Izba Gospodarcza
Ciepłownictwo Polskie

SZKOLENIE ONLINE
10 czerwca 2021

PROGRAM SZKOLENIA

Cyberbezpieczeństwo w ciepłownictwie – podstawy prawne i aspekty praktyczne

w formie zdalnej z wykorzystaniem aplikacji ZOOM

9.30-10.00 Logowanie uczestników

10.00-11.30 **Panel I: Podstawowe pojęcia związane z cyberbezpieczeństwem systemów ciepłowniczych i ich praktyczne stosowanie.**
Mec. Monika Bogdał
Kierownik Zespołu Nowych Technologii, Kancelaria Prawna Piszcz i Wspólnicy sp. k.
- Krajowe i unijne obowiązujące oraz planowane akty prawne dotyczące cyberbezpieczeństwa;
- Kwalifikacja przedsiębiorstw ciepłowniczych, ciepłowni i elektrociepłowni do operatorów usług kluczowych;
- Operator usługi kluczowej, podmiot publiczny, dostawca usługi cyfrowej – nabycie statusu, zakres obowiązków;
- Systemy Informacyjne – zasady kwalifikacji i identyfikacji zasobów, klasyfikacja podatności i zagrożeń;
- Pojęcia związane z zarządzaniem incydentami, zarządzanie infrastrukturą biurową i przemysłową;
- Struktury cyberbezpieczeństwa – możliwe modele działania, wymogi prawne;
- Organizacyjne środki bezpieczeństwa – jak optymalizować ich wykorzystanie;
- Kary związane z nieprawidłową realizacją obowiązków związanych z cyberbezpieczeństwem.

11.30-11.40 przerwa

11.40-13.10 **Panel II: Zarządzanie cyberbezpieczeństwem – dobre praktyki i doświadczenia**
Wojciech Wrzesień
Kierownik Działu Strategii i Rozwoju NASK S.A.
- inwentaryzacja i paszportyzacja zasobów, wykrywanie podatności/zagrożeń i szacowanie ryzyka – narzędzia i najlepsze praktyki;
- Security Operation Center (SOC) – zlecenie usługi vs. budowa własnych struktur cyberbezpieczeństwa (za i przeciw);
- techniczne środki bezpieczeństwa – jak wybrać konkretne rozwiązania dla już działającego systemu IT, OT i IoT;
- raportowanie i szkolenia personelu – wyzwania, rzeczywiste potrzeby.

Wystąpienie na podstawie doświadczeń związanych z realizacją usług w ramach NanoSOC, NSOC, NOZOMI (monitoring OT), wykonanych analiz i badań topologii sieci.

13.10-13.20 przerwa

13.20-14.20 **Panel III: Case study – dokumentowanie procesu wykrywania i zgłoszenia incydentówcyberbezpieczeństwadotyczącychsiecibiurowej(IT);przemysłowej (OT) i internetu rzeczy IoT.**
Źródła, narzędzia, przykłady incydentów i sposobów zabezpieczania się przed nimi.
Piotr Jagielski
Menedżer Produktów Cybersecurity, NASK SA.
- Case study do panelu II – przykłady incydentów i sposobu postepowania.