Cyber-Attacks Clogging the Safe Flow of Water

According to the U.S. Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), cyber incidents on industrial targets in 2014 had increased more than 25 percent since 2011. CS-CERT's latest report also said that in 40 percent of reported incidents, experts did not know how hackers intruded the system because of a lack of detection and monitoring capabilities.

It was also in this year when foreign attackers used a cyber-attack to damage a pump at an Illinois water plant— the first known kinetic attack on U.S. critical infrastructure.

The presence of kinetic attacks, cyber incursions that don't simply steal data, but actually affect the physical world, is a grave issue for critical infrastructure industries. In the water and wastewater industry, advancements in technology automation have dramatically increased productivity and reliability. However, an increased reliance on industrial control systems (ICSs), such as Supervisory Control and Data Acquisition (SCADA), has left this area of our nation's critical infrastructure vulnerable to both intentional, targeted cyber attacks as well as unintended cyber events.

A cyber-attack causing an interruption to drinking water and wastewater services would erode confidence in a bedrock public service, and could produce significant public health and economic consequences.

How Can Cyber-Attacks Affect Water Systems?

Cyber incidents can affect water system operations in a variety of ways— many of these have potentially significant adverse effects to public health and the environment.

Examples of potential impacts include:

- 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 resulting in disabled service, reduced pressure flows of water into fire hydrants, or overflow of untreated sewage into public waterways
- Changing or disabling alarm thresholds, which could delay detection of intrusion or water contamination.

What Are the Initial Steps that can be Taken to Protect Against Cyber Attacks?

To be effective, water utility cybersecurity programs must build upon strong organizational security policies, utility-wide security awareness of all threats – both

physical and virtual – and maintain effective security practices across both of these worlds.

Gray Matter Systems has more than 20 years of experience in the water and wastewater industry, delivering process automation solutions. Gray Matter Systems has recently partnered with Tempered Networks to provide a solution that secures ICS and SCADA environments for critical infrastructure industries including water and wastewater treatment plants. The solution gives service providers a simpler approach to security that bridges the gap between technology governance and operational goals, minimizing the likelihood and potential impact of cyber threats.

Segment and Cloak Process Control for SCADA Networks

The Gray Matter Systems solution establishes a private, virtual overlay network that enables utilities to segment and isolate connectivity to and between facilities and IPCs in any location, using any available physical network and an array of protocols.

The solution "cloaks" all devices within this private network, leaving no external access point for configuration to devices. The solution also leverages existing infrastructure to enable connectivity with remote sites and legacy devices over untrusted networks, without exposing device communications or requiring complex configurations.

Securely Connect and Monitor Water Control Stations and Remote Equipment

By introducing an independent layer of connectivity, security, and trust management, the solution enables the secure management of ICSs— even across third-party network infrastructure.

Utilities can easily connect and monitor upstream production equipment with centralized SCADA and Historian systems. The solution supports any mix of cellular, WiFi, wired Ethernet, or satellite communications networks, including failover to cellular connectivity if the wired network becomes unavailable.

In today's world, where kinetic threats are a real risk for critical infrastructure industries like water and wastewater processing, it is vital that service providers ensure that their industrial control equipment is protected while avoiding costly upgrades or replacement of older, insecure equipment. While there are many ways to address the problem, the use of private, virtual overlay networks is an innovative solution that meets these criteria by protecting industrial control endpoints regardless of their manufacturer, physical network infrastructure or function.

To learn more, register for a webinar: http://graymattersystems.com/cyber-security-for-water-wastewater-webinar/ or visit: www.graymattersystems.com, or by phone at 877-741-2410.