Rekomendacje cyberbezpieczeństwa dla sektora wodno-kanalizacyjnego

(R-CYBER-01/2021)

(luty 2021 r.)

Informacje o poradniku

Poradnik jest skierowany do specjalistów ds. bezpieczeństwa IT/OT, w szczególności, w następujących podmiotach:

- Organy właściwe ds. cyberbezpieczeństwa;
- Zespoły CSIRT poziomu krajowego;
- Operatorzy usług kluczowych;
- Operatorzy infrastruktury krytycznej;
- Urzędy administracji rządowej i samorządowej.

Celem poradnika jest przedstawienie zagrożeń związanych z wykorzystaniem infrastruktury IT/OT do dokonania ataków na:

- Sieci wodociągów i kanalizacji;
- Oczyszczalnie ścieków;
- Stacje uzdatniania wody;

Ponadto, w poradniku wskazane są rekomendowane zalecenia bezpieczeństwa, zwiększające odporność infrastruktury na cyberataki.

Wprowadzenie – czyli o jakim rodzaju zagrożenia jest mowa

Sektor wodno-kanalizacyjny jest jednym z elementów infrastruktury krytycznej państw i obejmuje zarówno obiekty zarządzane przez administrację rządową, jak i przez jednostki samorządu terytorialnego. Należy podkreślić, że większość obiektów z infrastruktury wodno-kanalizacyjnej m.in. oczyszczalnie ścieków, stacje uzdatniania wody czy systemy rurociągów są własnością gmin.

Systemy wodno-kanalizacyjne – jak wiele obiektów infrastruktury krytycznej państw – są często atakowane przez pojedynczych przestępców, zorganizowane grupy cyberprzestępców oraz przez instytucje powiązane lub wręcz nadzorowane przez inne państwa.

ul. Królewska 27, 00-060 Warszawa, tel. +48 (22) 245 54 12

Wybrane przykłady ataków na sektor wodno-kanalizacyjny w latach 2018-2020

1. Izrael - 1 grudnia 2020 r. izraelska firma Otorio poinformowała o ataku – najprawdopodobniej grupy z Iranu – na jeden z obiektów systemu zaopatrywania w wodę, który jest elementem infrastruktury krytycznej państwa. Atakujący dostali się do systemu poprzez przełamanie zabezpieczeń interfejsu Human Machine Interface – system był podłączony do globalnej sieci internet i nie był chroniony w wystarczający sposób.
   Wg informacji atakujący mogli dokonywać m.in. nieautoryzowanej zmiany ciśnienia wody, temperatury itp.

   Był to już kolejny w tym roku zidentyfikowany atak Irańczyków na systemy krytyczne Izraela. W lipcu zaatakowano system zarzadzania rolnictwem, w kwietniu i czerwcu systemy pozyskiwania energii słonecznej, w kwietniu i lipcu system zaopatrywania w wodę. Za każdym razem przestępcy dokonywali przełamania zabezpieczeń przemysłowych systemów sterowania.

2. Izrael – w listopadzie 2020 r. grupa irańskich hakerów o nazwie "Niezidentyfikowany zespół" twierdził na swoim kanale, że naruszyli przemysłowy system sterowania w jednym z systemów sterowania wodociągami w Izraelu.

3. Izrael – w czerwcu 2020 r. izraelski portal medialny Ynet poinformował, że dwa zakłady oczyszczania ścieków w izraelskim sektorze rolniczym stały się obiektem cyberataku. Pierwszy atak uderzył w rolnicze pompy wody w górnej Galilei, a drugi w pompy wody w centralnej prowincji Mateh Yehud.

4. Niemcy – w maju 2020 r. rząd Niemiec poinformował o długotrwałej kampanii rosyjskich cyberprzestępców z grupy APT Berserk Bear, którzy w sposób metodyczny atakowali niemieckie firmy z sektora wodnego i energetycznego.

5. Izrael – w kwietniu 2020 r. Izraelska Narodowa Dyrekcja ds. Cyberbezpieczeństwa (INCD) wydała alert ostrzegający organizacje działające w sektorze wodnym i energetycznym przed serią cyberataków wymierzonych w system nadzorujący przebieg procesu technologicznego lub produkcyjnego (SCADA) w oczyszczalniach ścieków, przepompowniach i obiektach kanalizacyjnych.

6. USA - Firma TrendMicro odkryła, że w 2019 irańska grupa cyberprzestępców APT33 obrała za cel instalację wodną, która była wykorzystywana przez armię amerykańską do zaopatrywania w wodę pitną jednej z baz wojskowych.

7. USA – w maju 2019 r. w wyniku ataku typu ransomware w mieście Baltimore spowodował trzymiesięczne opóźnienia w wystawianiu rachunków za wodę.

