

W dniu **12 czerwca 2025 r.**

odbędzie się szkolenie w transmisji live on-line

Bezpieczeństwo informacji i cyberbezpieczeństwo - kompendium wiedzy dla kadry zarządzającej instytucji publicznych

Cele i korzyści z udziału w szkoleniu:

Z uwagi na wyzwania związane z liczbą i częstotliwością cyberataków na jednostki publiczne oraz wymaganiami prawnymi (m.in.: RODO, KRI, KSC, NIS2), rekomendowane są szkolenia z tematyki cyberbezpieczeństwa dla pracowników, a szczególnie kadry zarządzającej, w tym najwyższego kierownictwa (wymóg NIS2) każdego urzędu.

Aktualizacja wiedzy kadry zarządzającej w tym obszarze ma kluczowe znaczenie dla zapewnienia skutecznej ochrony informacji w urzędzie i zapewnienia właściwego poziomu wdrożonych cyberzabezpieczeń.

Zapraszamy na spotkanie, na którym omówione zostaną główne zagadnienia związane z cyberbezpieczeństwem jednostek administracji publicznej, w tym m.in.:

- wymagania formalno-prawne jakie dotyczą cyberbezpieczeństwa w jst i jednostkach podległych,
- szczególną rolę kadry zarządzającej w zapewnieniu skutecznego cyberbezpieczeństwa
- dobre praktyki, które można „od ręki” i często bez dodatkowych kosztów wdrożyć w urzędzie,
- przykładowe cyberataki na jednostki administracji publicznej w Polsce oraz ich konsekwencje finansowe i wizerunkowe,
- sposoby skutecznego zwiększania świadomości cyberzagrożeń wśród pracowników,
- dobre praktyki minimalizowania konsekwencji cyberataków oraz wycieków danych,
- skuteczne metody unikania przez pracowników ataków phishingowych.

Wykładowca: audytor, trener, doradca i kierownik projektów. Specjalista w dziedzinie bezpieczeństwa informacji. Audytor wiodący ISO/IEC 27001. Trener i egzaminator ECDL. Członek Polskiego Towarzystwa Informatycznego. Doradza firmom i jednostkom administracji publicznej m.in. z zakresu ochrony informacji, cyberbezpieczeństwa oraz przygotowania i wdrożenia odpowiednich polityk bezpieczeństwa. W zakresie szkoleń specjalizuje się w tematach związanych z cyberzagrożeniami, bezpieczeństwem informacji i ochroną danych osobowych.

Forma szkolenia: Wykład, Analiza przypadków, Dyskusja moderowana przez trenera. Czas trwania szkolenia: 9.00 - 14.00

- Zajęcia odbywają się 'na żywo', uczestnicy biorący udział w szkoleniu sami decydują, w jakim miejscu z niego skorzystają - w domu czy w miejscu swojego zatrudnienia. Szkolenia prowadzone są w formie interaktywnej. Podczas spotkania uczestnik widzi na ekranie swojego komputera prezentację multimedialną, będącą podstawą wykładu, oraz trenera, omawiającego ujęte w programie szkolenia zagadnienia. W trakcie szkolenia uczestnicy mogą na bieżąco, na czacie lub łącząc się przez kamerę, zadawać pytania i wyjaśniać wątpliwości.
- Szkolenie on-line realizujemy na platformie ClickMeeting. Do uczestnictwa w szkoleniu potrzebny jest komputer/tablet/smartfon z połączeniem do internetu. Preferowaną przeglądarką do udziału w szkoleniu jest Google Chrome.
- Wykładu można słuchać korzystając z głośników wbudowanych w komputer, albo używając swoich słuchawek. Platforma nie wprowadza obowiązku korzystania ze słuchawek to uczestnik wybiera sposób słuchania wykładu.
- Po zakończeniu szkolenia każdy z uczestników otrzymuje certyfikat imienny potwierdzający udział w spotkaniu (wg preferencji - zeskanowany lub papierowy)
- Harmonogram szkolenia:

09.00 – rozpoczęcie szkolenia

09.00 – 10.30 – szkolenie

10.30 – 10.45 – przerwa

10.45 – 12.15 – szkolenie

12.30 – 12.45 – przerwa

12.45 – 14.00 – szkolenie

Koszt szkolenia on-line: 690 zł netto + VAT (Cena ze stawką VAT „zwolnione” dla instytucji opłacających szkolenie w co najmniej 70% ze środków publicznych).

