Cyber attacks: Is your critical infrastructure safe?

PricewaterhouseCoopers

A new breed of hacker threatens essential US infrastructure

In late October 2009, US utilities, manufacturers, and technology firms received $3.4 billion as part of the economic stimulus package. These funds are to be used to modernize the country's electric power system and increase energy efficiency. But as these "smart-grid" grants continue to be awarded, questions are being raised about how to safeguard smart meters and other critical infrastructure from cyber attack.

The threat of cyber attack is increasingly coming from a broader range of individuals and entities. This new breed of hacker understands cyber vulnerabilities and how to exploit them. And they play by a new set of rules.

As a result of this new threat, Congress is considering numerous bills to strengthen the Federal Energy Regulatory Commission's (FERC) ability to impose cyber security rules and potentially establish an Office of the National Cyber Security Advisor.

The proposed legislation aims to protect critical infrastructure, including:

- Electricity generation, transmission, and distribution
- Gas production, transport, and distribution
- Oil and oil products production, transport, and distribution
- Telecommunication
- Water supply (drinking water, waste water/sewage, and stemming of surface water such as dikes and sluices)
- Public health (hospitals, ambulances)
- Transportation systems (fuel supply, railway network, airports, harbors)
- Financial services (banking, clearing)
- Security services (police, military)

The energy and utility industry also is undergoing a multitude of challenges.

- Energy companies face cost control and regulatory constraints as they are increasingly pressured to demonstrate environmental leadership through use of smart grids, intelligent utility networks, emissions monitoring, and advanced water management, all of which require a secure, scalable infrastructure.
- Operational systems are increasingly subject to cyber attacks, as many are built around legacy technologies with weaker protocols that are inherently more vulnerable. In fact, since 2000, the number of successful cyber attacks has increased tenfold against Supervisory Control and Data Acquisition (SCADA) systems at power generation, petroleum production, and nuclear plants and water treatment facilities.
- Utilities must also comply with North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards, which require implementation of security management controls and new systems to meet the requirements.
- Although primarily directed toward chemical companies, utility, energy, and manufacturing companies may also be subject to compliance with the Chemical Facility Anti-Terrorism Standards (CFATS).

Emerging threats

In March 2007, an experiment conducted by the Idaho National Labs demonstrated that a large diesel generator could be severely damaged by exploiting a computer vulnerability. Named the "Aurora Generator Test," the experiment revealed that physical damage could be done through the computer system. The results of this test elevated the cyber attack threat to a new level. Prior to conducting the test, utility companies had focused primarily on protecting their physical assets from more conventional attacks.

In April and June 2009, The Wall Street Journal reported that Russian and Chinese spies had penetrated the US electrical grid and that the NERC was teaming with a defense contractor to create an initiative to evaluate power companies' ability to withstand cyber attacks. On November 8, 2009, *60 Minutes* aired an episode discussing the vulnerabilities of the power grid and other critical infrastructure.

The *60 Minutes* episode, along with FBI reports, confirmed that hackers had targeted and compromised large banks and other companies resulting in significant financial losses and reputational damage. The banking industry generally is regarded as being more secure than any other, lending credence to the suggestion that the exposure to cyber attack is real for other industries, including US energy, water, and electrical power sources.

Today's new breed of hacker, who is sophisticated, educated, and well funded, may have less difficulty getting into the network of a utility or energy company system and staying there, undetected.

Why are operational systems vulnerable?

Operational systems are the systems that monitor and control the infrastructure. These systems include SCADA systems or Distributed Control Systems (DCS).

In the energy and utility industry, there are several examples of SCADA or DCS systems, including the systems that control generation plants or refineries, computers that manage the flow of oil and gas through pipelines, and the energy management system that controls the power grid. These systems have been in place for years and are essential for the operation of plants and the electric grid; however they largely have been ignored from a security perspective. This was partially because the systems were physically separate from other networks and often used proprietary communication protocols. However, like many systems, these operational systems have become increasingly complex. The physical network boundaries have all but disappeared, and standard communications infrastructure is now commonly used.

Additionally, because these systems are operational systems, they are typically maintained by engineers at the plants or by the operators running the grid. Because the number and variety of users is small, the computerized controls that are standard for financial systems (such as formal segregation of duties and robust user management) historically have not been implemented on these systems. Many legacy systems (because of age or design) may also not support such technical controls. The FERC (via NERC) and the Department of Homeland Security (DHS) only recently began to regulate the security of these systems.

