

## **CYBERZAGROŻENIA A SKUTECZNE AUDYTY BEZPIECZEŃSTWA W DOBIE POWSZECHNEJ CYFRYZACJI JEDNOSTEK PUBLICZNYCH**

### **WAŻNE INFORMACJE O SZKOLENIU:**

Każda instytucja publiczna – zgodnie z obowiązującymi przepisami np. RODO, KRI, KSC - powinna dbać o ochronę informacji. Audyty i testy bezpieczeństwa stanowią doskonałe narzędzie weryfikacji czy, i w jakim stopniu, wdrożone polityki lub zabezpieczenia w Waszej jednostce spełniają wymagania standardów zabezpieczeń oraz wymogów przepisów prawa. Poza weryfikacją, przede wszystkim, należy dbać o cykliczne zwiększanie świadomości wśród kadry zarządzającej i pracowników dotyczącej aktualnych cyberzagrożeń oraz właściwej ochrony informacji. Powszechna cyfryzacja procesów przeprowadzanych w urzędzie wpływa na szybki wzrost zagrożeń a tym samym cyberbezpieczeństwo stało się jednym z najważniejszych wyzwań dla podmiotów publicznych.

- *Czy wiecie Państwo, że codziennie przeprowadzane są próby ataków cybernetycznych na instytucje publiczne?*
- *Czy wiecie Państwo, jaki jest koszt wycieku lub kradzieży danych?*
- *Czy znacie Państwo przykłady wycieku ważnych informacji z urzędów w Waszym regionie?*
- *A może Państwa pracownik dostał e-mail z podejrzanym załącznikiem lub linkiem i „tylko kliknął”?*
- *A jakie wnioski dla Państwa urzędu wypływają z kontroli NIK przeprowadzonych w jednostkach samorządowych w zakresie bezpieczeństwa informacji?*

**To ważne pytania, na które postaramy się znaleźć odpowiedzi podczas spotkania.**

Szkolenie pomoże Państwu poznać podstawowe rodzaje zagrożeń, typy ataków oraz skuteczne i często bezkosztowe sposoby ochrony danych a także podnieść świadomość dotyczącą wartości posiadanych informacji przez urząd. Istotnym elementem szkolenia są także aspekty audytów i kontroli dotyczących cyberbezpieczeństwa w jednostkach publicznych.

### **CELE I KORZYŚCI:**

- Omówienie na praktycznych przykładach zagadnień związanych z ochroną informacji (w tym danych osobowych) w jednostkach publicznych.
- Zapoznanie uczestników z prawnymi aspektami cyberbezpieczeństwa i bezpieczeństwa informacji.
- Poznanie przykładów ataków na instytucje publiczne i zasad ochrony przed atakami.
- Uzyskanie prostych narzędzi pomocnych w budowaniu „od zaraz” cyberbezpieczeństwa oraz kultury ochrony informacji w jednostce administracji publicznej.

## **PROGRAM:**

1. Kultura ochrony informacji.
2. Prawne aspekty bezpieczeństwa informacji i cyberbezpieczeństwa.
3. Obowiązki jednostek publicznych w obszarze bezpieczeństwa informacji.
4. Cyfryzacja przetwarzania danych w jst: szanse i wyzwania.
5. Audyty bezpieczeństwa: podstawowe zasady oraz korzyści.
6. Rodzaje testów bezpieczeństwa: przykładowe wyniki z urzędów.
7. Cyberataki, kradzieże i wyłudzenia informacji z jednostek publicznych. Przykłady.
8. Cyberbezpieczeństwo w pracy zdalnej.
9. Jak zachować poufność przesyłanych dokumentów?
10. Proste, skuteczne a często bezkosztowe metody codziennej ochrony informacji w urzędzie.
11. Czy można żyć bez pendrive'a? Co możemy wdrożyć zamiast?
12. Jak tworzyć silne hasła i jak „zapamiętać” 299 haseł?
13. Phishing czyli jak odróżnić fałszywą korespondencję e-mail przychodzącą do urzędu?
14. Ataki ransomware – największe zagrożenia z Internetu.
15. Metadane w dokumentach w BIP. Czy są cenne dla przestępców?
16. Pytania/Odpowiedzi.

