Cyberbezpieczeństwo wodociągów

Jakie cyberataki mogą wystąpić w przedsiębiorstwach wodociągowych - jak wykrywać i zapobiegać? Skąd i jak otrzymać dofinansowanie w zakresie cyberbezpieczeństwa? Jak zabezpieczyć dane w przypadku ataku? Jakie elementy sieci poza ujęciami i zbiornikami wymagają szczególnej ochrony?

Wideoszkolenie PCC Poland skierowane do podmiotów, które prowadzą działalność w zakresie zbiorowego zaopatrzenia w wodę i jednostek sektora finansów publicznych: dla przedsiębiorstw wodociągowo-kanalizacyjnych, zakładów wodociągów i kanalizacji, zakładów gospodarki komunalnej, pracowników urzędów miast i gmin, wydziałów gospodarki komunalnej oraz związków międzygminnych, spółek wodnych, oczyszczalni ścieków, stacji uzdatniania wody, a także do osób, które zajmują się cyberbezpieczeństwem wodociągów. Szczególnie zapraszamy informatyków, realizujących zadania wynikające z Ustawy o KSC i osoby zaangażowane w projekt “Cyberbezpieczne Wodociągi”.

Jakie są wytyczne wniosku o dofinansowanie z cyberbezpieczeństwa? Jakie normy trzeba spełnić, żeby otrzymać dofinansowanie?

Szkolenie obejmuje obszar cyberbezpieczeństwa w wodociągach, nowe obowiązki prawne, w tym NIS2 oraz praktyczne zagadnienia związane z analizą ryzyka, wdrażaniem zabezpieczeń, backupem i ochroną infrastruktury IT i OT. Omówione zostaną m.in. kwestie zabezpieczania infrastruktury fizycznej i systemów sterowania, organizacji sieci w rozproszonych lokalizacjach, ochrony danych (lokalnie i w chmurze), reagowania na cyberataki oraz zasady współpracy z podmiotami zewnętrznymi. Ważnym elementem programu są także możliwości uzyskania i rozliczenia dofinansowania. Szkolenie ma charakter praktyczny i odpowiada na pytanie, jakie konkretne działania powinno podjąć przedsiębiorstwo wodociągowe, aby spełnić wymagania prawne, ograniczyć ryzyko cyberataków i zapewnić ciągłość dostaw wody.

W programie m.in.:

- Jakie formy ataku mogą być wykorzystane w cyberprzestrzeni wobec przedsiębiorstw wodociągowych?
- Jakie zmiany w cyberbezpieczeństwie wprowadzi dyrektywa NIS2?
- Na co zwrócić uwagę we wniosku o dofinansowanie? Co jest punktowane i klasyfikowane?
- Co należy chronić w pierwszej kolejności, aby skutecznie przeciwdziałać atakom i zagrożeniom dla ciągłości dostaw wody?
- Jak zabezpieczać serwery pod kątem połączeń internetowych?
- Gdzie powinny być przechowywane kopie danych?
- Jak chronić stacje uzdatniania wody i ujęcia wody, jeśli są podłączone pod internet?

Szczegółowy program szkolenia:

1. Cyberbezpieczeństwo w wodociągach – czym jest i czego dotyczy w praktyce?

- Na co zwracać uwagę przy komputerze w odniesieniu do cyberbezpieczeństwa?
- Jakie dane w wodociągach wymagają szczególnej ochrony?
- Jakie są teoretyczne zagrożenia dla małych wodociągów?
- Jakie zagrożenia mogą wystąpić w przedsiębiorstwach wodociągowych?
- Czy przedsiębiorstwa wodociągowe mogą zostać zaatakowane zdalnie?
- Jakie formy ataku mogą być wykorzystane w cyberprzestrzeni wobec przedsiębiorstw wodociągowych?
- Czym jest cyberbezpieczeństwo? Na czym polega?
- Czego dotyczy cyberbezpieczeństwo w praktyce działalności spółek wodociągowych?
- Jakie są rodzaje cyberbezpieczeństwa?
- Jakie zagrożenia mogą wystąpić w cyberbezpieczeństwie?

