OPINIA

INFRASTRUKTURA WODNA: GDY DO GŁOSU DOCHODZĄ WROGIE PAŃSTWA I CYBERPRZESTĘPCY

Khobeib Ben Boubaker
Head of Industrial Security Business Line,
Stormshield

Cyberataki skierowane przeciwko zaporom wodnym, systemom nawadniania i oczyszczalniom ścieków przeważnie nie trafiają na pierwsze strony gazet i czołówki portali informacyjnych, jednak to nie zmienia ponurej rzeczywistości – tego rodzaju zagrożenia nie tylko istnieją, ale również stanowią poważne wyzwanie strategiczne. Jak wygląda stan cyberbezpieczeństwa systemów wodnych na świecie?

Gdy spojrzymy na zagadnienie ochrony ludzi w cyberprzestrzeni kompleksowo, szybko dojdziemy do wniosku, że mamy do czynienia z poważnym wyzwaniem obejmującym zarówno dostawy niezbędnych produktów i usług, jak i zdrowie oraz gospodarkę wodną. Poza wszystkimi kluczowymi kwestiami związanymi z tym sektorem jak i istotnym znaczeniem wody jako zasobu, sektor gospodarki wodnej musi również stawiać czoła coraz poważniejszym cyberatakom skierowanym przeciwko ich infrastrukturom. **Sektor gospodarki wodnej jest złożony, jednak cyberataki dorównują mu stopniem wyrafinowania.** Często są one wspierane lub organizowane przez jednostki działające za cichym przyzwoleniem władz państwowych, których celem jest destabilizacja gospodarki danego kraju. Przedsiębiorstwa zajmujące się gospodarką wodną muszą w związku z tym stawiać czoła wyzwaniom związanym z produkcją, jednocześnie spełniając coraz wyższe wymogi w zakresie bezpieczeństwa. Celem jest skuteczna ochrona całej krytycznej infrastruktury i sprzętu dzięki skupieniu się na obronie i możliwie jak największym ograniczeniu szkód, które mogą powstać w wyniku cyberataku przeprowadzonego na szeroką skalę.

STAN CYBERBEZPIECZEŃSTWA SYSTEMÓW WODNYCH

W ostatnich latach podmioty działające w sektorze infrastruktury wodnej wprowadziły szereg zmian w zakresie technologii cyfrowych, skupiając się na eliminacji przestarzałych połączeń RTC i zastąpienie ich sieciami przewodowymi, a także rozwiązaniami 4G i 5G, które oferują lepszą łączność. Obecnie zmiany te są wdrażane przez kolejne podmioty, które w ich wyniku wystawiają się na świat zewnętrzny, co stanowi w ich przypadku pewne novum – w czasach połączeń RTC, większość systemów (w tym sterowniki PLC) była odizolowana od Internetu, jednak zmierzch tej metody komunikacji sprawił, że obecnie systemy te mają dostęp do globalnej sieci, co wiąże się z narażeniem na nowe zagrożenia cybernetyczne.

"Sektor gospodarki wodnej musi skupić się obecnie na zabezpieczaniu swoich systemów, które stały się częścią Internetu Rzeczy, a nawet krajobrazu Przemysłowego Internetu Rzeczy – wraz ze wszystkimi problemami związanymi z bezpieczeństwem, które nieodłącznie towarzyszą tego rodzaju rozwiązaniom"

Raphaël Granger, Named Account Manager Stormshield

Nowy paradygmat wiąże się z podwójnym wyzwaniem dla sektora – wymianą starzejących się lub wręcz przestarzałych urządzeń przemysłowych działających pod kontrolą systemów takich jak Windows XP i starszych na nowocześniejsze technologie dysponujące lepszą łącznością, **a także koniecznością uwzględnienia cyberbezpieczeństwa jako integralnego elementu prowadzonej działalności**.

