BlastWave

Solution Brief

Navigating the Evolving Landscape:

EPA's Approach to Cybersecurity for Public Water Systems

The U.S. Environmental Protection Agency (EPA) has recently expanded the scope of its routine sanitary surveys of public water systems (PWSs) to include cybersecurity considerations.

The EPA introduced this scrutiny in a memorandum and a cybersecurity brief created for state officials. The EPA has since withdrawn this memorandum due to court order, but remains committed to achieving the goals detailed in its original mandate.

While these two documents released by the EPA have alerted PWSs to specific deficiencies, the responsibility of addressing and rectifying these deficiencies is still in the hands of the PWSs themselves.

10 Questions: EPA's Initial Cybersecurity Checklist for Public Water Systems

The EPA encourages states to proactively identify potential vulnerabilities in public water system cybersecurity by asking these questions:

01 **Inventory Management:** Have you cataloged all control system devices and isolated them from external networks?

02 **Network Segregation:** Have you classified IT assets and applied firewalls to segregate networks?

03 **Secure Remote Access:** Do you facilitate remote access only through secure methods?

04 **Access Roles:** Have you implemented role-based controls to manage network access based on job functions?

05 **Password Protocols:** Do you require the use of strong and diverse passwords for different accounts?

06 **Vulnerability Awareness:** Do you actively monitor and apply necessary system patches and updates?

07 **Mobile Device Security:** Have you instituted stringent policies for mobile device usage on networks, including password protection?

08 **Employee Training:** Do you provide regular cybersecurity training for all employees?

09 **Executive Involvement:** Are executives adequately informed and engaged in cybersecurity matters?

10 **Network Monitoring:** Can you quickly detect network intrusions and execute a response plan?

Understanding Significant Deficiencies in Cybersecurity

What is a “significant deficiency?”

According to the EPA, any design, operational, or maintenance flaws in a system—including breakdowns or malfunctions—that posed a contamination risk to the water supply were classified as a “significant deficiency.”

What is a significant deficiency in the realm of cybersecurity?

In the realm of cybersecurity, significant deficiencies might refer to a lack of security measures or existing vulnerabilities that present a high likelihood of being exploited. This could manifest in various ways, from the absence of secure remote access controls to unpatched systems vulnerable to cyberattacks.

Who is responsible for identifying deficiencies?

Although the recent withdrawal of EPA’s guidance has altered the formal role of states in identifying these deficiencies through sanitary surveys, the responsibility of PWSs remains unchanged. PWSs bear the duty of ensuring the safety of drinking water by identifying and addressing potential vulnerabilities in their systems.

Tackling EPA Cybersecurity Guidelines with BlastShield™

- Addressing these challenges within the intricate frameworks of PWSs can be daunting. However, BlastWave’s targeted solution supports the EPA's guidance and offers a direct route to robust cybersecurity measures.
- BlastWave BlastShield™ streamlines the process of securing the systems of a PWS by integrating multiple security controls into a unified solution.

Here’s how BlastShield helps:

Network Segregation:

BlastShield can segregate assets using micro-segmentation groups and zero-trust policy to provide isolation and local segmentation. BlastShield implements controls to prevent movement even within defined security zones, preventing users authorized on one system from accidentally (or purposefully) attempting unauthorized access to another nearby system.

- **Isolate control system devices:** The BlastShield Orchestrator offers a unified dashboard for managing Users, Agents, Groups, Policies, Services, and Proxies, ensuring each employee and vendor only has access to what they need and are authorized for.
- **Prevent Lateral Movement:** BlastShield actively prevents unauthorized internal movement on IT and OT networks, substantially reducing potential infiltration pathways to aid in monitoring networks for suspicious activity.
- **Segregate business enterprise and process control systems and require separate credentials for access:** Recognizing the need to separate business systems from process control mechanisms, BlastShield ensures a distinct boundary between IT and OT/ICS systems.

Secure Remote Access:

BlastShield outperforms traditional VPNs in performance and efficiency. It provides zero-trust remote access for each employee and vendor, ensuring secure and seamless entry with instantaneous access revocation to on-premise and cloud applications over the BlastShield network.

- **Eliminate Password Vulnerabilities:** BlastShield revolutionizes access security by introducing phishing-resistant, passwordless multi-factor authentication (MFA). This approach bypasses the pitfalls of traditional password management and ensures a more secure and user-friendly access experience.

Network Cloaking and System Security:

BlastShield expertly hides high-risk, unpatched, or inherently weak IT/OT systems, as well as outdated, unpatchable equipment within the protected network, rendering them invisible to unauthorized users.

- **Enhanced Infrastructure Integrity:** This strategic invisibility acts as a robust defense mechanism, shielding vulnerable systems from potential threats, ensuring uninterrupted business operations, and prolonging the lifespan of legacy equipment without the immediate need for patches or replacements.

Ready to Fortify Your Cybersecurity Posture?

With the heightened focus on the cybersecurity of PWSs, the importance of evolving cybersecurity measures has never been more pronounced.

It's not merely about adhering to safety suggestions—it's about envisioning a safer, more resilient public water system.

With BlastShield, integrating robust cybersecurity becomes part of a larger mission—a fortified, future-focused strategy that equally emphasizes business continuity.

Now, more than ever, is the time to reassess and fortify your cybersecurity measures for long-term resilience.

Schedule a Demo

Experience a seamless transition to becoming EPA-compliant with BlastShield. Simplify the path to compliance, save costs, and reduce cyber insurance premiums. Learn more and schedule a demo at https://www.blastwave.com/schedule-a-demo.