2. Obowiązki prawne i nowe regulacje (NIS2, prawo krajowe, normy)

- Czy muszą być oddzielne serwery zabezpieczeń według dyrektywy unijnej?
- Jakie przepisy unijne są wdrażane, jeżeli chodzi o bezpieczeństwo?
- Jakie zmiany w cyberbezpieczeństwie wprowadza dyrektywa NIS2 dla przedsiębiorstw wodociągowych?
- Jakie obowiązki w zakresie cyberbezpieczeństwa muszą spełnić wodociągi?
- Jakie wymogi są związane z cyberbezpieczeństwem?
- Jakie wymagania w zakresie cyberbezpieczeństwa dotyczą wodociągów?
- Jakie są minimalne wymagania, które wodociągi muszą spełnić?
- Jakie wymagania unijne w zakresie zabezpieczeń dotyczą przedsiębiorstw wodociągowych?
- Jakie są wymogi prawne dotyczące wprowadzenia rozwiązań z zakresu cyberbezpieczeństwa?
- Jakie kary mogą wystąpić za niewdrożenie cyberbezpieczeństwa?
- Kto będzie egzekwował kary?
- Jakie podstawowe wymagania w zakresie cyberbezpieczeństwa muszą spełniać przedsiębiorstwa wodociągowe?
- Z jakich przepisów prawa wynikają obowiązki dotyczące cyberbezpieczeństwa?
- Jakie są podstawy prawne cyberbezpieczeństwa w Polsce i Unii Europejskiej?
- Jakie normy i przepisy techniczne obowiązują w zakresie cyberbezpieczeństwa? Czy pojawiły się nowe regulacje?
- W jaki sposób należy wdrażać procedury i systemy zgodnie z tymi przepisami prawa?

3. Analiza ryzyka i plan wdrożenia cyberbezpieczeństwa

- Jak powinien wyglądać plan ciągłości działania w przypadku ataku?
- Jakie grupy pracowników wodociągów powinny być objęte podnoszeniem kompetencji w zakresie cyberbezpieczeństwa?
- Jak ma być wdrażane cyberbezpieczeństwo? Czy to będą kursy dotyczące zasad bezpieczeństwa i higieny pracy, oprogramowania bezpieczeństwa, zabezpieczenia sieci automatyki przemysłowej?
- Jak wodociągi mają się dostosować do wymagań?
- Jak zachować ciągłość procesów, aby nie doszło do przerwy w dostawie wody?
- Co należy chronić w pierwszej kolejności, aby skutecznie przeciwdziałać atakom i zagrożeniom dla ciągłości dostaw wody?
- Jak wdrażać rozwiązania, aby były zgodne z przepisami prawa o cyberbezpieczeństwie?

- Co w sytuacji, gdy w przedsiębiorstwie wodociągowym część infrastruktury jest obsługiwana ręcznie, a planowana jest budowa systemu cyberbezpieczeństwa?
- Jakie działania trzeba podjąć w procesie wdrażania cyberbezpieczeństwa? Czy trzeba się kontaktować z gminą?
- Co mają zrobić małe przedsiębiorstwa wodociągowe, jeśli programy dedykowane są do dużych przedsiębiorstw wodociągowych?
- W jaki sposób można określać obszary, w których występują problemy związane z cyberbezpieczeństwem? W jaki sposób te problemy powinny być prawidłowo definiowane?
- Gdzie szukać w danej jednostce wystąpienia ryzyka i zagrożenia?

4. Dofinansowanie na cyberbezpieczeństwo

- Jakie przedsiębiorstwa mają możliwości pozyskania dofinansowania na cyberbezpieczeństwo?
- Jakie środki można pozyskać w dofinansowaniu?
- Jakie elementy infrastruktury mogą zostać sfinansowane w ramach środków zewnętrznych? Co kupić i jak doposażyć wodociągi, by podnieść stopień bezpieczeństwa?
- Jakie rodzaje dofinansowań mogą dotyczyć cyberbezpieczeństwa?
- Kiedy pomocą zostaną wsparte przedsiębiorstwa wodociągowe, które nie mają żadnych zabezpieczeń?
- Czy przedsiębiorstwa wodociągowe, które nie mają podstawowych zabezpieczeń, mogą ubiegać się o dofinansowanie?
- Jakie działania w obszarze cyberbezpieczeństwa mogą być objęte dofinansowaniem? Co może być dofinansowane?
- Czy monitoring i systemy bezpieczeństwa są podstawą do ubiegania się o dofinansowanie?

