Cyberbezpieczeństwa nie wolno chować do szuflady

Zaopatrzenie w wodę i odprowadzanie ścieków jest jedną z najważniejszych usług komunalnych, od których zależy życie i zdrowie obywateli. Dlatego nikogo nie powinno dziwić, że branża wod-kan została objęta unijnymi regulacjami dotyczącymi cyberbezpieczeństwa, wprowadzonymi przepisami Dyrektywy NIS. W Polsce ich stosowanie opiera się na przepisach ustawy o krajowym systemie cyberbezpieczeństwa, która obowiązuje od 28 sierpnia 2018 r. Jakie obowiązki nałożyły nowe przepisy?

Najwięcej zadań doszło przedsiębiorstwom działającym w dużych aglomeracjach (przekraczających 500 tys. RLM lub 500 tys. podłączonych mieszkańców). Musiały one zorganizować cały system zarządzania bezpieczeństwem w swoich systemach informacyjnych. Wiązało się to z przygotowaniem i wdrożeniem polityk i procedur zapewniających nie tylko niezakłóconą pracę systemów, ale również rozwiązań organizacyjnych i technicznych, zwiększających bezpieczeństwo zgromadzonych w nich danych. Mniejsze przedsiębiorstwa musiały wdrożyć „tylko" informowanie swoich klientów o zagrożeniach cyberbezpieczeństwa, zarządzanie incydentami i ich zgłaszanie przez wskazaną do zadania osobę do wyznaczonych przepisami podmiotów, czyli Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym (art. 2 pkt. 1–3 Ustawy o KSC) (ang. CSIRT).

Biorąc pod uwagę, że pod tymi kilkunastoma słowami kryje się cały szereg działań obejmujących wykrywanie, rejestrowanie, analizę i podejmowanie działań naprawczych i zapobiegawczych, tak naprawdę cała branża wod-kan w Polsce musiała zweryfikować i zoptymalizować swoje działania dotyczące cyberbezpieczeństwa. Co można było zrobić, żeby nie utknąć w papierach i nie zakłócić normalnej pracy ludzi?

Cyberbezpieczeństwo rozumiane „po swojemu"

Często funkcjonuje błędne przekonanie, że cyberbezpieczeństwo to tylko kwestia ochrony danych na laptopach osób pracujących z domu czy serwerach, z którymi można połączyć się za pośrednictwem Internetu. Kwestia „e-bezpieczeństwa" jest również utożsamiana z problemami takimi jak unikanie scammingu (podawania danych na fałszywych stronach w sieci) czy phishingu (klikania w wiadomości e-mail wyłudzające dane).

Wbrew obiegowej opinii cyberbezpieczeństwo w przedsiębiorstwach wodociągowo-kanalizacyjnych dotyczy nawet bardziej infrastruktury sieci wod-kan i automatyki przemysłowej niż aktywności biurowej. Żeby dobrze wykonać obowiązki wynikające z przepisów, wystarczy być dobrze przygotowanym i mieć skuteczny system wykrywania i reagowania na incydenty. Problemy zaczynają się, kiedy pada pytanie, jak to w praktyce zrobić i co tak naprawdę znaczy „dobrze". Dołożenie obowiązków dyspozytorom czy utworzenie jednego nowego stanowiska, które ma realizować wszystkie nowe obowiązki to prosty przepis na katastrofę. Część działań związanych z bezpieczeństwem systemów informacyjnych oczywiście była i jest już realizowana, chociaż nie zawsze nazywa się je

„cyberbezpieczeństwem”. To kto i co dokładnie robi w dużej mierze zależy od specyfiki organizacji pracy w przedsiębiorstwie. Na podział zadań mocno wpływa historia firmy i kompetencje pracowników, z których wielu pracuje na swoich stanowiskach od kilkunastu, kilkudziesięciu lat.

