

METODY I NARZĘDZIA TECHNOLOGICZNE, ORGANIZACYJNE I PRAWNE ZWIĘKSZAJĄCE OCHRONĘ PRZED CYBERZAGROŻENIAMI

WAŻNE INFORMACJE:

W dobie XXI wieku zagrożenia dla bezpieczeństwa informacji oraz danych osobowych zmieniły swój wymiar diametralnie. Jeszcze kilka lat temu w analizach ryzyka można było w większości znaleźć jako główne zagrożenia takie hasła jak kradzież, włamanie czy inne akty wandalizmu. Z uwagi na zmieniające się otoczenie, rozwój technologii oraz jej dostępność obserwujemy zdecydowany spadek tego typu działań przestępczych. Niestety jest i druga strona medalu, przestępcy również zwiększyli swoją aktywność w cyberprzestrzeni, a rozwiązania typu firewall czy antywirus są zdecydowanie nie wystarczające.

Niestety ostatnie przypadki ataków hackerskich pokazały, iż nawet wielomilionowe budżety na IT nie są wystarczające. Jak więc poradzić sobie w tak trudnych czasach? Na szkoleniu prelegent wskaże jakie działania są niezbędne, aby zmniejszyć prawdopodobieństwo stania się ofiarą cyberataku, jak w sposób zrównoważony dzielić zasoby między właściwe procedury, zabezpieczenia techniczne w tym IT oraz właściwą organizację pracy. Duża część szkolenia skupi się również na analizie ryzyka, jednak nie na tabelkach, lecz na jej roli w bezpieczeństwie organizacji oraz właściwemu interpretowaniu jej wyników, a także jak unikać najczęstszych błędów z nią związanych. Spotkanie dedykowane do osób mających podstawową wiedzę z zakresu ochrony danych osobowych oraz bezpieczeństwa informacji.

CELE I KORZYŚCI:

- Zapoznanie uczestników ze sposobami wdrażania rozwiązań technologicznych, organizacyjnych i prawnych służących ochronie instytucji publicznych przez cyberatakami.
- Omówienie aspektów związanych z procedurami bezpieczeństwa Informacji oraz działań organizacyjnych i możliwości technologicznych dzięki, którym instytucja będzie mogła zadbać o zwiększenie swojej odporności na ataki cyberprzestępców.
- Konsultacje z trenerem oraz innymi uczestnikami spotkania.

PROGRAM:

- 1. Wprowadzenie do zagadnienia cyberbezpieczeństwa:**
 - a. Definicja i cele cyberbezpieczeństwa,
 - b. Podstawowe zagrożenia dla cyberbezpieczeństwa. Rola i znaczenie działań prewencyjnych w cyberbezpieczeństwie.
- 2. Metody i narzędzia technologiczne zwiększające ochronę przed cyberzagrożeniami:**
 - a. Firewall i IDS/IPS,
 - b. Antywirusy i oprogramowanie anty-malware,
 - c. Szyfrowanie i technologie kryptograficzne,
 - d. Wirtualne sieci prywatne (VPN),
 - e. Zasady bezpieczeństwa dla użytkowników.
- 3. Metody i narzędzia organizacyjne zwiększające ochronę przed cyberzagrożeniami:**
 - a. Polityki bezpieczeństwa informacji. Analiza ryzyka i zarządzanie ryzykiem. Planowanie awaryjne i procedury awaryjne,
 - b. Szkolenia i edukacja pracowników,
 - c. Wewnętrzne audyty bezpieczeństwa informacji.
- 4. Metody i narzędzia prawne zwiększające ochronę przed cyberzagrożeniami:** Ogólne rozporządzenie o ochronie danych osobowych (RODO); Ustawa o ochronie danych osobowych; Ustawa o cyberbezpieczeństwie; Kodeks cywilny i karny.
- 5. Praktyczne aspekty ochrony przed cyberzagrożeniami:**
 - a. Analiza przypadków i scenariuszy zagrożeń,
 - b. Demonstracja narzędzi i technologii,
 - c. Ćwiczenia praktyczne.

ADRESACI:

Pracownicy sektora finansów publicznych odpowiadających za bezpieczeństwo Informacji, ochronę danych osobowych, za sprawy organizacyjne, bezpieczeństwo prawne i zapewnienie ciągłości funkcjonowania jednostki. Szkolenie skierowane do takich stanowisk jak: sekretarze, informatycy, inspektorzy ochrony danych, pełnomocnicy systemu zarządzania bezpieczeństwem informacji, prawnicy.

PROWADZĄCY:

Inspektor Ochrony Danych, Auditor wiodący ISO 27001, akredytowany Projekt Manager Prince 2 2009 Foundation oraz certyfikowany analityk wymagań REQB. Z wykształcenia inżynier oprogramowania, ukończył studia podyplomowe Audytu wewnętrznego w Administracji i Gospodarce. Autor opinii do projektu kodeksu postępowania dla jednostek oświaty. W branży informatyzacji i ochrony danych osobowych administracji publicznej działa od 2006 roku. Członek Stowarzyszenia Praktyków Ochrony Danych oraz

Stowarzyszenia do spraw Bezpieczeństwa Systemów Informacyjnych ISSA Polska, a także członek rady programowej projektu Cyfrowy Skaut.

Metody i narzędzia technologiczne, organizacyjne i prawne zwiększające ochronę przed cyberzagrożeniami



Szkolenie będziemy realizowali w formie **webinarium on line**.



23 sierpnia 2023 r.

Szkolenie w godzinach 09:00-14:00



Cena: 379 PLN 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 DO KONTAKTU: Fundacja Rozwoju Demokracji Lokalnej, Świętokrzyskie Centrum
ul. Sienkiewicza 78, IV piętro, 25-501 Kielce
tel. 41 344 66 30, 730-696-423, centrum@frdl.kielce.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.kielce.pl oraz zawartej w nim Polityce prywatności i ochrony danych osobowych.

Wypełnioną kartę zgłoszenia należy przestać poprzez formularz zgłoszenia na www.frdl.kielce.pl do 18 sierpnia 2023 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 _____