4a. Wymogi formalne i dokumentacja wniosków

- Jak powinien wyglądać wniosek o dofinansowanie, jeżeli chodzi o cyberbezpieczeństwo?
- Jak prawidłowo wypełnić wniosek o dofinansowanie? Co w nim zawrzeć?
- Jak wygląda wzór wniosku o dofinansowanie?
- Na co zwrócić uwagę we wniosku o dofinansowanie? Co jest punktowane i klasyfikowane?
- Co konkretnie ma być ujęte we wniosku o dofinansowanie w zakresie cyberbezpieczeństwa?
- Jakie są wytyczne wniosku o dofinansowanie z cyberbezpieczeństwa?
- Jakie szczegółowe warunki techniczne powinny być wyszczególnione we wniosku o dofinansowanie?
- Jakie normy trzeba spełnić, żeby otrzymać dofinansowanie? Jakie są normy?
- Jakie procedury obowiązują przy reprezentacji dwuosobowej, jeśli regulamin dofinansowania umożliwia podpisanie wniosku tylko przez jedną osobę?

4b. Proces pozyskiwania środków i źródła finansowania

- Kto powinien finansować działania związane z cyberbezpieczeństwem w wodociągach? Kto będzie za to płacił?
- Skąd przedsiębiorstwa wodociągowe mają pozyskiwać środki finansowe na cyberbezpieczeństwo?
- Skąd wziąć pieniądze na modernizacje i wprowadzenie podstaw cyberbezpieczeństwa?
- Jak można uzyskać dofinansowanie? Jaka jest ścieżka w tym procesie?
- Jak pozyskać nowe fundusze zewnętrzne na cyberbezpieczeństwo?

- Od czego rozpocząć proces ubiegania się o środki zewnętrzne?
- Gdzie szukać środków zewnętrznych?
- Jakie koszty mogą wiązać się z wdrożeniem rozwiązań z zakresu cyberbezpieczeństwa?

4c. Rozliczenie i monitorowanie inwestycji

- W jaki sposób należy prawidłowo rozliczać inwestycje związane z cyberbezpieczeństwem?
- Jaki jest sposób rozliczenia wniosków o dofinansowanie?
- Jak ma wyglądać rozliczenie wniosków o dofinansowanie? Czy rozliczenie następuje po wykonaniu zadań, czy w trakcie ich realizacji?
- Jak ma wyglądać procedura rozliczenia?
- Jakie są terminy rozliczenia?
- Jaka dokumentacja jest potrzebna do rozliczenia projektu?
- Jak utrzymać monitoring, serwery i systemy nadzoru? Czy możliwe jest finansowanie z funduszy unijnych, krajowych?
- Jak rozpatrywane są wnioski o dofinansowanie?

4d. Kolejne kroki po otrzymaniu dofinansowania

- Co dalej po otrzymaniu dofinansowania? Jakie są następne kroki?
- Jak wygląda etap podpisania umowy o cyberbezpieczeństwie? Jakie dane są potrzebne i na jakie dane oczekujemy?

5. Reagowanie na incydenty i sytuacje kryzysowe. Reagowanie na incydent – co robić w przypadku ataku?

- Jak postępować w przypadku ataku?
- Jakie procedury i działania należy podjąć w przypadku ataku?
- Jak w przypadku ataku powinny wyglądać procedury, które jednoznacznie określają, co w danej sytuacji zrobić?
- Kto jest odpowiedzialny za podjęcie działań w przypadku ataku?
- Jak określić zakres obowiązków poszczególnych osób w przypadku ataku?
- Co zrobić, żeby ograniczyć rozprzestrzenianie się ataku w systemach wodociągowych?
- Jakie są możliwości jak najszybszego odbudowania infrastruktury po ataku?
- Jak zachować się w przypadku skażenia wody?
- Jak zapewnić dostęp do danych w przypadku ataku?
- Co zrobić w sytuacji, gdy haker zmieni hasło lub przyblokuje serwer?
- Jak zapewnić ciągłość dostępu do danych?
- Co zrobić w sytuacji zakłócenia pracy systemu, który steruje i odpowiada za wyłączenie pomp, opróżnienie zbiorników?
- Jak postąpić w sytuacji, gdy utracone zostaną dane umieszczone w chmurze, takie jak dane klientów, dane klientów powiązane z danym wodomierzem, historia transakcji, dane osobowe, dane księgowe?
- Co zrobić w przypadku kontroli urzędu skarbowego, a dane klientów i informacje zostały utracone?
- Jak wykryć zagrożenie i jakie działania należy podjąć w odpowiedzi? Czy odłączyć urządzenie, wprowadzić blokadę czy inne procedury reagowania?
- W przypadku podejrzenia ataku na systemy wodociągowe, co należy zrobić i komu zgłosić incydent?