Cena zawiera: uczestnictwo w szkoleniu, materiały szkoleniowe w wersji elektronicznej, certyfikat (wg preferencji - zeskanowany lub papierowy). Przy zgłoszeniu więcej niż jednej osoby istnieje możliwość negocjowania rabatów.

Zgłoszenia: Zgłoszenia można przesyłać e-mailem na adres: szkolenia@euro-training.com.pl

PROGRAM SZKOLENIA

[Program szkolenia jest własnością intelektualną wykładowcy i przetwarzanie go dla celów komercyjnych bez wiedzy i zgody autora jest zabronione]

1. Wykorzystywanie sztucznej inteligencji (AI) w dezinformacji i oszustwach internetowych - przykłady

2. Dezinformacja i fake news. Jak się bronić?

3. Prawne aspekty bezpieczeństwa informacji i cyberbezpieczeństwa:

- Jakie mamy obowiązki w naszej organizacji związane z ochroną informacji np. RODO, KRI, KSC, ...?
- Czy RODO jeszcze działa?
- Dyrektywa NIS2 i nowa ustawa o KSC, czyli nowe obowiązki dotyczące cyberbezpieczeństwa
- Wewnętrzne polityki i procedury bezpieczeństwa to też prawo

4. Budowanie kultury bezpieczeństwa (świadomości) jest kluczowe dla każdej organizacji

- Od czego zacząć
- Czy człowiek to najsłabsze ogniwo?
- Rola kadry zarządzającej w budowaniu świadomości

5. Co kontrolerzy NIK zobaczyli w urzędach i dlaczego wnioski z tych kontroli mogą dotyczyć naszego podmiotu?

6. Incydenty bezpieczeństwa

- Co to jest incydent?
- Kiedy i komu zgłaszać incydenty?
- Rejestr incydentów jako narzędzie zapewnienia ochrony informacji
- Dlaczego warto zgłaszać incydenty?
- Dlaczego warto zgłaszać incydenty do CERTu?

7. Aktualne zagrożenia w cyberprzestrzeni

- Typy ataków / główne cyberzagrożenia / schematy działania cyberprzestępców
- Kradzieże i wyłudzenia informacji – przykłady z polskich organizacji
- Jak się bronić?

8. Bezpieczna praca zdalna – dobre praktyki

- Zagrożenia dla urządzeń mobilnych i zasady bezpiecznego korzystania
- Szyfruj komunikację i dane tam, gdzie tylko można

9. Proste i skuteczne metody codziennej ochrony informacji przez pracowników – zasady cyberhigieny

- Kopia bezpieczeństwa wg zasady „3-2-1”
- Aktualizacja systemów i programów
- Czy chmurze można zawsze ufać?
- Szyfrowanie danych jako jedyna skuteczna metoda zachowania poufności
- Używaj dwuskładnikowego uwierzytelnienia (MFA) zawsze ..., jeśli jest to możliwe

10. Audyty i testy bezpieczeństwa mają sens, ponieważ lepiej sprawdzić własne zabezpieczenia zanim ... zrobią to cyberprzestępcy

- Rodzaje testów bezpieczeństwa
- Korzyści z testów
- Jak przygotować pracowników i organizację do testów socjotechnicznych?

11. Zasady bezpiecznego użytkowania poczty elektronicznej i mediów społecznościowych

- Pamiętaj hasło do poczty e-mail
- Szyfrowanie załączników do e-maili
- Korzystanie w „UDW”

12. Bezpieczne hasła do Twoich systemów:

- Jak tworzyć silne hasła?
- Jakie hasła musimy mieć zawsze „w głowie”?
- Menedżery haseł jako właściwe narzędzie do skutecznego zarządzania hasłami. Przykłady

13. Dwuskładnikowe uwierzytelnienie (2FA/MFA) to już standard w pracy i życiu prywatnym

- Smsy, aplikacje, klucze sprzętowe (U2F)
- Należy lepiej zabezpieczać konta szczególnie istotne dla organizacji

14. Wycieki i kradzieże haseł

- Jak sprawdzić, czy moje hasła wyciekły? Przykładowe serwisy
- Co zrobić, gdy moje hasła wyciekną?