- *Sektor gospodarki wodnej musi skupić się obecnie na zabezpieczaniu swoich systemów, które stały się częścią Internetu Rzeczy, a nawet krajobrazu Przemysłowego Internetu Rzeczy – wraz ze wszystkimi problemami związanymi z bezpieczeństwem, które nieodłącznie towarzyszą tego rodzaju rozwiązaniom* - wyjaśnia Raphaël Granger, Named Account Manager w firmie Stormshield.

Co więcej, sektor ten musi również stawiać czoła zagrożeniom wynikającym z jego natury. Ze względu na istnienie wielu fizycznych lokalizacji – zbiorników uzdatniania wody, centrów dystrybucji i wież ciśnień, działające w nim podmioty korzystają z rozproszonych architektur w celu przesyłania informacji oraz danych. Zapewnienie integralności i prywatności tych przepływów jest obecnie jednym z kluczy do zapewnienia jakości kluczowego zasobu na końcu łańcucha wartości, a w dodatku nabiera kluczowego znaczenia w czasach, gdy zdalne zarządzanie staje się powszechne. Skuteczne stawianie czoła tym wyzwaniom wymaga jednak świadomości zagrożeń wśród wszystkich podmiotów i uczestników tego łańcucha, w tym operatorów zajmujących się zdalną konserwacją i obsługą.

PRZEPISY WIELU PRĘDKOŚCI

Na arenie międzynarodowej większość kluczowych interesariuszy sektora w krajach rozwiniętych również zaczyna traktować cyberbezpieczeństwo jako jeden z wymaganych elementów działalności.

— *Stan cyberbezpieczeństwa systemów wodnych nie odpowiada jeszcze poziomowi zagrożeń i wyzwań, którym musi stawiać czoła cały sektor* — wyjaśnia **Nebras Alqurashi**, Business and Technical Development Manager (Middle East) w firmie Stormshield. — *Coraz częściej to władze i organy nadzorcze biją na alarm i wzywają do poprawy sytuacji* — dodaje.

Niestety, w krajach rozwijających się cyberbezpieczeństwo znajduje się daleko na końcu listy priorytetów dla przedsiębiorstw działających w sektorze wodno-kanalizacyjnym.

— *Kraje te stawiają czoła zupełnie innym wyzwaniom, wśród których można wymienić między innymi niedobór wody, uzdatnianie wody, wydajność sieci dystrybucyjnych, odprowadzanie ścieków i wiele innych. Z punktu widzenia gospodarki wodnej i dostępu do wody trudno jest mówić o równych warunkach panujących we wszystkich krajach* — podkreślił **Tarik Zeroual**, Global Account Manager w firmie Stormshield.

Nierównościom i niedoborom, z którymi mamy do czynienia między innymi w regionie Bliskiego Wschodu, często towarzyszą konflikty dotyczące wodą oraz walki o przejęcie kontroli nad sektorem wodnym. Tego rodzaju okoliczności gospodarcze i polityczne sprzyjają cyberatakom wykorzystywanym przez państwa w celu wywierania presji i wzajemnej destabilizacji.

GEOPOLITYKA, ZDROWIE PUBLICZNE I INNE ZAGADNIENIA… WYSOKA STAWKA CYBERATAKÓW NA INFRASTRUKTURĘ WODNĄ

Analiza sytuacji sektora wodnego sugeruje, że jeśli weźmiemy pod uwagę szczególnie wrażliwe obiekty i urządzenia działające pod kontrolą przestarzałych systemów operacyjnych, transformację w kierunku przemysłowego Internetu Rzeczy (IoT), czy wyzwania geopolityczne i strategiczne związane z zasobami wodnymi, zapewnienie stabilności jego działania rośnie do rangi poważnego problemu. Trudno zatem dziwić się, że coraz częściej zwracają nań uwagę hakerzy i cyberprzestępcy.

W rezultacie infrastruktura wodna stała się nowym frontem walki z cyberprzestępczością, a napastnicy zdają się preferować w tej walce jeden rodzaj broni – *oprogramowanie ransomware*. Jak czytamy w sprawozdaniu amerykańskiej spółki Gray Matter, w 2019 roku w samych Stanach Zjednoczonych odnotowano ponad 22 cyberataki tego rodzaju.

