PLC Security for Water / Wastewater Systems

Executive Summary

You have likely never worried about the possibility of a high school geek doing some programming that affects your home water quality. Well, neither had I until I learnt that some municipal networks have no security between the network their schools use and the one that runs their water/wastewater facility.

This was the situation in a mid-sized city in the Eastern U.S. In 2012, the Department of Water Resources upgraded their SCADA network to industrial Ethernet. At the time, there was little protection or separation of the SCADA network from the city's IT network. While this provided many benefits, it also made the controls network susceptible to malware attacks and traffic storms.

Fortunately, the team involved, particularly the plant electronics technician, recognized the issue and took the initiative to review the situation and look for ways to improve security. What unfolded next is a great example of how multiple industry players, that is, a standards organization, a cyber security services group and a vendor were able to work together to provide a robust solution.

Figure 1 – Water / wastewater facilities, such as this one in San Francisco, typically may not have prioritized cyber security. Nowadays, however, attacks on PLC-based systems are increasing.

The Challenge

In the city in question, the Department of Water Resources oversees the city's water and wastewater treatment facilities, as well as the local reservoir, water lines, storm sewers, sanitary sewers and water meter reading. The system is complex:

- 24 buildings house more than
- 500 pieces of equipment that run the
- 15 processes needed to treat the
- 13 million gallons of wastewater each day. And that's 24 hours a day

Possible solutions included locking the wastewater treatment network down and adding air gaps to physically separate the control and business networks. The operations team, however, needed a networked solution that allowed them to share data interdepartmentally, maintain remote support capabilities and secure wastewater operations.

THE SOLUTION

Parts 1 and 2: ISA Industrial Cyber Security Course and Tofino Security products

The proactive plant electronics technician attended the International Society of Automation's (ISA) Water/Wastewater and Automatic Controls Symposium and participated in a one-day security course that taught him the fundamentals of the ISA/IEC 62443 cyber security standards. In addition, a neutral third party presented Belden's EAGLE Tofino product portfolio.

After reviewing several other options, the city staff selected to move forward with Belden's solution due to some specific benefits it could provide. These included:

The ease with which the Tofino Security products can be installed.

The ability to significantly restrict traffic on the programmable logic controllers (PLCs).

The "test mode" option that allows for testing before pushing live onto the system.

In the end, the local team purchased a Tofino Central Management Platform (CMP) and 13 Tofino Security Appliances with firewalls to secure each PLC on the network. If a PLC crashes, so does the entire system. The city has now specified that all processors will be protected by a Tofino firewall moving forward. They also keep spare products on hand for new PLCs in need of similar protection.

Part 3: Simple Installation and Expert Training from exida

After purchasing the products, the plant found the Tofino solution intuitive to install. Working with an electrician, the Tofino Security Appliances were easily wired into the network, but support was required when it came to configuring and managing the quantity of traffic their network was facing.

Through Belden's strategic partnership with exida – a firm specializing in industrial automation safety and cyber security services – Senior Cyber Security Engineer Eric Persson arrived on-site for two days of training and testing. The training included everything from baseline networking knowledge to hands-on installation and trouble-shooting.

"The goal of our training was twofold – first, to have fully functional Tofinos in place to protect the critical areas and assets of the plant from malicious traffic and activity, and second, to have our customer fully competent and comfortable in the networking and configuration knowledge necessary to maintain these devices moving forward," said Persson.

During the configuration, several key steps were taken to ensure no disruption to the active network. This included notifying the control room that maintenance was underway on the network and using the test and passive modes to see the traffic flowing through the Tofino before pushing in operational mode.

The training, commissioning and testing process also included the creation of custom rules to manage the facility's network traffic. Firewall and traffic rules were set up to meet their specific needs.

Finally, the exida team ensured that the security implementation met the recommendations of the ISA/IEC 62443 cyber security standards.

