Angela Moscaritolo

February 01, 2010

Features

Critical condition: Utility infrastructure

Share this article:

- facebook
- twitter
- linkedin
- google
- Comments

- Email
- Print

When the FBI's Steven Chabinsky spoke recently to Congress, he shared a harrowing message, reports Angela Moscaritolo.

0210 critical opener

Individuals with ties to al Qaeda are interested in attacking United States critical infrastructure systems, Steven Chabinsky, the deputy assistant director of the FBI's Cyber Division, told the Senate Judiciary Committee in Nov. 2009. Terrorists have recognized vulnerabilities in the computer systems that control critical U.S. infrastructure systems, which could be leveraged to launch a devastating attack against our country, he said.

The FBI knows about and is investigating these individuals, he added, and have found that, currently, terrorist organizations do not have the high level of cyber-sophistication needed to launch such an attack. However, they are interested in developing their hacking skills.

“Should terrorists obtain such capabilities, they will be matched with deadly intent,” Chabinsky warned.

But, while terrorist organizations may lack the capabilities to launch a cyberattack against the nation's critical infrastructure now, there are others who don't. An increasing number of individuals, some working on behalf of foreign countries, have the resources to, in a worst-case scenario, manipulate the process control systems that regulate U.S. critical infrastructure systems, causing widespread outages and catastrophic effects.

A primary risk the nation faces is that many of the Supervisory Control and Data Acquisition (SCADA) systems – used to manage electric power generation plants, water systems, oil and gas pipelines, and other systems – are becoming interconnected with enterprise networks, making them accessible from the internet, says Alan Paller, director of research at computer security training organization SANS Institute.

“The vulnerability is that there is a bridge between the business systems and the systems that control the power, distribution and production,” Paller says.

Moreover, these process control systems were not engineered to operate as part of a corporate network, experts say. They are often 10 to 20 years old and are not regularly patched like typical computer systems, says Robert Brammer (*right*), vice president for advanced technology and CTO at Northrop Grumman Information Systems.

Others in the field concur. “Security was never built into the systems that manage our critical infrastructure,” says Steve Santorelli, a former Scotland Yard detective who is the director of global outreach at Team Cymru, a Chicago-based nonprofit IT security research company. Also, certain parts of process control systems are accessible through wireless connections and other unencrypted communication channels, which can be tapped into, Paller adds.

In the energy sector, for example, many of the systems that are required for power, production, transmission and distribution of energy are computerized, says Amit Yoran, chairman and CEO of network security monitoring vendor NetWitness. Adding to the risk factor, the computer systems that run physical cable plants, turbines and other equipment, have, over the past decade, become increasingly interconnected in ways for which they were not originally designed.

The owners of critical infrastructure systems, approximately 85 percent of which are companies in the private sector, have a good business reason to connect process control systems to their enterprise networks, experts say. Connecting them to corporate billing systems, for example, can make the organization more efficient. But since the systems are interconnected, an attacker could access a system by first making their way into the enterprise network.

To achieve that, an attacker would most likely use a socially engineered ploy to infect an end-user's computer with malware, which would provide the initial entryway into the enterprise network, says Eddie Schwartz, CSO of NetWitness. The primary objective of an attacker is to get an initial foothold into the enterprise network, he says. From that point, owing to the interconnectivity of systems, that intrusion can eventually lead into a SCADA system.

However, the scenario is not all doom and gloom. Should an attacker gain remote access to a process control system, total calamity is not guaranteed, says Levi Gundert, a former U.S. Secret Service agent who is the director of fraud cyber intelligence at Team Cymru. It may be possible to completely shut off electricity remotely, he says, but doing so would require detailed knowledge of the control system.

In its favor, the various controls in SCADA systems are very granular. Each piece of hardware performs a specific function and is generally responsible for a small percentage of the overall electric output. So, if a remote intruder were able to shut down one control system, the overall impact to electricity delivery may be relatively manageable, Gundert says.

Power penetration

However, attacks from outside the system are not the only worry. There is always the risk posed by insiders, particularly with the recent penchant for outsourcing IT services overseas, and that might just compound and complicate these issues in the long run. A rogue insider would likely have the critical knowledge of exactly how the control systems work together and which are the most high-impact targets, Gundert adds.

For these reasons, the critical U.S. infrastructure is a prime attack target, experts say. Furthermore, there is reason to believe that hackers have a foothold in U.S. critical infrastructure systems right now, Paller says.

“There is reasonably good evidence that nation-states have been taking remote control of computers and power companies for years,” he says. “If you were a country that might have to go to war with another country, you would put spies in place to map the power systems, identify the weaknesses, and pre-place weapons so that if and when you go to war, you are prepared to do real damage.”