Departament gospodarki wodnej w Północnej Karolinie stał się celem takiego ataku z wykorzystaniem oprogramowania ransomware jeszcze w 2018 roku. Atak ten nastąpił w bardzo niefortunnym momencie, gdy nadal trwało usuwanie skutków zniszczeń spowodowanych przez huragan Florence, który uderzył w stan zaledwie kilka tygodni wcześniej. Specjaliści podejrzewają, że napastnicy celowo wykorzystali kryzys, aby zaatakować systemy wodne i zaszkodzić ludności. Aby uzyskać dostęp do docelowych systemów atakujący użyli złośliwego oprogramowania Emotet, a następnie – gdy udało im się dostać do środka, wykorzystali ransomware Ryuk znany z ataków na obiekty użyteczności publicznej w celu zaszyfrowania części danych departamentu.

Cofnijmy się nieco dalej – w 2017 roku eksperci Georgia State University zajmujący się cyberbezpieczeństwem opracowali nową formę złośliwego oprogramowania zdolnego do zatruwania wody poprzez zmianę stężenia chloru w zakładach uzdatniania wody pitnej. W ramach symulowanego ataku, badacze przejęli kontrolę nad sterownikami PLC (*Programmable Logic Controllers*) obiektu. W późniejszym sprawozdaniu z przebiegu symulacji opisali metody działania, które mogli wykorzystać potencjalni napastnicy w celu przejęcia kontroli nad podatnymi na atak sterownikami PLC. Przeprowadzony przez badaczy atak przebiegał wieloetapowo – w pierwszej kolejności nastąpił etap rozpoznania mający na celu wykrycie podłączonych do Internetu sterowników PLC – dokonali tego między innymi przy pomocy specjalistycznej wyszukiwarki Shodan, a następnie wykorzystanie ich jako punktów dostępu. Po dostaniu się do systemu napastnicy uzyskaliby możliwość penetracji wszystkich systemów obiektu i kradzieży kluczowych informacji – w tym danych dostępowych pozwalających na kontrolowanie sterowników PLC. Ostatni etap ataku polegał na zwiększeniu ilości chloru dodawanego do wody i wyświetlaniu fałszywych odczytów.

- *Jesteśmy świadkami coraz częstszych ataków na sieci przemysłowe i to już nie są drobne incydenty które przechodzą bez echa, a stały, rosnący trend, dlatego przedsiębiorstwa działające w ramach infrastruktury krytycznej muszą dostrzec konieczność stosowania odpowiednich zabezpieczeń, by nie dopuszczać w przyszłości do takich incydentów* – komentuje **Piotr Zielaskiewicz**, product manager Stormshield.

Symulowany atak doskonale ilustruje cele napastników atakujących infrastrukturę wodną – każdy tego rodzaju atak może mieć podłoże strategiczne, a wywołane skutki mogą stanowić zagrożenie dla życia części ludności dotkniętego kraju i doprowadzić do jego destabilizacji. Ochrona zdrowia publicznego stanowi kluczowe wyzwanie, a przedsiębiorstwa sektora wodnego muszą również uwzględnić je w swoich działaniach ukierunkowanych na zapewnianie bezpieczeństwa swoich instalacji.

— Napastnik, który uzyska dostęp do obiektów odpowiedzialnych za dystrybucję wody, może zaatakować ludność i w związku z tym stanowi olbrzymie zagrożenie dla zdrowia i życia. Udany cyberatak na sektor wodny może wiązać się z poważnym zagrożeniem wymagającym natychmiastowej reakcji — ostrzega Tarik Zeroual.