Dlatego komunikat „od teraz będziesz się zajmował/zajmowała cyberbezpieczeństwem”, to za mało, żeby nakłady na zgodność z przepisami prawa miały szansę się zwrócić. W ten sposób można osiągnąć w najlepszym razie formalną zgodność z przepisami. Łatwo też zdublować już wykonywaną pracę albo dociążyć osobę, która faktycznie nie będzie w stanie wykonać dodatkowych działań. Dlatego nie ma sensu wymyślać koła na nowo. Trzeba dobrze ustalić, jakie obowiązki nakłada Ustawa o KSC i jakich systemów ma dotyczyć. Pozwoli to zweryfikować, kto już zajmuje się tymi systemami, ma faktyczną wiedzę i możliwości, by zapewnić właściwą realizację takich zadań. Jeżeli każdy zrobi to, na czym się zna, może się okazać, że bez dużego wysiłku duża część dodatkowej pracy zostanie wykonana bez pracy w nadgodzinach lub kosztownego powiększania zespołu.

Jest jeszcze jeden ważny aspekt: skuteczne funkcjonowanie przedsiębiorstwa opiera się na właściwych zasadach działania. Skuteczność pogotowia wodociągowo-kanalizacyjnego wynika z tego, że właściwi ludzie są na właściwym miejscu, a awarie usuwają osoby, które naprawdę znają się na swojej pracy. Nie potrzebują instrukcji grubości książki telefonicznej, żeby zlokalizować problem i go zlikwidować. Tak samo jest z cyberbezpieczeństwem. Najsłabszym ogniwem w bezpieczeństwie systemów na ogół jest ich użytkownik. Dlatego zamiast zakupu najdroższych zabezpieczeń technicznych i wymiany wszystkich urządzeń, często niedocenianym sposobem na cyberbezpieczeństwo pozostaje zwiększenie świadomości pracowników i odpowiednie dostosowanie procedur. Nie warto ich jednak tworzyć na bazie „gotowców z internetu”, tylko spersonalizowanej analizy specyfiki działania i potrzeb konkretnego przedsiębiorstwa i osób, które odpowiadają za jego prawidłowe funkcjonowanie. W tym obszarze przedsiębiorstw po prostu długofalowo nie stać na działanie „po taniości”.

Skutki zaniedbań da się obliczyć

Zarządzanie wydatkami na cyberbezpieczeństwo musi być przemyślane. Przedsiębiorstwa wodociągowo-kanalizacyjne powinny zabezpieczać swoje systemy nie tylko dlatego, że to pozwoli im normalnie funkcjonować. Chodzi również o wpływ na otoczenie, w którym funkcjonują. Wyobraźmy sobie, co się stanie, jeżeli połowa miasta zatruje się wodą z kranu. Albo jak przebiega zastępcza dostawa wody i jak długo można ją realizować, żeby mieszkańcy mogli w miarę normalnie żyć. Takie zdarzenia to konkretne skutki, które mają swoją cenę.

Cyberataki w ostatnich latach bardzo się intensyfikują, zwłaszcza ze względu na epidemię Covid-19 i elektronizację codziennego życia. Większość z nich ma jeden cel – zakłócić normalne funkcjonowanie – dla zabawy, dla pieniędzy lub żeby wykraść informacje gospodarcze czy też dotyczące bezpieczeństwa państwa. Skutki wyłączenia systemów można przeliczyć na utracone przychody, koszty walki ze skutkami ataków czy rozliczenia z poszkodowanymi. Jednak w działalności komunalnej nigdy nie chodzi wyłącznie o pieniądze, które trzeba wydać na odszkodowania czy odbudowę infrastruktury. Przede

wszystkim chodzi o ludzi, na których wpłynie incydent, ich życie, zdrowie czy ochronę środowiska, w jakim funkcjonują. To ogromna odpowiedzialność, którą trudno przeliczyć na pieniądze, a która leży u podstaw funkcjonowania każdej spółki komunalnej.

