

## **ZMIANY W CYBERBEZPIECZEŃSTWIE W ZWIĄZKU Z DYREKTYWĄ NIS2 I NOWĄ USTAWĄ O KRAJOWYM SYSTEMIE BEZPIECZEŃSTWA. NIEZBĘDNIK DLA KADRY ZARZĄDZAJĄCEJ JST I JEDNOSTEK PODLEGŁYCH**

### **WAŻNE INFORMACJE O SZKOLENIU:**

W 2023 r. weszła w życie nowa dyrektywa NIS2 dotycząca zapewnienia odpowiedniego poziomu cyberbezpieczeństwa w krajach Unii Europejskiej, a w tym roku ukaże się nowa ustawa o Krajowym Systemie Cyberbezpieczeństwa (KSC). Administracja publiczna zostanie włączona do grupy Podmiotów Kluczowych. Podmioty te będą miały szereg obowiązków m.in. w zakresie obsługi incydentów, ujawniania luk bezpieczeństwa, testowania poziomu cyberbezpieczeństwa swoich systemów oraz efektywnego wykorzystania szyfrowania danych. Wprowadzane zmiany mają istotny wpływ na dotychczasowo stosowaną praktykę w jednostkach, wobec czego aktualizacja wiedzy kierowników i dyrektorów w tym obszarze ma kluczowe znaczenia dla zapewnienia skutecznej ochrony informacji w urzędzie oraz zgodności z aktualnymi wymaganiami w tym także RODO i KRI. Dodatkowo Najwyższa Izba Kontroli prowadzi kontrole w jst w całym kraju, które przynoszą bardzo zaskakujące wyniki: większe i mniejsze jst mają kłopot ze skutecznością własnych polityk i procedur bezpieczeństwa w zakresie np. ochrony danych osobowych, korzystania z poczty e-mail oraz utrzymania podstawowej wiedzy i umiejętności pracowników z obszaru cyberbezpieczeństwa.

Podczas proponowanego szkolenia:

- Krok po kroku, omówimy zagadnienia związane z cyberbezpieczeństwem w jst oraz jednostkach podległych i roli kadry zarządzającej w zakresie rekomendowanym w powyższym projekcie oraz dyrektywie NIS2 i planowanej ustawie o KSC.
- Przeanalizujemy występujące cyberzagrożenia i ich konsekwencje.
- Przypominamy procedury jakie w zakresie cyberbezpieczeństwa powinny być wdrożone w jednostce oraz wskażemy na co w ich zapisach szczególnie zwracać uwagę.
- Zaprezentujemy zadania i obowiązki jednostek, ze szczególnym uwzględnieniem zgłaszania incydentów.
- Prezentowane zagadnienia prawne będziemy popierać licznymi przykładami z praktyki dla lepszego zobrazowania omawianych regulacji i zasad postępowania.

### **CELE I KORZYŚCI:**

- Poznanie odpowiedzi na kluczowe pytania:
  - Czy wdrażane przez jst zabezpieczenia faktycznie działają?
  - Czy kadra zarządzająca zdaje sobie sprawę ze swojej roli w procesie ochrony informacji?
  - Czy pracownicy wiedzą, jak zgłaszać incydenty i dlaczego to jest tak ważne?
- Zapoznanie z głównymi wymaganiami formalno-prawnymi jakie dotyczą cyberbezpieczeństwa w jst i jednostkach podległych wynikające z RODO, KRI i aktualnego KSC.
- Zdobywanie wiedzy z zakresu najnowszych zmian prawnych, w tym dyrektywę NIS2 i planowaną, nową KSC.
- Poznanie przykładowych cyberataków na jst oraz ich konsekwencji, a także dobre praktyki minimalizowania tych konsekwencji.
- Poznanie roli kadry zarządzającej w zapewnieniu skutecznej ochrony informacji.
- Zdobywanie informacji na temat wewnętrznych procedur dotyczących cyberbezpieczeństwa procedur i ich aktualizacji.
- Zapoznanie z najczęściej popełnianymi błędami w zakresie cyberbezpieczeństwa, które wskazywane są podczas kontroli np. NIK oraz testów i audytów bezpieczeństwa.