"Udany cyberatak na sektor wodny może wiązać się z poważnym zagrożeniem wymagającym natychmiastowej reakcji"

Tarik Zeroual, Global Account Manager Stormshield

Badacze nie są jedynymi, którzy zwrócili uwagę na zagrożenia związane z atakami na stacje chemicznego uzdatniania wody. W kwietniu ubiegłego roku irańscy hakerzy podjęli próbę wykorzystania tego wektora ataku, by zmienić jakość wody trafiającej do części ludności Izraela. Napastnicy najpierw przejęli kontrolę nad amerykańskimi serwerami, aby w ten sposób zatrzeć swoje ślady, a następnie przeszli do ataku na systemy dystrybucji wody. Na szczęście atak zakończył się niepowodzeniem – w innym przypadku mógłby wiązać się z poważnym zagrożeniem dla zdrowia publicznego, a część ludności prawdopodobnie zostałaby otruta.

W lipcu ubiegłego roku Izrael przekazał informacje dotyczące dwóch nowych ataków skierowanych przeciwko swojej krytycznej infrastrukturze wodnej. Tym razem napastnicy postanowili obrać za cel systemy wykorzystywane w sektorze rolniczym. Można zatem powiedzieć, że w tym wypadku mieliśmy do czynienia z atakiem niższego szczebla – w świetle podejrzeń ich inicjatorem mógł być Iran, a same ataki miały być motywowane chęcią destabilizacji państwa Izrael i jego polityczne osłabienie. W obu przypadkach atakujący po raz kolejny wykorzystali amerykańskie serwery, aby za ich pomocą kontrolować oprogramowanie sterujące pompami.

Cyberataki na infrastrukturę wodną wydają się być na ogół dobrze przygotowane – napastnicy są przygotowani i posiadają doskonałą wiedzę, znają również systemy, które obierają za swój cel. Żaden element ataku nie jest dziełem przypadku. Na tej podstawie można wysnuć przypuszczenie, że źródłem tych ataków mogą być państwa, natomiast sami napastnicy z pewnością nie są amatorami.

— Za cyberatakami skierowanymi w sektor gospodarki wodnej stoją zorganizowane grupy APT – na ogół rosyjskie, chińskie lub irańskie, często finansowane lub kierowane przez organy państwowe — wyjaśnia Tarik Zeroual.

Nie da się zaprzeczyć, że sektor wodny oferuje napastnikom możliwość przeprowadzania cyberataków na szeroką skalę, które mogą mieć strategiczne znaczenie dla bezpieczeństwa.. Z tego powodu przedsiębiorstwa muszą przygotować się na to, by w jak największym stopniu ograniczyć możliwość przejęcia swoich infrastruktur na potrzeby prowadzenia wojny cybernetycznej w kontekście geopolitycznym.

ODPOWIEDŹ SEKTORA: LEPSZA OCHRONA DZIĘKI SEGMENTACJI

Poważne problemy wymagają skutecznych rozwiązań, a ochrona przed cyberatakami wymaga filtrowania wszystkich danych trafiających do obiektów z zewnątrz. Obecnie przedsiębiorstwa działające w sektorze realizują te założenia dzięki wdrażaniu zasad segmentacji w swoich obiektach. Ochrona infrastruktury wodnej wymaga kompleksowego podejścia do bezpieczeństwa – dzięki wielopoziomowej segmentacji zainteresowane strony mogą dostosować je do swoich potrzeb.

— *Przedsiębiorstwa mogą oddzielać wszystkie obiekty i kontrolować przepływy komunikacji i danych* – wyjaśnia Raphaël Granger.

Oprócz segmentacji swoich obiektów operacyjnych, podmioty działające w sektorze mogą również oddzielać swoje środowisko IT, na które składają się komputery, serwery i użytkownicy, od operacyjnego środowiska OT Tego rodzaju segmentacja ma na celu odizolowanie części operacyjnej sieci na wypadek ataku. Co więcej, możliwa jest również dalsza segmentacja w ramach części OT – rozdział urządzeń kontrolnych oraz sterowników PLC.

