Cybersecurity Advisory for Public Water Suppliers

How public water suppliers can guard against cyber-attacks on water supplies.

Notice to Public Water Suppliers

Dear Public Water Suppliers,

Due to recent reports of cyber-attacks on the water sector, all utilities are advised to be on heightened alert and encouraged to actively monitor their computer systems for any unusual activity. The most recent attack that you may have heard about occurred in Oldsmar, Florida, and involved targeting the chemical feed system. Specifically, the malevolent actor attempted to increase sodium hydroxide dosages to very high levels. This was quickly identified as an unauthorized intrusion by the system's plant operator who took quick action to stop the threat before any public health and safety was compromised.

You can access the news reports and press conference through the links below to learn more about this specific event, which is currently an active investigation coordinated by the FBI with state and local authorities.

- https://www.wfla.com/news/local-news/hacker-caught-altering-chemicals-in-oldsmar-water-supply-to-damaging-levels/
- https://www.youtube.com/watch?v=MkXDSOgLQ6M&ab_channel=PinellasSheriff

Please remain vigilant, and also be aware that there are many resources and contacts available to you before, during and after any cybersecurity attack. Resources include:

- American Water Works Association (AWWA) Water Sector Cybersecurity Risk Management Tool, to be used in conjunction with AWWA Water Sector Cybersecurity Risk Management Guidance
- Cybersecurity and Infrastructure Security Agency (CISA) Cyber Security Evaluation Tool (CSET): https://us-cert.cisa.gov/ics/Downloading-and-Installing-CSET
- CISA & NSA Alert on Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems (7/23/2020): https://us-cert.cisa.gov/ncas/alerts/aa20-205a
- CISA Industrial Control Systems Advisories and Reports: https://us-cert.cisa.gov/ics
- EPA Incident Action Checklist for Cybersecurity: https://www.epa.gov/sites/production/files/2017-11/documents/171013-incidentactionchecklist-cybersecurity_form_508c.pdf
- EPA Water Sector Cybersecurity Sector Brief for States: https://www.epa.gov/sites/production/files/2018-06/documents/cybersecurity_guide_for_states_final_0.pdf
- EPA Cybersecurity Best Practices for the Water Sector: https://www.epa.gov/waterriskassessment/epa-cybersecurity-best-practices-water-sector
- WaterISAC's 15 Cybersecurity Fundamentals: https://www.waterisac.org/system/files/articles/15%20Cybersecurity%20Fundamentals%20%28WaterISAC%29.pdf
- Joining WaterISAC at: https://www.waterisac.org/
- Joining the MA Water/Wastewater Agency Response Network (MA WARN) at: http://www.mawarn.org/

Contacts include:

- Local police department of jurisdiction
- Commonwealth Fusion Center's Massachusetts Cybersecurity Program (CFC-MCP) at 508-820-2233
- Federal Bureau of Investigation's (FBI) 24/7 CyberWatch at 855-292-3937 or CyWatch@fbi.gov, and the Boston FBI Field Office at 857-386-2000 or bostonfbi.gov.
- Department of Homeland Security (DHS)/Cybersecurity and Infrastructure Security Agency (CISA) at 888-282-0870 or Central@cisa.dhs.gov, or through the DHS CISA Incident Reporting System
  CISA Region 1 at CISARegion1@hq.dhs.gov
- It is also recommended that events be shared with the Water Information Sharing & Analysis Center (WaterISAC) at analyst@waterisac.org or 866-H2O-ISAC.

Additional information about cybersecurity breach in Florida

Dear Public Water Supplier,

We appreciate your attention to cybersecurity and the recent incident in Florida. Here is a more specific description on the events and suggested protective measures.

The FBI, DHS, US Secret Service, and the Pinellas County Sheriff's Office have issued a joint situational report that concerns the water sector. EPA is providing critical information from this report to the WSCC and GCC for awareness. EPA recommends that all water systems implement the mitigation measures listed at the end of this report where applicable.

Background

On 5 February 2021, unidentified cyber actors obtained unauthorized access, on two separate occasions, approximately five hours apart, to the supervisory control and data acquisition (SCADA) system used at a local municipality's water treatment plant. The unidentified actors accessed the SCADA system's software and altered the amount of sodium hydroxide, a caustic chemical, used as part of the water treatment process. Water treatment plant personnel immediately noticed the change in dosing amounts and corrected the issue before the SCADA system's software detected the manipulation and alarmed due to the unauthorized change. As a result, the water treatment process remained unaffected and continued to operate as normal.

The unidentified actors accessed the water treatment plant's SCADA controls via remote access software, TeamViewer, which was installed on one of several computers the water treatment plant personnel used to conduct system status checks and to respond to alarms or any other issues that arose during the water treatment process. All computers used by water plant personnel were connected to the SCADA system and used the 32-bit version of the Windows 7 operating system. Further, all computers shared the same password for remote access and appeared to be connected directly to the Internet without any type of firewall protection installed.

Recommended Mitigation

- Restrict all remote connections to SCADA systems, specifically those that allow physical control and manipulation of devices within the SCADA network. One-way unidirectional monitoring devices are recommended to monitor SCADA systems remotely.
- Install a firewall software/hardware appliance with logging and ensure it is turned on. The firewall should be secluded and not permitted to communicate with unauthorized sources.
- Keep computers, devices, and applications, including SCADA/industrial control systems (ICS) software, patched and up-to-date.
- Use two-factor authentication with strong passwords.
- Only use secure networks and consider installing a virtual private network (VPN).

Implement an update- and patch-management cycle. Patch all systems for critical vulnerabilities, prioritizing timely patching of Internet-connected systems for known vulnerabilities and software processing Internet data, such as Web browsers, browser plugins, and document readers.

Did you find what you were looking for on this webpage? *

○ Yes ○ No

SEND FEEDBACK