## **PROGRAM:**

- 1. Wymagania dla kadry zarządzającej jst i jednostek podległych wynikające z aktualnych przepisów prawa:**
  - Ogólne Rozporządzenie o ochronie danych (RODO).
  - Rozporządzenie Krajowe Ramy Interoperacyjności (KRI).
  - Ustawa Krajowy System Cyberbezpieczeństwa (KSC).
- 2. Wymagania nowej dyrektywy NIS2:**
  - Co i w jakim stopniu dotyczy jst?
  - JST jako podmiot kluczowy - obowiązki
- 3. Aktualny stan planowanej, nowej ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC).**
- 4. System Zarządzania Bezpieczeństwem Informacji (SZBI) w praktyce codziennej pracy urzędu:**
  - Jak zbudować skuteczny SZBI w jst? Od czego zacząć?
  - Jak się przygotować do wdrożenia SZBI?
  - Ciągłe doskonalenie systemu.
- 5. Wewnętrzne polityki, procedury i instrukcje w obszarze bezpieczeństwa informacji i cyberbezpieczeństwa:**
  - Jak tworzyć dokumentację, aby były zrozumiała?
  - Jak sprawdzać, czy pracownicy znają wewnętrzne regulacje?
- 6. Kontrole Najwyższej Izby Kontroli w jst – omówienie głównych wniosków pokontrolnych. Jak się uczyć na błędach innych:**
  - Poczta e-mail w urzędzie.
  - Skuteczna ochrona danych osobowych szczególnie w obszarze ich szczególnej kategorii.
  - Wiedza i umiejętności pracowników w obszarze cyberbezpieczeństwa.
- 7. Subiektywny przegląd wyników Ankiety Dojrzałości Cyberbezpieczeństwa jst.**
- 8. Przykładowe ataki, kradzieże i wycieki danych w jst.**
- 9. Podstawy cyberhigieny dla każdego kierownika.**
- 10. Zalecenia dotyczące reakcji na incydenty bezpieczeństwa:**
  - Spokój, spokój, spokój („3 x S”).
  - Zgłaszać incydenty a nie ukrywać.
  - Skutecznie informować interesariuszy.
  - Wyciągać wnioski i wdrażać działania korygujące.
  - Monitorować infrastrukturę.
- 11. Jak bezkosztowo poprawić cyberbezpieczeństwo w jst? Co można zrobić „od ręki”.**
- 12. Jak przygotować urząd do testów bezpieczeństwa, w tym także socjotechnicznych, ponieważ nie ma lepszej drogi do sprawdzenia czy nasze zabezpieczenia działają jak ich zewnętrzna weryfikacja?**
- 13. Phishing - oszustwa i wyłudzenia z uwzględnieniem ataku typu BEC (Business E-mail Compromise).**
- 14. A co zrobić, gdy już „coś się jednak kliknęło”? Czy to już „koniec świata”? NIE!**
- 15. Ransomware jako wyjątkowo poważne zagrożenie dla jst:**
  - Jak uchronić urząd przed atakiem?
  - Co zrobić po ataku?
  - Czy można zapłacić okup?
- 16. Podsumowanie. Pytania. Dyskusja.**

## **ADRESACI:**

Kadra zarządzająca jst i jednostek podległych: sekretarze, skarbnicy, dyrektorzy, kierownicy, naczelnicy, Inspektorzy Ochrony Danych.

## **PROWADZĄCY:**

Audytor, trener, doradca. Specjalista w dziedzinie bezpieczeństwa informacji i cyberzagrożeń. Audytor wiodący normy ISO/IEC 27001. Członek Polskiego Towarzystwa Informatycznego. Prowadzi audyty bezpieczeństwa oraz szkolenia i konsultacje m.in. z zakresu bezpieczeństwa informacji i cyberbezpieczeństwa oraz budowania kultury ochrony informacji.

## Zmiany w cyberbezpieczeństwie w związku z dyrektywą NIS2 i nową ustawą o Krajowym Systemie Bezpieczeństwa. Niezbędnik dla kadry zarządzającej jst i jednostek podległych



Szkolenie będziemy realizowali w formie webinarium on line.



24 lipca 2024 r.

Szkolenie w godzinach 10:00-14:00



**Cena: 449 zł netto/os. Przy zgłoszeniu do 28 czerwca 2024 cena wynosi 409 zł netto/os.** Udział w szkoleniu zwolniony z VAT w przypadku finansowania szkolenia ze środków publicznych.

### CENA zawiera:

udział w profesjonalnym szkoleniu on-line z możliwością zadawania pytań, materiały szkoleniowe w wersji elektronicznej, certyfikat ukończenia szkolenia.

### DANE

Centrum Szkoleniowe FRDL

### DO

ul. Księcia Witolda 7-9 p.102, 71-063 Szczecin;

### KONTAKTU:

tel. +48 725 302 316 (313), [centrum@frdl.szczecin.pl](mailto:centrum@frdl.szczecin.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 przesłanie faktury na adres mailowy: .....

Proszę o przesłanie certyfikatu 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.frdl.szczecin.pl](http://www.frdl.szczecin.pl) oraz zawartej w nim Polityce prywatności i ochrony danych osobowych.

**Wypełnioną kartę zgłoszenia należy przestać poprzez formularz zgłoszenia na [www.frdl.szczecin.pl](http://www.frdl.szczecin.pl) do 18 lipca 2024 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 \_\_\_\_\_