## **ADRESACI:**

Kadra zarządzająca jednostek publicznych, pracownicy jednostek publicznych, którzy chcą poznać zagadnienia cyberbezpieczeństwa i bezpieczeństwa informacji (w tym danych osobowych) zgodnie z aktualnym stanem prawnym i zmieniającymi się zagrożeniami.

## **PROWADZĄCY:**

Trener, doradca i kierownik projektów. Specjalista w dziedzinie bezpieczeństwa informacji. Trener ECDL EPP e-Urzędnik oraz kierownik projektów ICT (Fn-TSPM). Specjalista IT Security (CISS - Certified IT Security Specialist). Członek Polskiego Towarzystwa Informatycznego. Ma za sobą również kilkuletnie doświadczenie wykładowcy wyższej uczelni. Poprzednio kierownik Wydziału Informatyki w dużej jednostce administracji samorządowej. Był odpowiedzialny za kluczowe projekty informatyczne realizowane w urzędzie oraz skuteczne wdrażanie Polityki Bezpieczeństwa Informacji. Prowadzi szkolenia oraz konsultacje w firmach i administracji.

## INFORMACJE ORGANIZACYJNE I KARTA ZGŁOSZENIA

### Cyberzagrożenia a skuteczne audyty bezpieczeństwa w dobie powszechnej cyfryzacji jednostek publicznych



Szkolenie będziemy realizowali w formie webinarium on line.



**3 grudnia 2021 r.**

**Szkolenie w godzinach 9:30-13:30**



**Cena: 320 PLN netto/os.** Udział w szkoleniu zwolniony z VAT w przypadku finansowania szkolenia ze środków publicznych.

#### CENA zawiera:

udział w profesjonalnym szkoleniu on-line,  
materiały szkoleniowe w wersji elektronicznej,  
certyfikat ukończenia szkolenia,  
możliwość konsultacji z trenerem.

#### DANE DO KONTAKTU:

Fundacja Rozwoju Demokracji Lokalnej Ośrodek Regionalny w Zielonej Górze  
al. Niepodległości 16/9, 65 – 048 Zielona Góra  
tel. 68 453 22 09, e-mail: [szkolenia.zg@frdl.org.pl](mailto:szkolenia.zg@frdl.org.pl), [www.zg.frdl.pl](http://www.zg.frdl.pl)

### DANE UCZESTNIKA ZGŁASZANEGO NA SZKOLENIE

Nazwa i adres nabywcy  
(dane do faktury)

Nazwa i adres odbiorcy

NIP

Telefon

1. Imię i nazwisko uczestnika,  
stanowisko,  
E-MAIL i TEL. DO KONTAKTU

2. Imię i nazwisko uczestnika,  
stanowisko,  
E-MAIL i TEL. DO KONTAKTU

Oświadczam, że szkolenie dla ww. pracowników jest kształceniem zawodowym finansowanym w całości lub co najmniej 70% ze środków publicznych (proszę zaznaczyć właściwe)

TAK ☐ NIE ☐

Proszę o certyfikat w formie: Elektronicznej ☐ e mail.....

Proszę o przesłanie faktury na adres mailowy: .....

Dokonanie zgłoszenia na szkolenie jest równoznaczne z zapoznaniem się i zaakceptowaniem regulaminu szkoleń Fundacji Rozwoju Demokracji Lokalnej zamieszczonym na stronie Organizatora [www.zg.frdl.pl](http://www.zg.frdl.pl) oraz zawartej w nim Polityce prywatności i ochrony danych osobowych.

**Wypełnioną kartę zgłoszenia należy przesłać poprzez formularz zgłoszenia na [www.zg.frdl.pl](http://www.zg.frdl.pl) do 29 listopada 2021 r.**

UWAGA Liczba miejsc ograniczona. O udziale w szkoleniu decyduje kolejność zgłoszeń. Zgłoszenie na szkolenie musi zostać potwierdzone przesłaniem do Ośrodka karty zgłoszenia. Brak pisemnej rezygnacji ze szkolenia najpóźniej na trzy dni robocze przed terminem jest równoznaczny z obciążeniem Państwa należnością za szkolenie niezależnie od przyczyny rezygnacji. Płatność należy uregulować przelewem na podstawie wystawionej i przesłanej FV.

Podpis osoby upoważnionej \_\_\_\_\_