SZKOLENIE ONLINE
10 czerwca 2021

NASK SA
secure and safe data

Izba Gospodarcza
Ciepłownictwo Polskie

Cyberbezpieczeństwo w ciepłownictwie – podstawy prawne i aspekty praktyczne

Szanowni Państwo, zapraszamy do udziału w szkoleniu nt. „Cyberbezpieczeństwo w ciepłownictwie – podstawy prawne i aspekty praktyczne", które odbędzie się w dniu 10 czerwca 2021 r. w godz. 10.00-14.20 w formie zdalnej z wykorzystaniem **aplikacji Zoom**.

Szkolenie organizujemy we współpracy z NASK SA.

PROGRAM SZKOLENIA

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. | www.piszcz.pl

- 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. | www.nask.pl

- 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 incydentów cyberbezpieczeństwa dotyczących sieci biurowej (IT); przemysłowej (OT) i internetu rzeczy IoT.
Źródła, narzędzia, przykłady incydentów i sposobów zabezpieczania się przed nimi.
Piotr Jagielski, Menedżer Produktów Cybersecurity, NASK SA. | www.nask.pl

- Case study do panelu II – przykłady incydentów i sposobu postepowania.

ZGŁOSZENIE UDZIAŁU

W załączeniu przesyłamy kartę zgłoszenia w formacie pdf i edytowalnej docx.

Wypełnioną kartę zgłoszenia prosimy przesłać e-mailem w formie skanu pdf/jpg lub formie zamkniętej w formacie pdf do Centrum Szkoleniowego IGCP na adres e-mail: c.szkoleniowe@igcp.org.pl

! **Bardzo prosimy, aby na karcie zgłoszenia został podany adres e-mail każdego zgłoszonego uczestnika szkolenia.**

Zakwalifikowani uczestnicy otrzymają potwierdzenia, które zostaną przesłane na adresy e-mail podane na karcie zgłoszenia.

Potwierdzenia będą zawierać:

- informację o zasadach rejestracji i udziału w szkoleniu,
- instrukcję korzystania z aplikacji Zoom,
- link do pobrania materiałów szkoleniowych w formie elektronicznej w pdf.

Zakwalifikowani uczestnicy na 1 dzień przed szkoleniem otrzymają na adresy e-mail podane na karcie zgłoszenia indywidualne linki umożliwiające zalogowanie się na szkolenie.

! **W czasie szkolenia uczestnicy będą mogli zadawać prelegentom pytania na czacie, na które prelegenci będą udzielali odpowiedzi.**

Szczegółowe informacje o szkoleniach i konferencjach IGCP: www.igcp.pl

W IMIENIU ORGANIZATORÓW SERDECZNIE ZAPRASZAMY

Bogusław Regulski
Wiceprezes Zarządu IGCP

Jacek Szymczak
Prezes Zarządu IGCP