ApexNet PIENIĄDZE PUBLICZNE WIEDZA, KTÓRA CHRONI

Obowiązki podmiotów publicznych w świetle aktualnej i projektowanej regulacji ustawy o Krajowy System Cyberbezpieczeństwa

Dlaczego warto

Dlaczego warto?

Cyberbezpieczeństwo to dziś obowiązek całego kierownictwa urzędu. Szkolenie pokaże, jak praktycznie zabezpieczyć jednostkę zgodnie z Ustawą o KSC i wymogami NIS2.

Uczestnicy nauczą się:

- kto odpowiada za bezpieczeństwo,
- jak reagować na incydenty,
- jak zarządzać ryzykiem i przygotować jednostkę do NIS2.

Zapisz się i wzmocnij cyberbezpieczeństwo swojej jednostki.

Szczegóły organizacyjne

TERMIN: 07-08 maja g. 09:30 - 15:30
MIEJSCE: Platforma szkoleń online
TRENER: MAŁGORZATA CZARTORYSKA

Prawnik, wykładowca przedmiotów prawniczych Wyższej Szkoły Bankowej we Wrocławiu oraz Uniwersytetu Ekonomicznego we Wrocławiu. Certyfikowany trener z wieloletnim doświadczeniem. Specjalista z dziedzin: postępowanie egzekucyjne w administracji i sądowe, prawo administracyjne materialne, postępowanie administracyjne, samorząd terytorialny, finanse publiczne, prawo cywilne materialne i procedura cywilna.

OFERTA SPECJALNA

W ramach oferty specjalnej otrzymujesz szkolenie ONLINE lub STACJONARNE + drugie szkolenie w formie WIDEO za 50% ceny.

Aktualna oferta szkoleń wideo znajduje się TUTAJ

Standardowa cena ~~2198 zł,~~ a w ofercie specjalnej 1649 zł i zawiera:

CENA ZAWIERA

- Roczny dostęp do EduStrefy
- Szkolenie on-line na żywo
- EduBox, czyli paczkę materiałów wysłaną pocztą
- 60 dni dostępu do nagrania szkolenia
- Certyfikat ukończenia szkolenia
- Szkolenie w godzinach 9:30-15:30

PROGRAM

1.Cyberbezpieczeństwo w JST/urzędzie – kontekst i odpowiedzialność kierownictwa.

- Cel KSC i architektura krajowa (CSIRT-y, współpraca, rola podmiotów publicznych).
- Odpowiedzialność kierownika jednostki za organizację bezpieczeństwa (nadzór, zasoby, decyzje).
- Relacja z kontrolą zarządczą, BCP/DR, zarządzaniem dokumentacją i RODO (punkty styku).

Ćwiczenie: „Mapa odpowiedzialności" – RACI dla: IT, IOD, kancelaria/EZD, PR, kadry, zamówienia.

2.Podstawowe pojęcia KSC i praktyczne granice obowiązków.

- Incydent / incydent poważny / obsługa incydentu; podatność; ryzyko.
- Usługa kluczowa / usługa cyfrowa (w obecnym KSC) – jak to „czytać" w realiach urzędu.
- Minimalny standard: polityki, uprawnienia, rejestrowanie zdarzeń, kopie, aktualizacje, zarządzanie dostępem.

Mini-case: „Wyciek danych z poczty / phishing / ransomware w sekretariacie" – co robimy w 2h, 24h, 72h.

3.Współpraca z CSIRT, zgłaszanie incydentów i komunikacja.

- Kiedy zgłaszamy incydent, komu i w jaki sposób.
- Rola CSIRT na poziomie krajowym (NASK itp.).
- Komunikacja kryzysowa: mieszkańcy, media, organ nadzorczy (RODO), podmioty współpracujące.
- Dowody i łańcuch czynności (forensic light) – jak nie „zniszczyć" śladów.

Ćwiczenie: wypełnienie „karty incydentu" oraz przygotowanie checklisty działań.

4.Zarządzanie ryzykiem cyber w jednostce – podejście praktyczne.

- Prosta metodyka ryzyka: aktywa – zagrożenia – podatności – skutki – zabezpieczenia.
- Katalog typowych ryzyk w administracji: EZD, ePUAP/eDoręczenia, BIP, domena, AD, kopie zapasowe, dostawcy, systemy dziedzinowe.
- Priorytetyzacja działań: co daje największą redukcję ryzyka przy najmniejszym koszcie.

Ćwiczenie: przygotowanie rejestru ryzyk (top 10) dla jednostki oraz plan działań 30/60/90 dni.

5.NIS2 → KSC: nowy model podmiotów i nadzoru.

- Przejście z podziału NIS1 na podmioty kluczowe i podmioty ważne.
- Rozszerzenie katalogu sektorów i objęcie większej liczby podmiotów (w tym publicznych).
- Wzmocnienie uprawnień organów właściwych i mechanizmów nadzorczych.

Ćwiczenie: „Samoocena jednostki" – czy i dlaczego możemy wpaść w kategorię podmiotu kluczowego lub ważnego (na podstawie usług i roli jednostki).