Złudne poczucie bezpieczeństwa

Działalność wodno-kanalizacyjna jest realizowana w skomplikowanej infrastrukturze przemysłowej. W przypadku starszych rozwiązań zarządzanie aparaturą na ujęciach wody czy pracą sieci wodociągowej bazowało w dużej mierze na rozwiązaniach hydraulicznych i prostej wymianie danych „po kablu", na zasadzie syreny alarmowej.Z każdym rokiem, kolejne modernizacje wprowadzają jednak coraz więcej automatyki i elektronicznych „gadżetów". Odczyty z urządzeń można sprawdzać na smartfonach i tabletach. W przypadku liczników zdalnego odczytu coraz częściej taka forma dostępu do informacji jest oferowana również odbiorcom. Serwisanci dokonują coraz większej liczby napraw zdalnie, z centrum serwisowego i bez konieczności dojazdu na miejsce. Dlatego poczucie bezpieczeństwa, wynikające z błędnego przekonania, że urządzenia nie mają miejsc styku z Internetem, jest bardzo złudne. Sprzęt w systemach przemysłowych może przecież przetwarzać i wymieniać ze sobą dane na różne sposoby – również drogą radiową, sygnałami optycznymi, GPRS czy GSM.

Często umyka fakt, że aktualizacje oprogramowania, które pozwalają zarządzać pracą instalacji, odbywają się automatycznie, bezpośrednio ze strony internetowej producenta albo poprzez instalację z pendrive, podłączonego wcześniej do komputera z dostępem do internetu. Czyli złośliwe oprogramowanie nie od razu, ale może dotrzeć do serca systemu przemysłowego. Poza tym w urządzeniach rozsianych po sieci wodociągowo-kanalizacyjnej znajduje się też oprogramowanie (sterowniki czy interfejsy) pozwalające na podłączenie urządzeń inkasentów, sprzętu serwisantów czy też wysyłające określone dane do dyspozytora sieci lub odbiorcy.

Zmiana fabrycznego hasła do logowania do systemów czy urządzeń? Po co, skoro szafa, w której fizycznie znajduje się urządzenie, jest tak głęboko schowana, a login „admin" i hasło „1234", które ustawił producent, tak dobrze zapada w pamięć. Niestety, ta luka bezpieczeństwa jest dobrze znana przestępcom. Patrząc na jednostajną pracę pompy na ujęciu wody czy parametry pracy oczyszczalni w pokoju dyspozytora, łatwo zapomnieć, że obok świata fizycznego, w którym zdarzają się kradzieże pokryw studzienek kanalizacyjnych i wycinanie rur na złom, istnieje też świat wirtualny. Bardziej nieuchwytny, ale nie mniej brutalny, bo pozwalający na dostęp do magicznego „czerwonego przycisku", który jednym kliknięciem pozwoli wszystko wyłączyć albo zepsuć w ułamku sekund, i to bez konieczności wyjścia na instalację. Trudno to sobie wyobrazić?

Jeszcze w 2017 r. na jednej z najbardziej znanych konferencji dla „legalnych hakerów" organizowanej w San Fransisco, zaprezentowano analizę szkodliwego oprogramowania atakującego sterowniki PLC w infrastrukturze wod-kan. Tego typu sterowniki są używane do dziś (mimo że protokół RTC zastępuje coraz częściej GSM), a sterują m.in. pracą pomp, kontrolą parametrów ścieków, dozowaniem chloru czy innych substancji dodawanych w procesie uzdatniania wody czy oczyszczania ścieków, czyli na dobrą sprawę tym wszystkim, co zgodnie z art. 6 ust. 3 pkt. 1 Ustawy o zbiorowym zaopatrzeniu w wodę

i zbiorowym odprowadzaniu ścieków wyznacza dotrzymanie parametrów jakościowych określonych w umowie z odbiorcą. Złośliwe oprogramowanie „Logic Locker" pozwalało już wtedy na przejęcie kontroli nad sterownikiem PLC, a przez zmianę hasła dostępu odbierało możliwość sterowania jego pracą dyspozytorowi. Zafałszowywało również informacje wyświetlane na ekranie prezentującym parametry pracy instalacji.