Homeland Security weighs in

DHS, under Homeland Security Presidential Directive-7, identifies the energy sector (electricity, petroleum, and natural gas) as a critical infrastructure asset "so vital to the United States that its incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof."

DHS has not mandated cyber controls over these assets, except for chemical facilities where DHS created the CFATS, which establish risk-based performance standards for the security of chemical facilities. It requires covered chemical facilities to prepare security vulnerability assessments, which identify facility security vulnerabilities, and to develop and implement site security plans. Most of the CFATS relate to the physical security of the plants, but a small section addresses cyber security of the assets.

NERC Critical Infrastructure Protection Standards

Understanding the new threats to the operational environments, NERC has begun to devote more effort to these issues. Several years ago the NERC released the CIP standards to address the security around these systems. As of this year, most utilities have implemented controls to address these standards for those components of the systems that are deemed "critical," based on the definition within the standards.

A concern, however, from the CIP perspective is that utilities are left to their own discretion in determining which assets are actually "critical." This potentially leaves a host of systems not covered and presumably less secure.

What can be done?

Companies should start by assessing their overall security posture with regard to SCADA and DCS environments. This should include reviews of controls' design and threat-based penetration testing to simulate actual attacks. If the controls are not as strong as they should be, companies should implement controls for systems that adhere to a robust framework, such as ITIL or COBIT. Utilizing these types of frameworks will provide a secure and flexible model, which may help companies adhere to new or changing regulations. Additional resources are also available from the Department of Commerce, National Institute of Standards and Technology, the Defense Information Systems Agency, and other industry organizations and associations.

Regardless of an organization's perception of the strength of its control environment, it should consider performing tailored forensic analysis procedures on the network and key servers to determine whether there is evidence of a breach.

This process is more difficult to accomplish because of the nature of today's advanced threats. The attacks are very sophisticated and are often company-specific, so commercial software—such as virus protection or intrusion detection systems—likely will not identify an attack or evidence of a breach. Companies may have to team with a service provider that has in-depth experience responding to such advanced threats. The network traffic analysis is relatively nonintrusive; however, assessing a system may require a full forensic image of the server. Due to the real time and "always available" nature of these systems, acquiring these images requires careful coordination and a skilled project team.

A question of privilege

When a breach occurs, many companies hire service providers through legal counsel to maximize the ability to claim privilege over the work performed. Although it may be advisable to do the same while companies are looking for possible breaches, companies should discuss the pros and cons of privilege prior to evaluating potential service providers.

Security program resources

Taking a "compliance approach" to security (i.e., doing the minimum to comply with NERC CIPS or CFATS) is not the most effective use of resources given the potential operational and reputational risks involved with these threats.

Security breaches of several prominent payment card industry-compliant companies reiterate the point that compliance does not ensure security. Companies should design their security capabilities using a flexible framework such as ITIL or COBIT to provide a solid, controls-based foundation to work from and should help minimize rework as regulatory requirements change.

Companies may also want to leverage information available from the Defense Information Systems Agency's Security Technical Implementation Guides as well as the Department of Commerce National Institute of Standards and Technology publications. These resources provide technical guidance on how to secure specific systems and resources. Additionally, professional organizations such as the Institute of Electrical and Electronics Engineers, American Gas Association, American Petroleum Institute, and International Electrotechnical Commission have informative, industry-specific international standards.

How PwC can help

PricewaterhouseCoopers has a long history of helping energy and utility companies understand their security landscape and helping management align security needs with business requirements. Across these and other industry sectors, we have helped our clients analyze and respond to targeted attacks. This experience helps us understand gaps in standard safeguards and how to build enhanced safeguards to bridge these gaps.

We understand current attack trends. As part of our cyber intrusion response practice, we have helped our clients understand and recover from the effects of an advanced attack. We understand the latest defensive countermeasures. As a leading provider of security assessment and implementation services, we know what it takes to design and implement effective information security.

As a security adviser, PricewaterhouseCoopers' first concern is to help organizations appraise their security landscape and improve their security posture by making the most of existing solutions. We take the time to help you understand and protect your information environment.

For more information, contact:

Brad Bauch
Principal, Energy and Utilities Advisory
(713) 356-4536
brad.bauch@us.pwc.com

Dave Burg
Principal, Forensic Services
(703) 918-1067
david.b.burg@us.pwc.com

Less Stoltenberg
Director, Energy and Utilities Advisory
(713) 356-4469
less.j.stoltenberg@us.pwc.com

www.pwc.com