6.Obowiązki w modelu NIS2: środki zarządzania ryzykiem.

- SZBI/ISMS „w wersji urzędowej": polityki, role, przeglądy ryzyka, szkolenia.
- Zabezpieczenia: zarządzanie dostępem, MFA, zarządzanie tożsamością, segmentacja sieci, backup 3-2-1, patching, EDR oraz logowanie zdarzeń.
- Łańcuch dostaw i dostawcy IT (umowy, SLA, audyty, wymagania bezpieczeństwa) – szczególnie istotne w zamówieniach publicznych.
- Ciągłość działania usług cyfrowych (BCP/DR) oraz minimalny katalog testów ciągłości działania.

Ćwiczenie: checklista „20 wymagań" oraz analiza luk (gap analysis): jest / częściowo / brak.

7.Incydenty w NIS2/KSC: nowe kanały i tempo zgłoszeń.

- Obowiązek i technika zgłaszania incydentów z użyciem systemu teleinformatycznego ministra (projekt).
- Rola CSIRT sektorowych (projekt) oraz współpraca operacyjna.
- Wewnętrzna procedura obsługi incydentu: detekcja → triage → eskalacja → decyzje → zgłoszenia → komunikacja.

Ćwiczenie: symulacja „incydent krytyczny w systemie dziedzinowym" – decyzje kierownictwa, działania IT oraz ścieżka formalna.

8.Odpowiedzialność, sankcje, kary administracyjne – jak się zabezpieczyć organizacyjnie.

- Kary administracyjne w projektowanej nowelizacji oraz obszary ryzyka niezgodności.
- Jak „dowodzić" należytej staranności: dokumenty, protokoły przeglądów, testy, szkolenia oraz audyty.

Ćwiczenie: przygotowanie „Teczki zgodności KSC/NIS2" – spisu dokumentów i dowodów.

9.Plan wdrożenia w jednostce: 90 dni / 6 miesięcy / 12 miesięcy.

- Szybkie działania podnoszące poziom bezpieczeństwa (quick wins): MFA, kopie zapasowe, segmentacja sieci, zarządzanie uprawnieniami, aktualizacje systemów, rejestr zasobów.
- Organizacja zarządzania cyberbezpieczeństwem: zespół ds. cyberbezpieczeństwa, cykl przeglądów, planowanie budżetu, raportowanie do kierownictwa jednostki.
- Integracja z EZD i zarządzaniem dokumentacją (incydent jako dokumentacja; retencja dokumentów; prowadzenie rejestrów).

Przygotowanie harmonogramu wdrożenia wraz z właścicielami działań i wskaźnikami realizacji.

„Wdrożenie na dokumentach” – warsztat.

- Projekt procedury obsługi incydentu cyberbezpieczeństwa (wersja urzędowa).
- Rejestr usług i systemów teleinformatycznych wraz z klasyfikacją krytyczności.
- Rejestr ryzyk cyberbezpieczeństwa (skala 1–4) oraz plan postępowania z ryzykiem.
- Wymagania bezpieczeństwa do SIWZ/OPZ oraz klauzule bezpieczeństwa do umów z dostawcami IT.

Dlaczego ApexNet?

Certyfikaty jakości

Po szczegółowym audycie uzyskaliśmy **certyfikat jakości TQLS Quality Alliance** dla instytucji szkoleniowych uznawany przez PARP.

Korzyści dla Ciebie:

- największe (ponad 21-letnie) doświadczenie w organizacji szkoleń z zamówień publicznych w Polsce,
- zewnętrznie potwierdzona najwyższa jakość organizacji szkoleń

Otrzymaliśmy **I miejsce** i tytuł "Lidera w organizacji szkoleń z zakresu zamówień publicznych".
Zgodnie z przeprowadzonymi badaniami rynku, na grupie 815 osób, jesteśmy także **najchętniej wybieraną firmą** szkoleniową z zakresu zamówień publicznych w Polsce!

Ponad 6000 opinii ★★★★★

Na naszej stronie internetowej znajdziesz ponad 6000 opinii zadowolonych klientów!

Korzyści dla Ciebie:

- wiarygodność potwierdzona opiniami klientów,
- przetestowana i zweryfikowana jakość merytoryki i organizacji szkoleń

EduStrefa

EduStrefa, to największy na rynku portal - społeczność, zrzeszający specjalistów. Roczny dostęp do EduStrefy przyznawany jest wyłącznie uczestnikom naszych szkoleń, którzy znajdą tam poszkoleniowe wsparcie w dalszej edukacji. Dostęp do EduStrefy ma już ponad **30 000** specjalistów!

Korzyści dla Ciebie:

- będziesz częścią **zamkniętej społeczności specjalistów**,
- zyskasz **setki** materiałów wspierających dalszy rozwój

Chcesz dowiedzieć się więcej?
skontaktuj się z opiekunem, który przesłał Ci tę ofertę

lub **zapisz się bezpośrednio na szkolenie**
www.apexnet.pl/szkolenia-otwarte