kod szkolenia: PFK CS / CB_WOD_ITOT_DL

Cyberbezpieczeństwo systemów IT i OT w przedsiębiorstwach wodociągowo-kanalizacyjnych

Przedsiębiorstwa wodociągowo-kanalizacyjne odpowiadają za funkcjonowanie infrastruktury krytycznej, dlatego ich systemy informatyczne oraz przemysłowe coraz częściej stają się celem cyberataków. Skuteczna ochrona środowisk IT i OT wymaga nie tylko odpowiednich technologii, ale również znajomości obowiązujących przepisów, procedur oraz sposobów reagowania na incydenty.

Szkolenie zostało przygotowane z myślą o osobach odpowiedzialnych za bezpieczeństwo informacji, utrzymanie systemów IT i OT oraz ciągłość działania przedsiębiorstw wodociągowo-kanalizacyjnych. Program obejmuje wymagania wynikające z dyrektywy NIS2, ustawy o krajowym systemie cyberbezpieczeństwa, norm ISO oraz standardów ISA/IEC 62443. Uczestnicy poznają również zagrożenia charakterystyczne dla środowisk przemysłowych, zasady zarządzania ryzykiem oraz procedury postępowania w przypadku cyberataku.

Odbiorcy szkolenia

Szkolenie skierowane jest do:

- kadry zarządzającej przedsiębiorstw wodociągowo-kanalizacyjnych,
- administratorów systemów IT,
- administratorów i operatorów systemów OT,
- osób odpowiedzialnych za cyberbezpieczeństwo,

- specjalistów ds. bezpieczeństwa informacji,
- pracowników działów IT i automatyki przemysłowej,
- osób odpowiedzialnych za zgodność z wymaganiami NIS2 i KSC,
- audytorów bezpieczeństwa,
- osób odpowiedzialnych za zarządzanie ryzykiem i ciągłość działania.

Korzyści

Po ukończeniu szkolenia uczestnik:

- rozumie wymagania prawne dotyczące cyberbezpieczeństwa przedsiębiorstw wodociągowo-kanalizacyjnych,
- zna zasady ochrony systemów IT i OT,
- potrafi identyfikować podatności i analizować ryzyko,
- rozumie zależności pomiędzy środowiskami IT i OT,
- potrafi przygotować procedury reagowania na incydenty,
- zna dobre praktyki zabezpieczania infrastruktury przemysłowej,
- potrafi współpracować z zespołami odpowiedzialnymi za cyberbezpieczeństwo,
- zwiększa poziom odporności organizacji na cyberzagrożenia.

Program szkolenia

Moduł I. Wymagania prawne i organizacja cyberbezpieczeństwa

- wymagania wynikające z dyrektywy NIS2, ustawy o krajowym systemie cyberbezpieczeństwa oraz obowiązujących norm,
- obowiązki podmiotów kluczowych i ważnych,
- organizacja systemu zarządzania bezpieczeństwem informacji,
- role i odpowiedzialności w zakresie cyberbezpieczeństwa,
- analiza ryzyka,
- audyty, testy oraz ocena skuteczności wdrożonych zabezpieczeń.

Moduł II. Bezpieczeństwo systemów OT w przedsiębiorstwach wodociągowo-kanalizacyjnych

- środowiska SCADA, HMI oraz PLC wykorzystywane w przedsiębiorstwach wodociągowych,
- podstawowe wymagania bezpieczeństwa systemów OT,
- współpraca środowisk IT i OT,
- zagrożenia wynikające z integracji systemów,
- zarządzanie podatnościami oraz aktualizacjami.

Moduł III. Cyberzagrożenia dla infrastruktury wodociągowej

- przykłady ataków na systemy przemysłowe oraz infrastrukturę krytyczną,

- phishing, ransomware, BEC i inne współczesne zagrożenia,
- wektory ataku na systemy OT,
- narzędzia wspierające ochronę środowisk przemysłowych,
- działania ograniczające skutki cyberataków,
- zmiany konfiguracji oraz aktualizacja planów DRP i BCP.

Moduł IV. Reagowanie na incydenty cyberbezpieczeństwa

- procedury reagowania na incydenty,
- role i odpowiedzialności w organizacji,
- współpraca z SOC,
- analiza incydentów,
- eskalacja zdarzeń,
- obowiązki związane z powiadamianiem właściwych organów,
- analiza przyczyn incydentów oraz wdrażanie działań zapobiegawczych.

Oczekiwane przygotowanie uczestnika

Szkolenie nie wymaga specjalistycznej wiedzy z zakresu cyberbezpieczeństwa. Podstawowa znajomość funkcjonowania systemów IT lub OT będzie dodatkowym atutem i ułatwi wykorzystanie zdobytej wiedzy w praktyce.

Czas trwania

1 dni / 3 godzin

Język

polski