- W jaki sposób można wykryć zagrożenie?
- Jak odróżnić, czy zakłócenia w działaniu urządzeń np. manipulacja parametrami, ustawienia na maksymalne wartości są wynikiem awarii sprzętowej czy cyberataku?
- Jak wykryć cyberatak? Jak można się dowiedzieć, czy to cyberatak?

6. Serwery i systemy IT – architektura i konfiguracja

- W jakim celu stosuje się oddzielne serwery i oddzielne połączenia w systemach cyberbezpieczeństwa wody?
- Jakie urządzenia techniczne i systemy informatyczne powinny być zakupione w celu zapewnienia bezpieczeństwa sieci wodociągowej?
- Jakie urządzenia mogą być zakupione w ramach dofinansowania na cyberbezpieczeństwo?
- Jakie urządzenia warto zastosować, aby zwiększyć bezpieczeństwo wodociągów?
- Jak zabezpieczać serwery pod kątem połączeń internetowych?
- Które urządzenia końcowe mogą generować ryzyko dla bezpieczeństwa systemów?
- Czy serwery powinny być replikowane w celu zwiększenia bezpieczeństwa?
- Czy powinny być dwa serwery w celu zwiększenia bezpieczeństwa?
- Jak w urządzeniu FortiGate (7.6) prawidłowo ustalić tunel GRE IPsec do urządzeń CISCO?
- Jakie rodzaje serwerów są stosowane w przedsiębiorstwach wodociągowych? Jakie serwery są dostępne?

7. Backup, kopie zapasowe i przechowywanie danych

- Jak często należy wykonywać kopie zapasowe systemów?
- Gdzie powinny być przechowywane kopie danych?
- Jak zabezpieczyć dane na wypadek ataku cybernetycznego?
- Jak powinien wyglądać harmonogram wykonywania kopii zapasowych? Co ile czasu powinno się je robić?
- Jak tworzyć kopię bezpieczeństwa? Czy wykonać ją od razu, czy stopniowo?
- Ile kopii zapasowych należy tworzyć?
- W jaki sposób przechowywać kopie? Czy wystarczy zapis na dysku lokalnym, czy należy je szyfrować?

8. Ochrona infrastruktury OT i fizyczna

- Czy samo ogrodzenie hydroforni jest wystarczającym zabezpieczeniem? Czy obowiązkowy jest monitoring?
- Jak zabezpieczyć systemy uzdatniania wody przed osobami niepożądanymi?
- Jak chronić fizycznie studnie i inne obiekty wodociągowe?
- Jak zabezpieczyć infrastrukturę na wypadek pożaru?
- Jakie środki fizycznego zabezpieczenia są wymagane dla szaf i urządzeń?
- Jakie elementy sieci poza ujęciami i zbiornikami wymagają ochrony?
- Jakie rozwiązania można zastosować, aby hydrant był chroniony, ale nadal dostępny dla straży pożarnej?
- Czy hydranty powinno się zabezpieczać?
- Czym zabezpieczyć hydranty?

- Jak zabezpieczyć sieci wodociągowe?
- Jaką dokumentację dotyczącą zabezpieczeń powinno posiadać przedsiębiorstwo wodociągowe?

9. Sieci, połączenia i infrastruktura rozproszona

- Jak prawidłowo zabezpieczyć i połączyć kilka lokalizacji w jedną spójną strukturę sieciową przy wykorzystaniu urządzeń brzegowych?
- Czy w sytuacji, gdy jedna z lokalizacji posiada światłowód, a pozostałe mają słabsze łącza, warto wprowadzać wdrożenie serwera domenowego?
- Co w sytuacji utraty łączności z internetem i potencjalnego odcięcia biura od dostępu do domeny? Jak to rozwiązać?
- W jaki sposób może się uszkodzić łącze sieciowe w przypadku cyberbezpieczeństwa?
- Jakie mogą być systemy i rozwiązania dla przedsiębiorstw wodociągowych, jeżeli ręcznie obsługują zawory?

10. Systemy, oprogramowanie i praktyczne rozwiązania IT

- Jakie są dostępne systemy i programy w cyberbezpieczeństwie?
- Na czym polega zabezpieczanie systemów teleinformatycznych?
- Jakie będą nowe systemy zarządzania wodą w cyberbezpieczeństwie?
- Jakie oprogramowania i sprzęt są rzeczywiście niezbędne do spełnienia wymagań o cyberbezpieczeństwie?
- Jak odróżnić rozwiązania podstawowe od zaawansowanych?
- Jakie jest najlepsze oprogramowanie? Czy od wersji 11?
- Jakie są rozwiązania w cyberbezpieczeństwie kierowane dla mniejszych przedsiębiorstw wodociągowych?
- Jak chronić sieć do sterowania urządzeń? Jakie są konkretne i praktyczne rozwiązania?

