United States Environmental Protection Agency

Cyber Security 101 for Water Utilities

Many drinking water and wastewater utilities today depend on computer networks and automated control systems to operate and monitor processes such as treatment, testing and movement of water. These industrial control systems (ICSs) have improved drinking water and wastewater service and increased their reliability. However, this reliance on ICSs, such as Supervisory Control and Data Acquisition (SCADA), has left the Water Sector and other interdependent critical infrastructures, including energy, transportation and food and agriculture, potentially vulnerable to targeted cyber attacks or accidental cyber events. A cyber attack causing an interruption to drinking water and wastewater services could erode public confidence, or worse, produce significant public health and economic consequences.[1]

Establishing facility and information access controls, which includes cyber security, is one of the Key Features of an Active and Effective Protective Program. The U.S. Environmental Protection Agency (EPA), in collaboration with the Water Sector, developed the Key Features to strengthen the security and resiliency of water systems in the face of all hazards.

THE KEY FEATURES

1. Integrate protective concepts into organizational culture, leadership and daily operations
2. Identify and support protective program priorities, resources and utility-specific measures
3. Employ protocols for detection of contamination
4. Assess risks and review vulnerability assessments (VAs)
5. **Establish facility and information access control**
6. Incorporate resiliency concepts into physical infrastructure
7. Prepare, test, and update emergency response and business continuity plans
8. Develop partnerships with first responders, managers of critical interdependent infrastructure, other utilities and response organizations
9. Develop and implement internal and external communication strategies
10. Monitor incidents and threat-level information

Types of Cyber Attacks on Water Systems

A cyber attack is an attempt to undermine or compromise the function of ICSs, or attempt to track the online movements of individuals without their permission. Attacks of this type may be undetectable to the water utility or SCADA system administrator but can lead to a total disruption of a water utility's network. Examples of these attacks include:

- **Denial of Service:** Flooding a resource (a network or Web server) with thousands of false requests so as to crash or make the resource unavailable to its intended users
- **Spyware:** Monitors user activity
- **Trojan Horse:** Malicious file or program that disguises itself as a legitimate file or program
- **Virus:** Attaches to existing programs, then replicates and spreads from one computer to another
- **Worm:** Malicious file that replicates itself and spreads to other computers
- **Sniffer:** Monitors information traveling over a network
- **Key Loggers:** Records and transmits keystrokes and transmits to the originator
- **Phishing:** Fake websites or e-mail messages that look genuine and ask users for confidential personal data

1 "Water Security Roadmap to Secure Control Systems in the Water Sector," developed by the Water Sector Coordinating Council Cyber Security Working Group, March 2008.

How Can Cyber Attacks Affect Water Systems?

Cyber incidents can affect water system operations in a variety of ways, some with potentially significant adverse effects to public health and the environment. Examples of potential impacts include:[1]

- Interference with operation of water treatment equipment, causing chemical over- or under-dosing
- Unauthorized changes to programmed instructions in local processors which enable individuals to take control of drinking water distribution or wastewater collection systems potentially resulting in disabled service, reduced pressure flows of water into fire hydrants, or overflow of untreated sewage into public waterways
- Changing or disabling alarm threshold, which could delay detection of intrusion or water contamination

Preventing Cyber Attacks

Water utilities can reduce vulnerabilities from cyber attacks or events by: (1) identifying systems that need to be protected, (2) separating systems into functional groups, (3) implementing layered or tiered defenses around each system, and (4) controlling access into, and between, each group. Utilities should also:

- Institute procedures to limit number of individuals with authorized access to networks
- Update software on a regular basis
- Require strong passwords
- Install and maintain anti-virus software
- Employ intrusion detection systems and firewalls

To be most effective, water utility cyber security programs should build on strong organizational security policies, utility-wide security awareness, and effective personnel and physical security practices.

Highlighting Real-World Cyber Attacks

The following are actual cyber incidents that impacted water utilities and illustrate the types of damages and impacts these attacks can cause:[1]

Queensland, Australia, 2001: Former employee of software development company hacked 46 times into the SCADA system that controlled a sewage treatment plant, releasing over 264,000 gallons of raw sewage into nearby rivers and parks.

Harrisburg, PA, 2006: Foreign hacker penetrated security of a water filtering plant through the Internet. The intruder planted malicious software that was capable of affecting the plant's water treatment operations.

Where to go for additional information on Cyber Security

Additional resources and guidance documents on cyber security applicable to the Water Sector include:

- **Water Security Roadmap to Secure Control Systems in the Water Sector:** Developed by Water Sector Coordinating Council Cyber Security Working Group, in accordance with the Department of Homeland Security's National Infrastructure Protection Plan partnership model: http://www.awwa.org/files/GovtPublicAffairs/PDF/WaterSecurityRoadmap031908.pdf
- **Water Information Sharing and Analysis Center (WaterISAC):** Secure, Web-based clearinghouse that helps water utilities, state and federal agencies, first responders, law enforcement, and public health officials prepare for water service interruptions: https://portal.waterisac.org
- **U.S. Department of Homeland Security, Control Systems Security Programs (CSSP):** Coordinates activities to reduce likelihood of success, and severity of impact, of cyber attacks against critical ICSs: http://www.us-cert.gov/control_systems
- **CSSP's Cyber Security Evaluation Tool (CSET):** Desktop software tool that guides users through step-by-step process to assess their control systems and IT network security practices: http://us-cert.gov/control_systems/satool.html

FOR MORE INFORMATION: EPA is committed to ensuring the Water Sector can access information and tools that enable utilities to enhance the security of their cyber systems. For more information on EPA's support for the Key Features of an Active and Effective Protective Program, visit http://water.epa.gov/infrastructure/watersecurity/features or email WSD-Outreach@epa.gov.