TLP:CLEAR

Top Cyber Actions for Securing Water Systems

Overview

Water and Wastewater Systems Sector entities (herein referred to as "water systems") run operational technology (OT) and information technology (IT) systems that are too often vulnerable to cyberattacks. This fact sheet highlights the top cyber actions water systems can take today to reduce cyber risk and improve resilience to cyberattacks and provides free services, resources, and tools to support these actions, which can be taken concurrently.[1,2,3] Visit CISA's Water and Wastewater Systems Cybersecurity and EPA's Cybersecurity for the Water Sector webpages for more information and resources.

Buyer beware: Technology manufacturers make security choices that affect the quality of their software and hardware. Review CISA's Secure by Design guidance and ask your vendors how they are adopting the secure by design principles and tactics within their products to mitigate cybersecurity threats.

1. Reduce Exposure to the Public-Facing Internet

Use cyber hygiene services to reduce exposure of key assets to the public-facing internet. OT devices such as controllers and remote terminal units (RTUs) are easy targets for cyberattacks when connected to the internet.

- **Free resource**: CISA's Free Cyber Vulnerability Scanning for Water Utilities fact sheet explains the process and benefits of signing up for CISA's free vulnerability scanning program.
- **Free service:** Email vulnerability@cisa.dhs.gov with the subject line, "Requesting Cyber Hygiene Services" for CISA Cyber Hygiene Services, which proactively identify and enable timely mitigation of internet-exposed assets.

2. Conduct Regular Cybersecurity Assessments

Conduct a cybersecurity assessment on a regular basis to understand the existing vulnerabilities within OT and IT systems. Assessments enable you to identify, assess, and prioritize threats to vulnerabilities in both OT and IT networks.

- **Free service:** EPA Cybersecurity Assessments can help assess cybersecurity posture.
- **Free resource:** CISA's Cross-Sector Cybersecurity Performance Goals (CPGs) provide a set of baseline cyber protections. CISA provides a free CPG assessment that can be administered by a CISA cybersecurity advisor (listed at CISA Regions | CISA) or through a self-assessment.

3. Change Default Passwords Immediately

Require unique, strong, and complex passwords for all water systems, including connected infrastructure. Weak default or insecure passwords are easy to discover and exploit, and they may allow cyber threat actors to make changes to a water systems' operational processes. This can negatively impact public health and safety. Change default or insecure passwords and implement multifactor authentication (MFA) where possible. Focus on deploying MFA to IT infrastructure, such as email, to make it difficult for threat actors to access OT systems. Consider asking manufacturers to eliminate default passwords.

- **Free resources:** CISA's Secure our World Campaign: Use Strong Passwords and More than a Password Campaign. For additional cyber guidance, see CISA's Cyber Guidance for Small Businesses.

[1] The Cybersecurity and Infrastructure Security Agency (CISA), Environmental Protection Agency (EPA), and Federal Bureau of Investigation (FBI) jointly authored this fact sheet.
[2] Joint FBI-CISA-NSA-EPA-INCD Advisory: IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. WWS Facilities
[3] Joint FBI-CISA-EPA-NSA Cybersecurity Advisory: Ongoing Cyber Threats to U.S. Water and Wastewater Systems

TLP:CLEAR

4. Conduct an Inventory of OT/IT Assets

Create an inventory of software and hardware assets to help understand what you need to protect. Focus initial efforts on internet-connected devices and devices where manual operations are not possible. Use monitoring to identify the devices communicating on your network.

- **Free service:** EPA's Cybersecurity Technical Assistance Program supports you in conducting an inventory.
- **Free tool:** A first step in conducting an inventory is identifying the devices on the network. CISA's Malcolm tool enables network monitoring with custom parsers designed for industrial control system (ICS)/OT protocols.

5. Develop and Exercise Cybersecurity Incident Response and Recovery Plans

Develop

Understand incident response actions, roles, responsibilities, as well as who to contact and how to report a cyber incident before one occurs to ensure readiness against potential targeting.

- **Free resources**: EPA's Cybersecurity Action Checklist and CISA's Incident Response Plan (IRP) Basics help to develop cyber incident response plans. The Joint CISA-FBI-EPA Water Incident Response Guide provides valuable information on how to work with federal response partners before, during, and after a cyber incident. **Note:** See this guide for contact information for CISA, FBI, and the EPA Water Infrastructure and Cyber Resilience Division.

Exercise

Test your incident response plan annually to ensure all operators are familiar with roles and responsibilities.

- **Free tools:** CISA Tabletop Exercise Package (CTEP) and EPA tabletop exercise (TTX) scenario tools assists critical infrastructure owners and operators in developing their own tabletop exercises to meet their specific needs.

6. Backup OT/IT Systems

Regularly backup OT/IT systems so you can recover to a known and safe state in the event of a compromise. Test backup procedures and isolate backups from network connections. Implement the NIST 3-2-1 rule: 3) Keep three copies: one primary and two backups; 2) Keep the backups on two different media types; 1) Store one copy offsite.

- **Free resources:** CISA's Cyber Essentials Toolkit Chapter 5: Your Data and NIST's Protecting Data From Ransomware and Other Data Loss Events provide guidance on backing up your systems.

7. Reduce Exposure to Vulnerabilities

Mitigate known vulnerabilities and keep all systems up to date with patches and security updates. Prioritize OT patches in accordance with CISA's Known Exploited Vulnerabilities (KEV) catalog during scheduled downtime of OT equipment; prioritize patches in IT, as applicable. CISA's Secure our World Campaign provides guidance on updating software.

8. Conduct Cybersecurity Awareness Training

Conduct cybersecurity awareness training annually, at a minimum, to help all employees understand the importance of cybersecurity and how to prevent and respond to cyberattacks.

- **Free resources:** See EPA Cybersecurity Training and CISA's free Industrial Control Systems cybersecurity virtual training to learn how to protect against cyberattacks to critical infrastructure. Also see CISA's Secure our World Campaign: Employee Phishing Training for practical steps to help your employees avoid phishing scams.

Support

If you require additional support for implementing any of these actions, contact EPA and/or your regional CISA cybersecurity advisor for assistance.