Kluczowe podmioty sektora cybernetycznego, w tym wydawcy oprogramowania, wspierają wysiłki sektora wodnego ukierunkowane na wdrażanie segmentacji oraz kolejnych zabezpieczeń.

— *W ten sposób gwarantują bezpieczeństwo systemów wodnych, pomagając firmom działającym w tym sektorze w sprawdzaniu niezawodności i zgodności ich protokołów sieciowych. Wykorzystując przemysłowe zapory sieciowe chcemy zagwarantować, że protokoły te nie zostaną zmodyfikowane lub naruszone przez napastników* – dodaje Raphaël Granger.

Specyfika branży wymaga wdrażania rozwiązań pozwalających na weryfikację prawidłowości poleceń wykonywanych przez sterowniki PLC oraz systemów umożliwiających zarządzanie zdalnym dostępem i zapewnianie jego bezpieczeństwa, by umożliwić zdalną konserwację, zarządzanie alarmami i inne czynności.

Podmioty działające w sektorze wodnym weszły do wyścigu zbrojeń, ale to dopiero początek – w najbliższej przyszłości sektor będzie musiał zmierzyć się z nowym wyzwaniem, jakim jest rozszerzenie zasad bezpieczeństwa na cały łańcuch wartości obejmujący dodatkowe obiekty poza stacjami uzdatniania wody, a także przyjęcie bardziej zaawansowanego podejścia do przemysłowego Internetu Rzeczy obejmującego kompleksowe zabezpieczenie systemów i protokołów komunikacji w całym łańcuchu - od obiektu, aż po odbiorcę.

RZĄDOWE REKOMENDACJE DLA SEKTORA WOD-KAN / LUTY 2021

Sytuacje opisane w tym tekście pokazują, że w sektorze wodno-kanalizacyjnym – który jest jednym z najbardziej krytycznych- brakuje podstawowych zasad bezpieczeństwa. To wszystko prawdopodobnie skłoniło Departament Cyberbezpieczeństwa Kancelarii Prezesa Rady Ministrów do wydania rekomendacji dla podmiotów infrastruktury krytycznej, dotyczących ochrony przed cyberatakami.

1. Należy zmniejszyć do minimum ekspozycję sieci przemysłowej, zarówno sieci lokalnej, jak i punktów styku, poprzez identyfikację i ograniczenie do koniecznych, połączeń „z" i „do" tej sieci – ograniczamy (lub wręcz uniemożliwiamy) w ten sposób nieautoryzowane połączenia z zewnątrz.

2. Należy oddzielić systemy OT od systemów IT zorientowanych na klienta oraz monitorować i kontrolować interakcje pomiędzy tymi dwoma obszarami. Rekomendowanym rozwiązaniem jest unikanie podłączeń urządzeń przemysłowych do sieci publicznych, w szczególności Internetu.

3. Należy zmniejszyć do minimum ekspozycję sieci przemysłowej, zarówno sieci lokalnej, jak i punktów styku, poprzez identyfikację i ograniczenie do koniecznych, połączeń „z" i „do" tej sieci – ograniczamy (lub wręcz uniemożliwiamy) w ten sposób nieautoryzowane połączenia z zewnątrz.

4. Należy oddzielić systemy OT od systemów IT zorientowanych na klienta oraz monitorować i kontrolować interakcje pomiędzy tymi dwoma obszarami. Rekomendowanym rozwiązaniem jest unikanie podłączeń urządzeń przemysłowych do sieci publicznych, w szczególności Internetu.

5. W przypadku gdy zdalny dostęp jest niezbędny (np. do monitorowania i zarządzania rozległą infrastrukturą) powinien być zawsze realizowany za pomocą VPN6 z wykorzystaniem konfiguracji umożliwiającej zastosowanie uwierzytelnienia wieloskładnikowego (MFA)7 .

6. Należy dokonać przeglądu zdalnego dostępu i ograniczyć go do niezbędnego minimum, w szczególności należy zwrócić uwagę na modemy komórkowe i metody zdalnego dostępu podwykonawców.

