WaterISAC
Water Security Network

10 Basic Cybersecurity Measures to Reduce Exploitable Weaknesses and Attacks

According to the *2012 Data Breach Investigations Report*, 79 percent of data breach victims had computers or other systems with an easily exploitable weakness rather than being pre-identified for attack. 96 percent of victims succumbed to attacks that cannot even be described as highly difficult. As a result of its investigation, Verizon Business concluded that most data breaches are avoidable without difficult or expensive countermeasures.

WaterISAC, with the U.S. Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), the Multi-State ISAC, and the Information Technology ISAC, has developed a list of 10 basic cybersecurity recommendations water and wastewater utilities can use to reduce exploitable weaknesses and defend against avoidable data breaches and cyber attacks through basic measures.

Each recommendation is accompanied by links to corresponding technical resources[*].

1) Update systems and software
Set systems and software to auto-update to avoid missing critical updates. Vendors and security researchers identify new vulnerabilities in software and hardware products frequently, and without the proper updates your systems are open to attack via these vulnerabilities. Updates are designed to fix known vulnerabilities and should be done for any product that can access the Internet.
   - Recommended Practice for Patch Management of Control Systems (ICS-CERT)
   - Software Update Management Guidelines (Microsoft)

2) Use only strong passwords and change default passwords
Use strong passwords to secure your information, and keep different passwords for different accounts. Passwords should have at least eight characters and include uppercase and lowercase letters, numerals, and special characters. Change all default passwords upon installation, particularly for administrator accounts and control system devices, and regularly thereafter.
   - US-CERT Security Tip: Choosing and Protecting Passwords (US-CERT)

3) Apply firewalls to implement network segmentation
A firewall is a software program or hardware device that filters the inbound and outbound traffic between your network or computer and the Internet. Firewalls segment one large network into

[*] The technical resources published by the SANS Institute are used with permission. Analysis and recommendations in this document do not necessarily reflect the official views of the authors or organizations cited.

smaller functional networks so that if one segment of the network or a device is compromised, the threat cannot be spread to others as easily.

- Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies (ICS-CERT)
- Beginners Guide to Firewalls: A Non-Technical Guide (MS-ISAC)

4) Minimize network exposure for all control system devices

Conduct a thorough assessment of your system, including the business network and control system devices. Unless there is a compelling explanation, control system devices should not be accessible via the Internet. Those devices that must maintain accessibility should have role-based access controls and network segmentation, described in the document, to enhance security and be isolated from the portion of your network devoted to business and administrative operations.

- ICS-ALERT-12-046-01 Increasing Threat to Industrial Control Systems (ICS-CERT)
- ICS-ALERT-11-343-01A Control Systems Internet Accessibility (ICS-CERT)

5) Establish role-based access controls

Role-based access control grants or denies access to network resources based on job functions. This will limit the ability of individual users – or an attacker – to change security settings in your system. For example, SCADA system operators likely do not need access to the billing department or certain administrative files. Define the permissions based on the level of access each job function needs in order to perform its duties, and work with human resources to implement standard operating procedures to remove network access of former employees and contractors. By limiting employee permissions through role-based access controls it is easier to track network intrusions or suspicious activities during an audit.

- An Introduction to Role Based Access Control (NIST)
- Extending Role Based Access Control (SANS Institute)

6) Use secure remote access methods

The ability to remotely connect to a network has added a great deal of convenience for end users, but a secure remote access method, such as a Virtual Private Network (VPN), should be used if remote access is required. A VPN is a private data network that uses the infrastructure of the public Internet to transmit data in a secure manner. Through a VPN users are able to remotely access network resources like files, printers, databases or internal websites as if directly connected to the network. Note that a VPN is only as secure as the devices connected to it. A laptop computer infected with malware can introduce those vulnerabilities into the network, leading to additional infections and negating the security of the VPN.

- Configuring and Managing Remote Access for Industrial Control Systems (ICS-CERT)
- Virtual Private Networking: An Overview (Microsoft)

7) Do not open suspicious email or respond to suspicious phone calls

Phishing and social engineering are used by hackers and criminals to entice users to provide sensitive personal or corporate information like credit card numbers, account passwords or details about information technology infrastructure. Be cautious about email and telephone communications you receive asking for sensitive information, including those claiming to be from trusted entities such as corporate management. Avoid links or attachments that appear suspicious or unsolicited, and report all suspicious activity to the appropriate organizational representative and WaterISAC.

- US-CERT Security Tip: Avoiding Social Engineering and Phishing Attacks (US-CERT)
- Recognizing and Avoiding Email Scams (US-CERT)

8) Limit use of removable storage devices
Removable storage devices provide valuable functionality but are frequent carriers of malware. Lost or stolen devices can compromise sensitive data, and computers can be infected even without Internet access. The Stuxnet virus infected the Iranian nuclear facility through a USB device, and infected devices may be distributed at conference or industry events. Portable test equipment should also be considered a potential vulnerability for this reason.

- USB – Ubiquitous Security Backdoor (SANS Institute)

9) Develop and enforce policies on mobile devices
Proliferation of smartphones and other mobile devices combined with opportunities to bring personal devices into the workplace present security challenges. Develop policies that establish reasonable limits on the use of mobile devices in your office and on your networks and strictly enforce them with all employees and contractors. Password protect your own devices and be cautious about devices that do not belong to you as you cannot be sure they are properly protected or comply with established policy.

- Guidelines on Cell Phone and PDA Security (NIST)
- "Your Pad or Mine?" Enabling Secure Personal and Mobile Device Use on Your Network (SANS Institute)

10) Develop a cybersecurity incident response plan
Incident response plans are a critical yet underutilized component of emergency preparedness and resilience. The need for incident response plans applies to cybersecurity as well. Understanding and exercising the procedures that would be implemented in the event of a significant cyber disruption or breach of sensitive information will enable a more effective and efficient response within your organization.

- Developing an ICS Cybersecurity Incident Response Plan (ICS-CERT)

About WaterISAC

WaterISAC is the U.S. water sector's official terrorism and emergency response communications center. It is governed by a board of utility executives and a state drinking water administrator – all appointed by U.S. water and wastewater associations.

Thousands of staff with utilities and state, local, and federal government agencies in the United States, United Kingdom, Canada, New Zealand, Australia, and the Netherlands subscribe to WaterISAC Pro and Basic.

WaterISAC helps water and wastewater utilities measure and reduce risk, improve resiliency, prepare against acts of physical and cyber terrorism, and recover from disasters. WaterISAC also supports federal, state, and local government agencies involved in drinking water, law enforcement, intelligence, public health, and natural resources to support water and wastewater utilities, inform their own agency programs and initiatives, and otherwise protect public health and safety.

Using email and a secure web-based portal, WaterISAC Pro provides members with –

- Hundreds of guides and briefs on threats, disaster preparedness, and recovery;
- Terrorism threat alerts;
- Best practices and training from experts in the field;
- Webinars on threats, risks, and solutions;
- Sector-endorsed vulnerability assessment tools;
- Proprietary and federal databases on biological, chemical, and radiological agents;
- The water sector's only intelligence analysts, on call 24/7; and
- Weekly and monthly newsletters.

To login to the secure portal or to join, go to www.waterisac.org.

WaterISAC

866-H2O-ISAC | www.waterisac.org | info@waterisac.org
1620 I Street NW, Suite 500, Washington, DC 20006