Compiled by Amy McIntosh

Under Attack

Jonathan Pollet

Minimizing cyber security risks

As technologies advance, simplifying monitoring and operations for utilities, the risk of cyber attacks is becoming greater. Jonathan Pollet, founder of Red Tiger Security, shared some potentially devastating cyber threats, as well as useful security measures to keep the hackers away, with SWS Associate Editor Amy McIntosh.

Amy McIntosh: What are some of the major cyber threats that water utilities face?

Jonathan Pollet: Water utilities are at risk for dozens of different types of serious cyber attacks, and every year the threats become more sophisticated and dangerous. The biggest risk a utility can face is an attack that interferes with its physical operations, resulting in service denial, key safety process shutdowns or mistakes, or bodily harm to its workers.

This type of destructive attack is possible through a number of different ways. First, the industrial control system (ICS), such as a SCADA system, can be disabled or caused to malfunction through targeted attacks or malware. Another type of attack, the denial-of-service, can cripple the Windows-based networks used to run the utility. Additionally, "ransomware" and "wiper" malware can be used to hijack or destroy critical data and systems used to run these networks and machines.

McIntosh: What are common weaknesses found in water utility networks?

Pollet: The biggest mistake we find in these systems is a failure to anticipate a truly sophisticated attacker. Utilities are being probed constantly by state-sponsored groups, organized crime and other advanced actors.

A wide range of mistakes is common in these networks: old or outdated equipment; well-known vulnerabilities in the organization's Web apps that remain unpatched (or in other software programs widely used by employees and management); an ICS exposed to attackers due to failure to air-gap, change default passwords or install software updates; employee susceptibility to "phishing" e-mails and "drive-by download" attacks; failure to properly segment the network to prevent infections from spreading; not enough "access control" for employees; insufficient password policies, etc.

McIntosh: How can water utilities protect themselves from cyber attacks?

Pollet: Make sure you are at least compliant with the National Institute of Standards and Technology Cyber Security Framework, which establishes a number of minimum cyber security controls for devices connected to critical infrastructure systems.

Key to defending a utility against the worst type of cyber attack, which can interfere with physical operations, is to make sure you are protecting the controllers in all of the equipment. To that end, plant managers need to make sure key security features are supported within their hardware and software. It is preferred that these security features be pre-set at the factory to the maximum level, but allow flexibility to the user (the utility), so its team can log in and change these settings to better adapt them to their own environment. SWS

Jonathan Pollet is founder of Red Tiger Security. Pollet can be reached at info@redtigersecurity.com or 877.387.7733.

Amy McIntosh is associate editor for SWS. McIntosh can be reached at amcintosh@sgcmail.com.