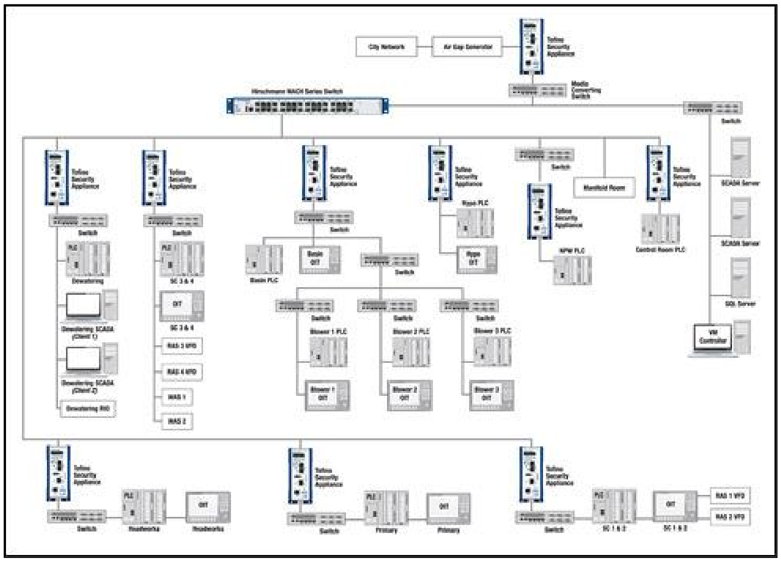

Figure 2: The SCADA wastewater network in this mid-sized U.S. city is segmented according to ISA/IEC 62443 standards and is secured using Belden's Tofino Security Appliances. Downloadable Image

RESULTS

Trained Staff and a Cyber Secure Facility

The local team's willingness to learn, coupled with exida's expertise on cyber security, Belden products, and interactive training, made for a successful installation.

As a result of the training and installation:

There is significantly less traffic on the plant's network. The Tofinos are operational and have been tested to confirm they are passing what is needed and blocking what is not. The team feels secure in managing the traffic themselves.

The Department of Water Resources is on the forefront of cyber security for industrial facilities. The network is very secure, making it impossible for even the internal IT department to impact the PLCs.

The plant is also meeting the guidelines and mandates for general wastewater practices and will be well prepared when those guidelines become law.

Into the Future – Deep Packet Inspection

There is an expression in the security business: “Security is a journey, not a destination.” Cyber threats to a city’s water system are constantly evolving, as new PLC vulnerabilities are discovered and new attacker’s toolkits are released.

The team at this particular plant is aware of these concerning facts and knows they cannot rest on their laurels. One of the next steps for them will be the addition of Deep Packet Inspection (DPI) technology to their firewalls.

This technology provides superior security over what can be achieved with conventional firewall solutions by performing multi-level analysis and filtering of network messages at the upper layers of the protocol. And unlike intrusion detection and prevention technologies, it offers very fast message forwarding for time sensitive applications, like SCADA control.

(For more information on this, see the Deep Packet Inspection Technical Kit available for download here.)

While this city’s water systems are now secure, facilities across the country and around the world likely are not. The good news is that securing them is not rocket science; it just takes one keen employee and good industry and vendor resources to call upon.

About Belden

Belden Inc. designs, manufactures, and markets cable, connectivity, and networking products in markets including industrial automation, enterprise, transportation, infrastructure, and consumer electronics. It has approximately 6,800 employees, and provides value for industrial automation, enterprise, education, healthcare, entertainment and broadcast, sound and security, transportation, infrastructure, consumer electronics and other industries. Belden has manufacturing capabilities in North America, South America, Europe, and Asia, and a market presence in nearly every region of the world. Belden was founded in 1902, and today is a leader with some of the strongest brands in the signal transmission industry. For more information, visit www.belden.com.

About the Industrial Internet Consortium

Belden has been a member of the Industrial Internet Consortium since June 2105. The Industrial Internet Consortium is a global public-private organization of over 140 members, formed to accelerate the development, adoption and wide-spread use of interconnected machines and devices, intelligent analytics, and people at work. Founded by AT&T, Cisco, General Electric, IBM and Intel in March 2014, the Industrial Internet Consortium catalyzes and coordinates the priorities and enabling technologies of the Industrial Internet. Visit www.iiconsortium.org.