15. Phishing i Ransomware jako największe zagrożenia dla każdej organizacji

- Dlaczego ataki typu ransomware są tak niebezpieczne? Konsekwencje dla organizacji
- Spoofing, Phishing, Smishing, Vishing, ...
- Jak odróżnić fałszywą korespondencję e-mail przychodzącą do naszej organizacji?
- Jak sprawdzić czy otrzymany link lub załącznik jest bezpieczny? Przykładowe narzędzia

16. Metadane w dokumentach BIP. Czy są cenne dla cyberprzestępców?

17. Jak wdrażać System Zarządzania Bezpieczeństwem Informacji (SZBI) np. wg normy ISO 27001?

18. Polityki Bezpieczeństwa Informacji (PBI) oraz procedury i instrukcje jako skuteczne narzędzie ochrony informacji

19. Pytanie / Odpowiedzi / Dyskusja



Euro-Training
Centrum Szkoleniowo-Doradcze
ul. Św. Marcin 45c/16, 61-806 Poznań
tel. 61 850 19 99, fax 61 850 19 32
e-mail: szkolenia@euro-training.com.pl
www.euro-training.com.pl

KARTA ZGŁOSZENIA NA SZKOLENIE:

Bezpieczeństwo informacji i cyberbezpieczeństwo - kompendium wiedzy dla kadry zarządzającej instytucji publicznych

☐ 12 czerwca 2025 r.

☐ udział w szkoleniu on-line - 690 zł netto/os.

(cena bez VAT dla instytucji opłacających szkolenie w co najmniej 70% ze środków publicznych)

☐ Oświadczamy, że ww. szkolenie jest finansowane w całości ze środków publicznych oraz ma charakter kształcenia zawodowego lub służy przekwalifikowaniu zawodowemu co uprawnia nas do korzystania z przysługującego nam zwolnienia z VAT (zwolnienie na podstawie art. 43 ust. 1 pkt 29 c ustawy z dnia 11.03.2004 o podatku od towarów i usług (ze zm.))

☐ Oświadczamy, że ww. szkolenie jest finansowane przynajmniej w 70% ze środków publicznych oraz ma charakter kształcenia zawodowego lub służy przekwalifikowaniu zawodowemu co uprawnia nas do korzystania z przysługującego nam zwolnienia VAT (zwolnienie na podstawie § 3 ust. 1 pkt 14 Rozporządzenia Ministra Finansów z dnia 20.12.2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień).

Prosimy o wystawienie faktury: ☐ Zwolnienie z VAT ☐ VAT 23%

UCZESTNIK :

Imię i nazwisko.....e-mail.....

Wydział/stanowisko.....tel. i fax.....

ZGŁASZAJĄCY:

Imię i nazwisko.....e-mail.....

Wydział/stanowisko.....tel. i fax.....

DANE DO WYSTAWIENIA FAKTURY VAT:

Nazwa Firmy.....

Adres.....

NIP.....

☐ Proszę o przesłanie faktury w wersji elektronicznej na adres e-mail:

Upoważniam Centrum Szkoleniowo-Doradcze Euro-Training do wystawienia faktury VAT bez podpisu odbiorcy. Wyrażam zgodę na umieszczenie moich danych osobowych w bazie adresowej Centrum Szkoleniowo-Doradcze Euro-Training oraz na przetwarzanie ich dla potrzeb marketingu. Klauzula informacyjna- zgodnie z art. 13 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679z 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). Podającemu swoje dane przysługuje prawo wglądu do nich oraz możliwość ich poprawiania. Informacja dotycząca ochrony danych osobowych: <http://euro-training.com.pl>

Warunki zgłoszenia na szkolenie.

1. Przesłanie wypełnionego formularza jest zobowiązaniem do zapłaty za szkolenie.
2. Rezygnacja z udziału w szkoleniu może być dokonana najpóźniej na 7 dni przed datą szkolenia, wyłącznie w formie pisemnej. Rezygnacja w późniejszym terminie lub nieobecność na szkoleniu online nie zwalnia od zapłaty za szkolenie.
3. EURO-TRAINING zastrzega sobie prawo do odwołania szkolenia z przyczyn od siebie niezależnych i odstąpienia od realizacji szkolenia. EURO-TRAINING nie ponosi odpowiedzialności za szkody powstałe z powodu odwołania szkolenia.
4. Oświadczamy, że zapoznaliśmy się z warunkami w pkt. 1-3 i je akceptujemy.

.....
pieczęć i podpis

Dane firmy szkoleniowej:

EURO-TRAINING Centrum Szkoleniowo-Doradcze Honorata Filipiak
ul. Św. Marcin 45c/16, 61-806 Poznań
NIP 784-145-27-21
Nr konta: Credit Agricole 21 1940 1076 5261 0235 0000 0000