Z punktu widzenia zmian technologicznych od konferencji w San Francisco minęło sporo czasu, jednak infrastruktura wodociągowa i kanalizacyjna nadal pada celem ataków hakerów. Częściowo zmodyfikowali oni technologie, jednak ich sposób działania zasadniczo się nie zmienił. Przykładem może być ostatni atak na pompy wody w Izraelu (2020). Liczba ataków wzrasta. W samych tylko USA, w 2019 r. wodociągi podały ofiarą złośliwego oprogramowania szyfrującego 22 razy, a są to dane dotyczące tylko zgłoszonych, a więc poważnych incydentów. Najbardziej przerażające jest to, że większość z tych ataków bazuje na bardzo dobrym zrozumieniu specyfiki działania infrastruktury wodociągowo-kanalizacyjnej, co wskazuje na długi czas zbierania informacji o atakowanym. Wiele z nich może też niestety pozostać niewykryta.

Co zrobić, żeby dobrze zacząć wdrażać cyberbezpieczeństwo?
Podatność na cyberzagrożenia w znacznej mierze wynika z braku wiedzy o tym, co składa się na wykorzystywaną infrastrukturę. Nie chodzi jednak o znajomość samych instalacji i trybie ich codziennej pracy, ale raczej specyfikację wchodzących w ich skład urządzeń i systemów. Zdarza się, że nowe mechanizmy nie są w ogóle wykorzystywane – urządzenie może być online, ale nikt go w tym celu specjalnie nie konfiguruje. Dlatego łatwo zapomnieć, żeby sprawdzić, czy nieużywane funkcje na pewno są zablokowane lub wyłączone. Nie można mówić więc o pełnej świadomości, co tak naprawdę funkcjonuje i w jaki sposób, bez ustalenia wszystkich wysyłanych w przedsiębiorstwie danych i stosowanych sposobów ich wykorzystania. Takie braki będą skutkowały problemami przy zapewnieniu właściwych zabezpieczeń.

Przedsiębiorstwa wodociągowo-kanalizacyjne często wykorzystują systemy zarzadzania jakością czy środowiskiem. Cyberbezpieczeństwo można budować na bazie już wypracowanego podejścia. Tworzenie procedur powinno przebiegać „od ogółu do szczegółu", zgodnie z zasadą „mniej znaczy sprawniej".

Paradoksalnie wcale nie jest łatwo napisać skuteczne i elastyczne zasady, które zmieszczą się na kilku stronach. Dlatego prace dobrze jest też rozłożyć. Jeżeli na danym etapie nie uda się wszystkiego przygotować, trzeba skupić się na najważniejszym procesach i systemach, a potem zacząć systematycznie je zabezpieczać, na miarę dostępnego budżetu i możliwości zaangażowania kompetentnych ludzi.

Cyberbezpieczeństwo w 2021 r. walczy o uwagę z takimi krytycznymi tematami, jak podwyżki taryf, zmiany przepisów o zamówieniach publicznych czy przepisów dotyczących osadów ściekowych. Jednak nie można zapominać, że procedury w tym zakresie stanowią ogrodzenie, które chroni przed wizytą niepożądanych gości i szkodami, które będą się liczyć w milionach. Dlatego w żadnym razie ten temat nie powinien trafić do szuflady.

Autor: Monika Bogdał, radca prawny, Szef Specjalizacji Nowe Technologie, Kancelaria Prawna Piszcz i Wspólnicy sp.k.

Bibliografia dostępna na Portal Komunalny Plus:

1. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, (Dz.U.UE.L.2016.194.1)
2. Ustawa z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. DzU 2020, poz. 1369, ze zm.; dalej jako: „Ustawa o KSC").
3. Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym (art. 2 pkt. 1-3 Ustawy o KSC).
4.https://sciekiprzemyslowe.pl/kontenerowe-oczyszczalnie-sciekow-przemyslowych/automatyka-oczyszczalni-plc-i-scada/, [dostęp 25.01.2021].
5. Ustawa z dnia 07 czerwca 2001 r. o zbiorowym zaopatrzeniu w wodę i zbiorowym odprowadzaniu ścieków (DzU 2020, poz. 2028, ze zm.).
6.https://thehackernews.com/2017/02/scary-scada-ransomware.html, [dostęp 25.01.2021].
7.https://www.stormshield.com/news/water-infrastructure-when-states-and-cyber-attacks-rear-their-ugly-heads/, [dostęp 25.01.2021].