikacja informacji: publiczne, wewnętrzne, poufne i szczególnie chronione.
- Zasada minimalnych uprawnień.
- Bezpieczne przesyłanie informacji do klientów i kontrahentów.
- Ochrona dokumentów papierowych i elektronicznych.
- Bezpieczna praca poza biurem i w podróży służbowej.
- Odpowiedzialność pracownika za powierzony sprzęt i informacje.

Reagowanie na incydenty cyberbezpieczeństwa:
- Jak rozpoznać, że mogło dojść do cyberataku?
- Co zrobić po kliknięciu podejrzanego linku?

- Jak postępować po otwarciu zainfekowanego załącznika?
- Co zrobić w przypadku utraty laptopa lub telefonu służbowego?
- Jak zgłosić incydent do działu IT lub osoby odpowiedzialnej za bezpieczeństwo?
- Dlaczego szybkie zgłoszenie jest ważniejsze niż samodzielne naprawianie problemu?
- Czego nie robić po wykryciu incydentu?

Podsumowanie:

- Najważniejsze zasady cyberhigieny.
- Lista dobrych praktyk do stosowania w codziennej pracy.
- Omówienie najczęściej popełnianych błędów.
- Indywidualna odpowiedzialność za bezpieczeństwo organizacji.

Prelegent:

Beata Konieczna-Drzewiecka

- Inspektor Ochrony Danych MSWiA.

Dr nauk prawnych, asystent w Katedrze Prawa Informatycznego WPIA UKSW, od 2003 r. Sekretarz Podyplomowych Studiów Ochrony Danych Osobowych i Informacji Niejawnych, wykładowca i autorka opracowań z problematyki ochrony danych osobowych.-

Harmonogram:

8:45 - 09:00	**Logowanie**
09:00 - 10:30	**Szkolenie**
10:30 - 10:45	**Przerwa**
10:45 - 12:30	**Szkolenie**
12:30 - 13:00	**Lunch**
13:00 - 15:00	**Szkolenie**
15:00	**Zakończenie szkolenia**

KARTA ZGŁOSZENIA

Prosimy przesłać e-mailem: **wlr@wlr.com.pl** lub faksem: **+48 22 832 01 98**

Webinar: Cyberbezpieczeństwo w praktyce - jak chronić firmę i pracowników przed cyberzagrożeniami?

21 stycznia 2027 r. - Online

Imiona oraz nazwiska uczestników:

Nazwa, adres NIP firmy:

Telefon uczestnika / osoby kontaktowej:

E-mail uczestnika / osoby kontaktowej:

❑ *Proszę o wysłanie e-faktury VAT w formie załącznika PDF na adres e-mail:*

Uwagi:

Cena uczestnictwa

❑ **1250 zł + VAT** koszt dostępu do streamingu dla jednego uczestnika, przy zgłoszeniu do 15 stycznia 2027r.

❑ **1450 zł + VAT** koszt dostępu do streamingu dla jednego uczestnika, przy zgłoszeniu po 15 stycznia 2027r.

Warunki uczestnictwa

Cena obejmuje: prelekcje, materiały, certyfikat. ● Organizator zastrzega sobie prawo do zmian w programie. ● Wpłaty należy dokonać na konto podane na dokumencie proforma lub fakturze VAT. ● Niedokonanie wpłaty nie jest jednoznaczne z rezygnacją z udziału. ● Zamiast zgłoszonej osoby w szkoleniu może wziąć udział inny pracownik firmy. ● Rezygnację z udziału należy przesyłać listem poleconym na adres organizatora. ● Prosimy o dokonanie wpłaty zgodnie z terminem płatności podanym na fakturze proforma. ● Po otrzymaniu zgłoszenia prześlemy Państwu potwierdzenie udziału w szkoleniu oraz fakturę pro forma. ● Nieodwołanie zgłoszenia lub niewzięcie udziału w szkoleniu powoduje obciążenie pełnymi kosztami udziału. ● W przypadku rezygnacji w terminie mniejszym niż 14 dni przed rozpoczęciem szkolenia pobierane jest 100% opłaty za udział bez względu na termin wysłania formularza zgłoszeniowego. ● W przypadku, gdy wykładowca z przyczyn losowych nie będzie mógł przeprowadzić zajęć w podanym wcześniej terminie WLR Training Group zastrzega sobie prawo zmiany terminu zajęć. ● Uczestnicy szkolenia wskazani przez osobę zgłaszającą zostaną niezwłocznie poinformowani o tym fakcie. ● W przypadku finansowania ze środków publicznych faktura VAT zostanie wystawiona ze stawką VAT zw. ale cena na fakturze będzie ceną brutto z tego formularza zgłoszeniowego.

Zgody marketingowe

❑ Wyrażam zgodę na przetwarzanie moich danych osobowych w celu administrowania nim przez zleceniodawcę w myśl rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1). Wiem, że mam pełne prawo do wglądu i zmiany swoich danych, jak też ich usunięcia z bazy.

❑ Wyrażam zgodę na otrzymywanie informacji handlowej drogą elektroniczną od WLR Training Group Wojciech Jędrzejczyk (zgodnie z ustawą z dnia 18.07.2002 r. Dz. U. Nr 144 poz. 1204 'o świadczeniu usług drogą elektroniczną'). W każdym momencie przysługuje mi prawo do odwołania powyższej zgody. Oświadczam, że znam i akceptuję warunki uczestnictwa i rezygnacji w szkoleniu

Oświadczamy, że akceptujemy warunki uczestnictwa w szkoleniu oraz zobowiązujemy się do zapłaty.

Podpis i pieczątka