11. Cyberbezpieczeństwo a jawność i chmura

- Jak należy zabezpieczyć przed atakami system działający w chmurze, do którego dostęp odbywa się za pomocą loginu i hasła, gdy infrastrukturą i serwerami zarządza firma zewnętrzna?
- Czy ogólnodostępne informacje np. z geoportalu, dotyczące przebiegu sieci wodociągowej mogą stanowić zagrożenie dla bezpieczeństwa infrastruktury?
- Jak minimalizować ryzyko wynikające z jawności części informacji o infrastrukturze?
- Jak chronić stacje uzdatniania wody i ujęcia wody, jeśli są podłączone pod internet?
- Co w sytuacji, gdy część danych znajduje się w chmurze, a część na własnym serwerze? Co może się stać z danymi w chmurze, jeśli będą z nich korzystać użytkownicy w warunkach braku połączenia sieciowego lub internetu?

12. Zarządzanie i narzędzia IT/OT dla informatyków

- Jakich narzędzi, systemów i zasobów potrzebują informatycy, aby skutecznie wdrożyć cyberbezpieczeństwo w przedsiębiorstwie wodociągowym?
- Jak zabezpieczyć dane bazy klientów, w tym dane osobowe i historię rozliczeń?
- Jak zapobiec utracie danych klientów?

- Jak zabezpieczyć system sterowania, aby nikt nie miał do niego dostępu oprócz osoby uprawnionej?
- Jak monitorować sieci OT? Jakie programy i narzędzia mogą w tym pomóc?
- Jak zabezpieczyć sieci OT? Co musimy zrobić?
- Jakie typy switchy przemysłowych są dopuszczalne do stosowania, a których należy unikać?
- Jakie nowe sprzęty i aplikacje warto wprowadzić, aby zapewnić odpowiedni poziom bezpieczeństwa?
- Jak obszary problemowe w cyberbezpieczeństwie można przełożyć na konkretne rozwiązania techniczne?
- Gdzie i w jaki sposób definiować zapory?

13. Współpraca z podmiotami zewnętrznymi i SOC

- Co w sytuacji wymiany danych? Co jest po stronie przedsiębiorstwa wodociągowego a co po stronie Operation Security Center?
- Czy podmioty zajmujące się wodociągami będą mogły liczyć na integrację z Operation Security Center? Czy będą musiały polegać na rozwiązaniach komercyjnych? Jakie są plany z tym związane?
- Jaka jest rola firm zewnętrznych w procesie cyberbezpieczeństwa?

Prowadzący:

Od 15 lat pracuje jako informatyk, inspektor ochrony danych osobowych w firmach prywatnych, urzędach gmin, jednostkach służby zdrowia, szkołach i innych jednostkach samorządowych. Dodatkowo zajmuje się tematyką cyberbezpieczeństwa dla klientów kancelarii prawnej w Krakowie. Prowadził i prowadzi projekty finansowane z środków unijnych, państwowych i własnych jednostek samorządowych. Zajmuje stanowiska specjalistyczne i kierownicze dotyczące organizacji pracy techniczno – informatycznej w organizacjach. Absolwent studiów II stopnia (systemyCAD/CAE) na Politechnice Świętokrzyskiej w Kielcach.

Posiada dyplomy z: organizacji i zarządzania w ochronie zdrowia, zarządzania zasobami ludzkimi, Inspektor Ochrony Danych i Executive Master of Business Administration (EMBA). Ponadto posiada doświadczenie w pracy w firmach powyżej 650 pracowników, ciągły rozwój osobisty w kierunkach związanych z szeroko pojętą informatyką. Certyfikat Audytora Wiodącego Systemu Zarządzania Bezpieczeństwem Informacji wg Normy PN-EN ISO/IEC 27001 – Polskie Centrum Akredytacji. Certyfikat ERCA: Auditor Wiodący ISO/IEC 27001:2022 CeCert.

Prawa autorskie do niniejszego programu przysługują Private Corporate Consulting Sp. z o.o. Udostępnianie, kopiowanie i przerabianie niniejszego programu bez pisemnej zgody Private Corporate Consulting Sp. z o.o., zagrożone jest odpowiedzialnością karną oraz cywilną