This past April, for example, it was widely reported that intruders, believed to be from China and Russia, hacked into the U.S. power grid and left behind malicious software that could be activated at a later date to disrupt the nation's electric system. Federal intelligence officials – not utility companies connected to the grid – detected these compromises. While saying there was no immediate threat, they cautioned that if there was a war, the hackers may try to “turn on” the malware left behind.

“This is real stuff happening,” says NetWitness' Schwartz. Officials in the government and the power companies need to take these issues very seriously, he warns.

Steps being taken

And steps have been taken by owners of critical infrastructure to mitigate the vulnerabilities, but much more work is needed, experts say.

“There's been a move to retrofit security [into process control systems], with varying degrees of success,” Team Cymru's Santorelli says. “The security discussion has been going on for years in very closed security communities.”

Seth Bromberger, director of the Energy Sector Security Consortium (SEC), a nonprofit whose mission is to facilitate information sharing among those interested in protecting the power grid, says cybersecurity is a top concern of power companies. “We have made significant strides in protecting our infrastructures,” he adds. As an example, Bromberger explains that the industry collaborated with the North American Electric Reliability Corp. (NERC) – the organization that sets and enforces standards for power company owners, operators and users that comprise the bulk power system – to draft the Critical Infrastructure Protection (CIP) Reliability Standards. These standards contain roughly 40 requirements which serve as a foundation to secure the electric critical infrastructure from cyberthreats.

Team Cymru's Gundert sees progress as well. “NERC and the Department of Homeland Security (DHS) continue to work toward increased security awareness, and companies continue to improve security strategies,” he says.

In contrast, Paller argues that critical infrastructure owners and operators have spent more time denying that vulnerabilities exist than they have fixing them. In addition, they have hired lobbyists to ask Congress to block various security initiatives, claiming there is no real problem.

“The penetrations that have already taken place are being denied,” Paller says.

Securing critical infrastructure systems against cyberattacks is far from a high priority for electric power companies. These utilities are more concerned with the cost of fuel and an aging infrastructure, says Northrop Grumman's Brammer. “They would acknowledge that it is a theoretical threat, but it is not high on their list to worry about. A lot of these threats only become real in retrospect.”

The mindset in the utilities industry is that an attacker could do equal damage by launching a physical attack, says Brian Ahern (*left*), president and chief executive officer of Industrial Defender, a provider of cybersecurity solutions for SCADA systems.

But, denial is the least expensive solution. Critical infrastructure operators are able to deny the problem because they don't have hard evidence that their systems have been penetrated, Paller says.

Getting secure

Complying with security best practices, such as those set forth by NERC, is often a very costly process, Gundert adds.

“Cost will always be a driving factor for utility companies – they are, after all, a business at the end of the day,” he says.

The solution, he suggests, is that governments around the world should provide incentives that encourage organizations to secure their existing infrastructures, along with any technologies they are planning to implement in the future.

Ahern agrees, saying that when it comes down to it, the only way to truly mitigate the risks is for those in the private sector to take action to secure the infrastructures they control. However, SANS' Paller says it's up to the vendors to ensure security, pointing out that vendors of critical infrastructure process control and business systems need to take responsibility for delivering systems that are harder to penetrate.

“The procurement of new technology and every maintenance contract for every one of these control systems needs to have a much higher level of security built into it,” Paller says. “You can change your procurement quickly, whereas regulations take years to become part of the fabric of organizations.”

While individuals have differing

views as to what needs to happen to secure critical infrastructure systems, all agree that a greater level of information-sharing among members of the private and public sectors is needed.

“The best thing we can do as an industry is keep talking, communicating and working as a partnership,” says EnergySec's Bromberger.

[sidebar]

IN THE WORKS: New legislation

Currently, there are several pending bills related to critical infrastructure cybersecurity making their way through the federal government. Those applying to the energy sector include the following:

Critical Electric Infrastructure Protection Act, introduced in April, would give the Federal Energy Regulatory Commission, the U.S. agency responsible for overseeing electric rates and natural gas pricing, the authority to issue emergency rules if a cyberthreat is imminent.

Bulk Power System Protection Act of 2009, introduced in April, is similar to the bill above but would give FERC the authority to take emergency measures lasting up to a year.

American Clean Energy Leadership Act of 2009, in July was placed on Senate Legislative Calendar. It is a comprehensive energy bill that includes cybersecurity provisions similar to the bills, but establishes cybersecurity jurisdiction within the Department of Energy, instead of the Department of Homeland Security.

From the February 2010 Issue of SCMagazine »