Fundacja Rozwoju Demokracji Lokalnej im. Jerzego Regulskiego

Centrum Mazowsze

Sesja konsultacyjno-szkoleniowa Forum Sekretarzy

Wybrane aspekty cyberbezpieczeństwa i dyrektywy NIS2 dla Sekretarzy

28 sierpnia 2024 r. 10.00 - 14.00.

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.

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 podstępowania.

Prowadzący spotkanie:

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.

Uczestnicy spotkania będą mieli możliwość przedstawienia kwestii problemowych, wymiany doświadczeń, zarówno z ekspertem prowadzącym spotkanie, jak innymi uczestnikami spotkania. Celem spotkania jest uzyskanie wielu cennych wskazówek i podpowiedzi, niezbędnych w codziennej pracy, dyskusji i uzyskania odpowiedzi na pytania od eksperta w przedmiotowy zakresie. Liczymy na Państwa aktywne uczestnictwo w spotkaniu.

Spotkanie będzie realizowane w formule hybrydowej: *formuła stacjonarna odbędzie się w wieżowcu przy ul. T. Chałubińskiego 8, piętro 10,* . Poniżej prezentujemy szczegółowy program oraz informacje organizacyjne dotyczące zgłoszenia udziału.

Zapraszamy do zrzeszenia i udziału w najbliższym spotkaniu Forum

Michał Wójcik
Dyrektor FRDL CM

Fundacja Rozwoju Demokracji Lokalnej Centrum Mazowsze
Biuro Fundacji Jelinka 6 01-646 Warszawa
+48 666 661 039 szkolenia@frdl.org.pl www.frdl.mazowsze.pl

Fundacja Rozwoju Demokracji Lokalnej im. Jerzego Regulskiego

Centrum Mazowsze

Sesja konsultacyjno-szkoleniowa Forum Sekretarzy

Wybrane aspekty cyberbezpieczeństwa i dyrektywy NIS2 dla Sekretarzy

28 sierpnia 2024 r. 10.00 - 14.00.

Cele i korzyści ze szkolenia:

- 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.
- Zdobycie wiedzy z zakresu najnowszych zmian prawnych, w tym dyrektywą NIS2 i planowaną, nową KSC.
- Poznanie przykładowych cyberataków na jst oraz ich konsekwencji, a także dobre praktyk minimalizowania tych konsekwencji.
- Poznanie roli kadry zarządzającej w zapewnieniu skutecznej ochrony informacji.
- Zdobycie 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 sesji:

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).
   - Nowa dyrektywa NIS2 i projekt nowej Ustawy Krajowy System Cyberbezpieczeństwa (KSC).
2. Kluczowa rola sekretarzy jst w codziennej ochronie informacji w urzędzie i budowaniu świadomości użytkowników.
3. Kontrole Najwyższej Izby Kontroli w jst – omówienie głównych wniosków pokontrolnych, czyli jak się uczyć na błędach …, ale nie swoich:
   - Poczta e-mail w urzędzie – bezpieczne korzystanie.
   - Skuteczna ochrona danych osobowych szczególnie w obszarze szczególnej kategorii danych.
   - Rozwój wiedzy i umiejętności pracowników w obszarze cyberbezpieczeństwa.
4. Jak (prawie) bezkosztowo poprawić cyberbezpieczeństwo w jst? Co można zrobić „od ręki”?
   - Aktywność kadry zarządzającej.
   - Korzystanie z grantów / projektów.
   - Ograniczenie uprawnień w systemach IT.
   - Blokada portów USB.
   - Blokada stron www.