7. Należy zmienić domyślne dane uwierzytelniające stosując dobre praktyki silnych haseł (o ile urządzenie takie hasła wspiera), na wszystkich urządzeniach, w szczególności urządzeniach posiadających interfejs webowy oraz wyłączyć niewykorzystywane konta.

8. Tam gdzie to możliwe, należy ograniczyć dostęp do VPN dla określonych adresów IP lub ich zakresów. Przykładowo gdy podmiot nie posiada współpracowników ani podwykonawców zagranicznych, rekomenduje się zastosować możliwość próby nawiązania sesji VPN tylko dla polskich adresów IP.

9. W przypadku, gdy niezbędny jest zdalny przesył danych telemetrycznych za pomocą sieci komórkowej należy korzystać z dedykowanych prywatnych APN8 .

10. Należy aktualizować oprogramowanie wykorzystywanych systemów i urządzeń, w szczególności podczas planowych postojów. Przed aktualizacją należy przeprowadzić analizę potencjalnego wpływu aktualizacji na utrzymanie ciągłości działania (w szczególności aktualizacja może wprowadzać elementy, które spowodują utratę zgodności np. z oprogramowaniem niskopoziomowym) – dlatego też przed dokonaniem aktualizacji należy przetestować ją w środowisku testowym, przed zastosowaniem w środowisku produkcyjnym.

11. Należy stosować segmentację sieci - minimalnie na styku sieci przemysłowej, a preferencyjnie, zależnie od rozmiaru i złożoności zakładu, również wewnątrz.

12. Należy prowadzić okresową analizę widoczności urządzeń poprzez zewnętrzne skanowanie zakresu adresacji należącej do obiektu, czy wykorzystanie narzędzi typu Shodan.

13. Należy zgłosić osoby do kontaktu do zespołów reagowania na incydenty - CSIRT poziomu krajowego - w celu ustanowienia szybkiej ścieżki reakcji w przypadku incydentu:

14. Każde zdarzenie mające znamiona cyberataku oraz incydent bezpieczeństwa należy niezwłocznie zgłosić do właściwego zespołu CSIRT poziomu krajowego.

Piotr Zielaskiewicz dodaje, że urządzenia Stormshield pomagają w spełnianiu wskazanych rekomendacji. - *W jaki sposób? Przypomnijmy, że Stormshield to dedykowane rozwiązania Next Generation Firewall, które chronią, kontrolują i autoryzują ruch sieciowy oraz pozwalają bezpiecznie łączyć ze sobą oddziały i użytkowników za pomocą tuneli VPN. Dzięki monitoringowi na żywo, zaawansowanemu IDS/IPS i DPI protokołów przemysłowych takich jak S7, Modbus, UMAS, OPC Classic (DA/HDA/AE), OPC UA, EtherNet/IP, CIP, BACnet/IP, Profinet, IEC 60780-5-104, DNP3, IEC 61850 (MMS/GOOSE) są to obecnie najchętniej wybierane firewalle do zabezpieczania sieci przemysłowych.*

STORMSHIELD

Obecnie przedsiębiorstwa, instytucje rządowe i organizacje obronne na całym świecie stawiają czoła wyzwaniu jakim jest zagwarantowanie cyberbezpieczeństwa kluczowych elementów infrastruktury, danych i środowisk operacyjnych. Rozwiązania Stormshield posiadające najwyższe europejskie certyfikaty spełniają wszystkie wymagania IT i OT w zakresie ochrony bezpieczeństwa. Chcemy zapewniać bezpieczeństwo naszym klientom, by dzięki temu mogli skoncentrować się na swojej podstawowej działalności – to sprawia, że instytucje i operatorzy będą w stanie funkcjonować bez zakłóceń, a społeczeństwa będą mogły korzystać z wysokiej jakości usług. Wybierając Stormshield, wybierasz zaufanego europejskiego dostawcę usług i rozwiązań w zakresie cyberbezpieczeństwa. Więcej informacji: **www.stormshield.pl**