In September 2007, an experiment called "Aurora" was made public. The project involved a Department of Energy laboratory in Idaho Falls, Idaho—with permission and funding from the Department of Homeland Security (DHS)—hacking into a power plant's control station via computers and digital devices. By doing this, the lab was able to change the operating cycle of a generator, thus severely damaging it and sending it out of control. In short, the lab turned a protective digital device into an attack device and destroyed a generator.[1]

By Clare Pierson

Is Your Plant Secure?

An update for plants and utilities; new information about cyber security

This event made clear that U.S. utilities, whether electric, nuclear or water/wastewater, have a long way to go in protecting themselves from these kinds of attacks—intentional or unintentional.

"Any device that is controlled electronically in water/wastewater facilities is at risk," said Richard Hein, global product manager at Cooper Power Systems.

Hein explained that there is a protection gap in any equipment that rotates. In the water industry, this could be pumps, motors or generators. This gap has existed and been known about, but the Aurora project exploited it fully for the first time. The gap is only about 15 milliseconds long, but severe damage can be done if it is exploited properly.

This information leads to the following questions: Who would do something like this, and why? Hein cited a few examples. In Europe, a group of Russian hackers recently took control of a municipality and turned off all of its lights from a remote location. The hackers then extorted more than $100,000 from the municipality in exchange for turning the lights back on. There was also a recent incident in Australia, where a disgruntled employee of a municipal wastewater station used his knowledge of its control system to discharge large amounts of wastewater into the nearby environment.

Consequences of these cyber attacks are that plants lose extremely valuable assets such as computer networks and actual equipment, environmental damage is caused, area security is threatened and monetary damage is most certainly done.

Taking Action

Cyber security breaches have increased substantially in the past few years. As a result, action has been taken to mitigate factors that could lead to these attacks. Water/wastewater treatment and controller and SCADA manufacturers have begun to offer security-related products.

An area of operation in water treatment plants that is particularly vulnerable is control systems and SCADA equipment. Damage to these systems can do serious harm to water plants that may require costly repairs.

Industrial Defender is a company that specializes in cyber security technology and services for water/wastewater plants in the municipal and industrial sector, as well as the power, oil and gas, and chemical sectors. The company offers real-time application platform (RTAP) technology software, a high-availability database designed for SCADA environments. The RTAP platform specializes in monitoring and controlling large-mission critical operations.

Industrial Defender also completes vulnerability risk assessments for water plants and facilities, where security experts from the company go in and look at the vulnerabilities of a plant's control and SCADA systems. The team will create a list of vulnerabilities and recommendations for technology that could mitigate them.

There are two types of vulnerability risk assessments: penetration and red-team, according to Todd Nicholson, chief marketing officer for Industrial Defender. Penetration teams are experts who have the goal of gaining unauthorized access to a network or computer system at a plant. Red-team assessments concentrate more on physical access to a plant, where an Industrial Defender team will attempt to gain authorized physical access into a plant and ultimately its computer network.

Red-team assessments have included Industrial Defender experts "pretending like they're employees, dressing in the proper uniform and hard hat or even hopping fences," Nicholson said. "With both types of assessment, more times than not we are able to gain access to networks and buildings."

Nicholson said the company is proud of its "defense in depth" approach, which consists of a vulnerability risk assessment followed by implementing the proper mitigation technology. Usually it begins with a firewall device that protects the network's perimeter. Then it deploys network- and host-intrusion technologies within the plant network to ensure all elements of the process control/SCADA system are adequately protected. For plants and facilities that do not have the knowledge or resources to support a comprehensive cyber security solution, Industrial Defender also offers a service that will monitor and manage these plants' control/SCADA systems 24 hours a day, seven days a week, year-round from the company's security operations center.

Cooper Power Systems also offers the rotating equipment isolation device (REID) relay that ensures security for pumps, motors, generators and other rotating equipment with high value and long lead times. The relay is supposed to protect from unwanted and unauthorized manipulation of the equipment's digital controls. Other companies like Hach Co. Homeland Security Technologies and Emerson Process Management have begun to offer products such as controller and firewall protection and real-time water security detection and response technology.

Getting Real

"For the water/wastewater sector, I can see a place like California—where they use large pumps to move material from place to place—as an area that could be vulnerable," Hein said. "These pumps need electricity and therefore are connected to a commercial grid. The many digital protective devices used at the facility or at the grid can be vulnerable. Also, any substations that use these devices are particularly vulnerable as well."

"Water utilities and plants should ask themselves, 'What is really critical that if I lose it, it will cause damage for a long time?'" Hein said.

Dan Kroll, chief scientist for Hach Homeland Security Technologies, said online monitoring technologies such as Hach's GuardianBlue have become popular in the past few years because they are "dual-use" products, meaning they are products already in general use within a plant to which security applications can be added for further benefit. This way plants get the benefits of increased security, improved water quality and the ability to meet more stringent environmental regulations.

"After 9/11, there was a huge awareness [regarding water plant security], but in the past few years there have been no major attacks, so that awareness has started to wane a little," Kroll said. "But there has been a spike in interest in the past few years in dual-use products."

The GuardianBlue system notifies plant operators in real time when water quality has changed dramatically. Programmed into this system are profiles of typical serious threat agents such as pesticides and other toxins. Even if utility operators think a terrorist attack is highly unlikely, they still need protection against random occurrences such as extreme weather events or broken water mains, which are much more likely to occur at some point.

Challenges

The banking, finance, telecommunications and electric companies in the U.S. have perhaps the most sophisticated cyber defense programs in place. Water/wastewater systems, however, lag behind, according to Hein.

Nicholson said that his company is seeing a trend where companies are moving to a "converged IT mode" and connecting enterprise, information technology and plant networks in order to drive higher levels of efficiency. While this is great for business, it has introduced greater cyber security risk into the plant's environment.

"Another trend which is introducing additional levels of risk is the effort to improve employee productivity by providing [more employees] remote access to the corporate network," Nicholson said.

"The biggest challenge for critical infrastructure industries is the ability to respond to the introduction of new levels of risk into the plant network environment," he said. "As the plant environment needs to increasingly connect to the outside world, they must continue to assess their cyber security protection strategy. They must also educate their IT staff on the unique requirements of protecting a process control/SCADA system. The mindset of playing the percentages and not taking action must change."

Perhaps this industry lags behind because the U.S. Environmental Protection Agency and DHS do not yet regulate cyber security for water plants. But probably the biggest obstacle for municipalities and utilities in getting the proper security measures is and has always been funding, said Kroll, although he said he is starting to see large cities and industries do more in-depth security planning with smaller cities watching and following their lead.

Small Steps

The Internet Security Alliance offers small businesses many steps they can take to improve cyber security. Although most of these steps focus more on Internet security and viruses, some are vital for the water industry.

These steps include: improve physical security around network equipment; give access—especially remote access—to as few employees as possible; create backup files of all important files; limit access to sensitive and confidential data to as few people as possible; establish and follow an emergency security breach plan; and finally, get help from outside sources when you do not have the knowledge or resources to protect yourself fully. WWD

References

[1] "Sources: Staged Cyber Attack Reveals Vulnerability in Power Grid." CNN.com. Sept. 26, 2007.

Clare Pierson is associate editor for *Water & Wastes Digest*. Pierson can be reached at 847.391.1012 or by e-mail at cpierson@sgcmail.com.

For more information, write in 1108 on this issue's Reader Service Card.

LEARN MORE
For additional articles on this topic, visit:
www.wwdmag.com/lm.cfm/wd040801