Fundacja Rozwoju Demokracji Lokalnej Centrum Mazowsze
Biuro Fundacji Jelinka 6 01-646 Warszawa
+48 666 661 039 szkolenia@frdl.org.pl www.frdl.mazowsze.pl

- Black-list na serwerze poczty e-mail.
- Przekierowanie komunikacji z urzędem z e-maila na bezpieczne kanały np. e-Puap.
- Wewnętrzna edukacja z tematyki cyberzagrożeń i cyberhigieny.
- Mniej zadań dla informatyków.
- Wzrost umiejętności pracowników w tematach często zgłaszanych na help-desk.
- Inne pomysły uczestników …

5. Zalecenia dotyczące reakcji na incydenty bezpieczeństwa w jst:
   - Zgłaszać incydenty a nie ukrywać.
   - Rejestrować zgłaszane incydenty.
   - Skutecznie informować interesariuszy.
   - Wyciągać wnioski i wdrażać działania korygujące.
   - Monitorować infrastrukturę IT i pracowników.
6. Dobre praktyki służbowej cyberhigieny, które zadziałają także prywatnie:
   - Robić kopie bezpieczeństwa („Zasada: 3-2-1”).
   - Dbać o aktualizację systemów i programów.
   - Korzystać z programów antywirusowych.
   - Nie klikać w podejrzane linki i załączniki.
7. Jak przygotować urząd do testów bezpieczeństwa, w tym także socjotechnicznych? Ponieważ nie ma lepszej drogi do sprawdzenia czy zabezpieczenia działają jak ich zewnętrzna weryfikacja.
8. Phishing - oszustwa i wyłudzenia poprzez e-mail, sms, telefon, komunikator, ….
9. Jak sprawdzić, czy e-mail jest dobry czy fałszywy?
   - Weryfikacja adresu nadawcy i treści e-maila.
   - Weryfikacja nagłówka e-maila.
10. Jak sprawdzić czy link i załącznik są szkodliwe? Przykładowe narzędzia.
11. A co zrobić, gdy już „coś się jednak kliknęło”? Czy to już „koniec świata”? NIE!
12. Ransomware, czyli okup za odzyskanie danych - wyjątkowo poważne zagrożenie dla jst:
    - Jak uchronić urząd przed atakiem?
    - Co zrobić po ataku?
    - Czy można zapłacić okup cyberprzestępcom?
13. Pytanie / Odpowiedzi / Dyskusja.

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.

INFORMACJE ORGANIZACYJNE i KARTA ZGŁOSZENIOWA

Sesja konsultacyjno-szkoleniowa Forum Sekretarzy nt.:

Wybrane aspekty cyberbezpieczeństwa i dyrektywy NIS2 dla Sekretarzy

28 sierpnia 2024 2024 r. Szkolenie w godzinach 10:00-14:00

Hybrydowa sesja konsultacyjno-szkoleniowa będzie prowadzona i realizowana *w wieżowcu przy ul. T. Chałubińskiego 8, piętro 10,* **oraz online.**
Koszt udziału w spotkaniu dla osoby niezrzeszonej w Forum wynosi: 639 PLN – formuła stacjonarnym / 439 PLN formuła online. W przypadku członka Forum wynosi 220 PLN.
Cena obejmuje: Udział w profesjonalnej sesji konsultacyjno-szkoleniowej, materiały szkoleniowe w wersji papierowej, możliwość konsultacji z trenerem **i uczestnikami sesji.**

DANE DO KONTAKTU:	Fundacja Rozwoju Demokracji Lokalnej Centrum Mazowsze ul. Jelinka 6, 01-646 Warszawa; tel. 517 515 717, szkolenia@frdl.org.pl
Nazwa jednostki	
Dane jednostki NIP	
Dane jednostki adres	
Imię i nazwisko uczestnika **Kontakt: telefon i mail**	
Forma udziału w zajęciach (proszę zaznaczyć właściwe)	Stacjonarna ☐ Online ☐
Oświadczam, że szkolenie dla ww. pracowników jest kształceniem zawodowym finansowanym w całości lub co najmniej 70% ze środków publicznych (proszę zaznaczyć właściwe)	TAK ☐ NIE ☐

Dokonanie zgłoszenia na szkolenie jest równoznaczne z zapoznaniem się i zaakceptowaniem regulaminu szkoleń FRDL zamieszczonym na stronie Organizatora **www.frdl.mazowsze.pl** oraz zawartej w nim Polityce prywatności i ochrony danych osobowych.

Wypełnioną kartę zgłoszenia należy przesłać poprzez formularz zgłoszenia na www.frdl.mazowsze.pl lub mailem na adres szkolenia@frdl.org.pl do 23 sierpnia 2024 r.

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

Podpis osoby upoważnionej _____