8. Europa – w 2018 r. firma Radiflow, odkryła złośliwe oprogramowanie do wydobywania kryptowalut w sieci dostawcy usług wodociągowych w Europie. Atak był pierwszym publicznym odkryciem nieautoryzowanego tworzenia kryptowalut

ul. Królewska 27, 00-060 Warszawa, tel. +48 (22) 245 54 12

wpływającego na systemy kontroli przemysłowej (ICS) lub serwery systemu nadzorującego przebieg procesu technologicznego lub produkcyjnego (SCADA).

9. USA – w 2016 r. firma Verizon poinformowała, że przestępcy byli w stanie włamać się do firmy wodociągowej, która w swojej sieci IT posiadała przestarzałe oprogramowanie i sprzęt.

Atak na stację uzdatniania wody na Florydzie - niebezpieczny precedens, ale też ostrzeżenie przed kolejnymi incydentami

W ostatnim czasie **obserwuje się rosnącą liczbę urządzeń wykonujących funkcje przemysłowych systemów sterowania** (ang. *Industrial Control System)* **zarządzanych i dostępnych bezpośrednio z Internetu, często z możliwością zdalnego sterowania**. Niejednokrotnie systemy te są skonfigurowane z wykorzystaniem domyślnych haseł lub posiadają niezaktualizowane oprogramowanie. Szczególnie często dotyczy to przypadków, gdzie dane telemetryczne przesyłane są za pomocą publicznych sieci łączności mobilnej.

Jak informuje amerykańska agencja DHS CISA (Cybersecurity and Infrastructure Security Agency)[1], która stale monitoruje zagrożenia występujące w cyberprzestrzeni, znane są przypadki ataków cyberprzestępców poszukujących tego typu urządzenia (zarządzane zdalnie przez Internet), aby wykorzystać ich dostępność jako wektor ataku na sieci przemysłowe.

Dodatkowo, **5 lutego 2021 r., został ujawniony przypadek ataku na stację uzdatniania wody na Florydzie (USA), skutkujący zmianą nastawień dozowania środków chemicznych.**

Jak przebiegał atak na stację uzdatniania wody na Florydzie?

5 lutego 2021 r. stacja uzdatniania wody w Oldsmar (Floryda, USA) zgłosiła[2] włamanie do swojej sieci zarządzania obiektem, w której nieznana osoba była w stanie na krótko zmodyfikować skład chemiczny przetwarzanej wody poprzez zwiększenie ilości wodorotlenku sodu (znanego również jako ług lub soda kaustyczna) do poziomu niebezpiecznego dla spożycia przez ludzi[3].

Według organów ścigania, około godziny 13:00, tego dnia, napastnik uzyskał dostęp do systemu kontroli poprzez preinstalowaną instancję oprogramowania zdalnego pulpitu TeamViewer[4] - podczas 3-5 minutowego ataku, napastnik zmienił ilość wodorotlenku sodu ze 100 części na milion (ppm) do 11100 ppm. Po zakończeniu połączenia napastnika

[1] Agencja rządu USA odpowiedzialna za zapewnienie bezpieczeństwa, w tym cyberbezpieczeństwa amerykańskiej infrastruktury krytycznej.
[2] https://www.youtube.com/watch?v=MkXDSOgLQ6M
[3] https://sekurak.pl/przez-teamviewer-a-az-do-systemu-kontroli-uzdatniania-wody-hacker-zmienil-parametry-chemiczne-wody/
[4] TeamViewer, jest jednym z najpopularniejszych oprogramowana do wykonywania zdalnej kontroli/pracy. Inne bardzo rozpowszechnione aplikacje to m.in. AnyDesk, Ultra VNC, czy TightVNC. Aplikacja TeamViewer umożliwia zdalną pomoc techniczną dla systemów komputerowych.

ul. Królewska 27, 00-060 Warszawa, tel. +48 (22) 245 54 12

z systemem, operator zakładu monitorujący sytuację cofnął zmianę. W tym miejscu należy podkreślić czujność operatora systemu, który w porę zauważył taki dość niespodziewany wzrost i natychmiast przywrócił stężenie wodorotlenku sodu do normalnego poziomu. Co więcej, operator natychmiast powiadomił odpowiednie służby, w tym organy ścigania, o ataku.

Wodorotlenek sodu jest powszechnie stosowany w domowych środkach czyszczących, ale może być bardzo niebezpieczny, jeśli zostanie użyty w dużym stężeniu. Jednak w niższych stężeniach jest on stosowany w stacjach uzdatniania wody do regulacji kwasowości (pH) i usuwania metali ciężkich.

FBI i amerykańskie służby specjalne zostały wezwane do pomocy w śledztwie dotyczącym tego incydentu[5].

Co zawiodło w stacji uzdatniania wody w Oldsmar?

Zawiódł przede wszystkim człowiek oraz nieadekwatne procedury i słaba organizacja systemu bezpieczeństwa wykorzystywanych narzędzi do kontroli i nadzoru procesu.

