Izba Gospodarcza
Ciepłownictwo Polskie

SZKOLENIE ONLINE
2 lutego 2021

PROGRAM

Cyberbezpieczeństwo w przedsiębiorstwach ciepłowniczych

HARMONOGRAM SZKOLENIA

■ **od 9.30** **Logowanie uczestników**

■ **10.00-11.40** **Cyberbezpieczeństwo w przedsiębiorstwach ciepłowniczych od strony prawnej**

1. Podatność infrastruktury IT – cyberataki na systemy informatyczne.
2. Obowiązki przedsiębiorstw ciepłowniczych w zakresie cyberbezpieczeństwa:
   a. Przedsiębiorstwa ciepłownicze jako operatorzy usług kluczowych,
   b. Obowiązki operatorów usług kluczowych wynikające z ustawy o Krajowym Systemie Cyberbezpieczeństwa.
3. Incydent cyberbezpieczeństwa, i co dalej?
   a. Obowiązki przedsiębiorstw ciepłowniczych w zakresie reagowania na incydenty cyberbezpieczeństwa.
4. Współpraca przedsiębiorstw ciepłowniczych z organami właściwymi do spraw cyberbezpieczeństwa.
5. Odpowiedzialność przedsiębiorstw ciepłowniczych za nieprzestrzeganie przepisów dot. cyberbezpieczeństwa.

Jarosław Jerszyński | Kancelaria Prawna Doktór Jerszyński Pietras
Bartosz Góźdź | Kancelaria Prawna Doktór Jerszyński Pietras

■ **11.40-12.00** **Przerwa**

■ **12.00-14.00** **Cyberbezpieczeństwo w przedsiębiorstwach ciepłowniczych od strony praktycznej**

W połowie wykładu ok. godz. 13.00 przerwa 10 minut

1. Klasyfikacja obiektu w infrastrukturze OT.
   Zagadnienia rozumienia czym jest obiekt w infrastrukturze przemysłowej w kontekście monitorowania cyfrowego.
2. Identyfikacja obiektu.
   Zasady interpretowania danych zebranych z infrastruktury przemysłowej celem doprowadzenia do pełnej identyfikowalności wszystkich komponentów logicznych i fizycznych.
3. Źródła i ekstrakcja danych.
   Omówienie źródeł danych dla systemów monitorowania i sposoby ich wydobywania z różnych rodzajów komponentów automatyki przemysłowej z minimalizacją wpływu na ciągłość procesów technologicznych.
4. Analityka wstępna.
   Zasady analizy danych w skali całej infrastruktury przemysłowej w zakładzie.
5. Efekt „big data".
   Przybliżenie skali danych przetwarzanych przez systemy sterowania i w konsekwencji przez układy monitorowania i bezpieczeństwa.
6. Efektywność struktur HMI dla systemów cyberbezpieczeństwa.
   Interfejsy pomiędzy ludźmi a systemami cyfrowymi lub urządzeniami z punktu widzenia optymalizacji pracy zespołów SOC (zespołów ds. bezpieczeństwa).
7. Rekomendowana architektura.
   Wprowadzenie do zasad budowy rozwiązań komunikacji procesowej i serwisowej zgodnie z wymaganiami normatywnymi, dobrymi praktykami i faktycznie zrealizowanymi projektami na infrastrukturze krytycznej kraju.

Andrzej Cieślak | Prezes Zarządu, Dynacon Sp. z o.o.