Co konkretnie zawiodło:

- Słabe zasady zarządzania hasłami. Wszystkie komputery posiadały to samo hasło umożliwiające zdalny dostęp;
- Wszystkie komputery służące do zarządzania usługą były podłączone do Internetu;
- Brak firewalla;

Incydent ten po raz kolejny pokazuje, że każde rozwiązanie zdalnego dostępu musi być starannie zabezpieczone i monitorowane.

[5] https://www.reuters.com/article/us-usa-cyber-florida/hackers-broke-into-florida-towns-watertreatment-plant-attempted-to-poison-supply-sheriff-says-idUSKBN2A82FV

ul. Królewska 27, 00-060 Warszawa, tel. +48 (22) 245 54 12

REKOMENDACJE - Co zatem należy zrobić?

Wydarzenie w USA wyraźnie pokazuje jak szkodliwe mogą być ataki nakierowane na przemysłowe systemy sterowania, które są dostępne przez Internet, w szczególności w przypadku sieci i systemów gospodarowania wodą. Co więcej, analizy ekspertów z zespołu reagowania na incydenty komputerowe CSIRT NASK wskazują, że podobne luki bezpieczeństwa posiada wiele podmiotów funkcjonujących w Polsce.

Mając na uwadze cyberzagrożenia, które mogą dotyczyć obiektów infrastruktury wodnej zarządzanej przemysłowymi systemami sterowania należy stosować **rekomendowane środki organizacyjne i techniczne zwiększające odporność infrastruktury na cyberataki**:

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. W przypadku gdy zdalny dostęp jest niezbędny (np. do monitorowania i zarządzania rozległą infrastrukturą) powinien być zawsze realizowany za pomocą VPN[6] z wykorzystaniem konfiguracji umożliwiającej zastosowanie uwierzytelnienia wieloskładnikowego (MFA)[7].
4. **Należy dokonać przeglądu zdalnego dostępu i ograniczyć go do niezbędnego minimum**, w szczególności należy zwrócić uwagę na modemy komórkowe i **metody zdalnego dostępu podwykonawców**.
5. **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.
6. 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.
7. W przypadku, **gdy niezbędny jest zdalny przesył danych telemetrycznych za pomocą sieci komórkowej należy korzystać z dedykowanych prywatnych APN**[8].

[6] Virtual Private Network - mechanizm działania sieci VPN opiera się przede wszystkim na ukryciu prawdziwego adresu IP urządzenia oraz na szyfrowaniu danych, przesyłanych podczas trwania połączenia internetowego.
[7] Multi-Factor Authentication.
[8] Access Point Name – nazwa bądź adres bramy pomiędzy siecią komórkową operatora a zewnętrzną siecią komputerową, umożliwiającą m.in. rutowanie pakietów między tymi sieciami.

ul. Królewska 27, 00-060 Warszawa, tel. +48 (22) 245 54 12

8. 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.
9. Należy stosować segmentację sieci - minimalnie na styku sieci przemysłowej, a preferencyjnie, zależnie od rozmiaru i złożoności zakładu, również wewnątrz.
10. Należy prowadzić okresową analizę widoczności urządzeń poprzez zewnętrzne skanowanie zakresu adresacji należącej do obiektu, czy wykorzystanie narzędzi typu Shodan.
11. Należy zgłosić osoby do kontaktu do zespołów reagowania na incydenty - CSIRT poziomu krajowego - w celu ustanowienia szybkiej ścieżki reakcji w przypadku incydentu:
    a. CSIRT NASK: https://incydent.cert.pl/osoba-kontaktowa#!/lang=pl i przesłać zgłoszenie osoby do kontaktu. Zaleca się także wskazanie osoby dodatkowej.
    b. CSIRT GOV: https://csirt.gov.pl/cer/zgloszenie-osob-do-kont/961,Zgloszenie-osob-do-kontaktow-z-CSIRT-GOV.html. Zaleca się także wskazanie osoby dodatkowej.
12. Każde zdarzenie mające znamiona cyberataku oraz incydent bezpieczeństwa należy niezwłocznie zgłosić do właściwego zespołu CSIRT poziomu krajowego:
    a. **Operatorzy infrastruktury krytycznej do CSIRT GOV**: https://csirt.gov.pl/cer/zglaszanie-incydentu/16,Zglaszanie-incydentu.html
    b. **Pozostałe podmioty publiczne** m.in. obiekty znajdujące się pod nadzorem jednostek samorządów terytorialnych, lecz nie znajdujące się w wykazie infrastruktury krytycznej państwa **do CSIRT NASK**: https://incydent.cert.pl/#!/lang=pl

Zachęcamy również do korzystania z bazy wiedzy o cyberbezpieczeństwie dostępnej na portalu gov.pl – adres https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo.

Kontakt ws. uwag do Rekomendacji: sekretariat.dc@mc.gov.pl

ul. Królewska 27, 00-060 Warszawa, tel. +48 (22) 245 54 12