Sharing threat data is key to securing the power grid

By **WILLIAM JACKSON** // **SEPTEMBER 24, 2009**

An electrical power industry consortium is creating a forum to help share information about cyber threats to the nation's power grid, a growing concern as our critical infrastructure becomes increasingly interconnected.

COMMUNICATIONS NETWORKING CYBERSECURITY IT INFRASTRUCTURE - TELECOM SECURITY

The ability to share timely information about threats is critical in securing the nation's critical infrastructure. But in the power industry, exchanging data through the traditional channel, the Electricity Sector Information Sharing and Analysis Center, is complicated because the ISAC is managed by the North American Electric Reliability Corp., the industry's designated international self-regulatory authority.

Seth Bromberger, director of the Energy Sector Security Consortium (EnergySec), has been involved in network and systems security for more than 16 years. EnergySec is a not-for-profit consortium, a member-driven organization created to foster the exchange of security information among energy asset owners, industry, and government.

GCN: How interconnected is the nation's power grid? Is it essentially a single nationwide grid?

BROMBERGER: The power grid is regionalized; it is not a single nationwide grid. There are inter-ties between three main regions, the Western, Texas, and Eastern.

How exposed is the grid to the Internet?

In general, the systems used to control the stability of the grid, and the systems that are critical to the reliable operation of the transmission networks, are not publicly accessible. They may use third-party networks for data transit, but in those cases, they're linked via [virtual private network] or are otherwise segregated from the Internet.

What is EnergySec?

EnergySec is a non-profit organization dedicated to the exchange of security information among asset owners, industry partners, and the U.S. government. It started in 2005 as E-SEC NW, which was an informal gathering of utility security, operations, and compliance professionals in the Pacific Northwest. Since that time it has grown to over 220 members across this country and in Canada whose organizations represent about one-third of the power generation in the United States, and almost half of the distribution.

is EnergySec needed?

EnergySec fills the need to share threat and vulnerability information — it's what our organization was created to do. Because EnergySec was established by professionals who work for asset owners and understand the unique environments in which we work, the trust among the membership is inherent to the organization. Providing the ability for the members to share information in an open, non-threatening way, and without worrying about where else their information might be disclosed, is part of what makes EnergySec successful.

What is the organization doing? How well is it working?

We're sharing information and exchanging ideas, and doing it pretty effectively. We've seen rapid growth in membership over the past several months. When our information sharing portal went live in June, we anticipated it would take about a year to see a doubling of our membership. We exceeded that goal within three months.

The volume and quality of information being shared continues to be high. [Recently], we've seen over three dozen posts on compliance issues, new security vulnerabilities, situational awareness reports, secure code development and auditing techniques, and other items of interest to the membership.

Has it improved security in the industry?

We think it has, primarily by getting folks talking and exchanging ideas. Our annual summit gives members an opportunity to meet face to face with their peers in the utility space, in government, and in the security industry; we're arranging hands-on demonstrations of security products and techniques, and the ideas shared both on the portal and at the summit should give members new insights on how to secure their own environments.

You have said of information sharing, "if we can't make it work in the energy sector, it's not likely to work anywhere else." Are there any lessons here for other sectors of our critical infrastructure?

I think there are a couple of lessons we learned as the organization grew. First is that you can't just start something like this and expect folks to jump on board. The success of our organization is due to the fact that it was a grass-roots effort from the beginning and still is, despite the formalization of some of the processes and structures.

Second, it's a unique model. EnergySec is not run by a for-profit company; incorporation came as a result of the growth beyond the original membership. We developed and continue to grow based solely on the needs of the members. The members *are* the organization.

Why do we need a smarter grid?

What people are calling the "smart grid" has benefits across the board. On the one hand, the new metering platforms, which are just one component of the smart grid, provide consumers the ability to make more informed decisions regarding their use of this resource. On the other hand, a massive deployment of smart grid technology allows the providers of the power to gain a much finer-grained understanding of what the power use should be in order to optimize their generation, and to respond to fluctuations in supply and demand in a much more rapid fashion. There are other side benefits as well—the ability to determine, for example, exactly where and how many customers might be experiencing an outage, and from that information to be able to infer something about the cause of the outage. These benefits can be achieved because of the proliferation of devices that act both as monitors and sensors.

Does this increase the risks?

It really depends on how you define the risk. From a security perspective, I think it's fair to say that deployment of this technology poses new challenges for our industry. These challenges aren't necessarily new by themselves, but we've never really had to focus on them within the utility space until now. Some of the security issues are just increases in existing risk, but there are some that represent new risks, and fortunately, we've got folks from academia, government and industry working on them right now.

Every decision has its risks and rewards; it's the analysis that's important. That is, whether it makes sense to follow a course of action and incur a specific set of risks given the benefit of that action. The best we as security professionals can do right now is to ensure that the security risks are identified in a timely manner and to work to mitigate them as much as possible.

NEXT STORY: NIST targets security steps for a more mobile WiMAX

DOD asset-tracking tool wins Kantara award for innovative ID management

By **WILLIAM JACKSON** // **SEPTEMBER 17, 2009**

The Defense Department's Synchronized Pre-Deployment and Operational Tracker earns the Kantara Initiative's Identity Deployment of the Year award for its innovative use of Web-based technology to track contractor assets in the field.

AUTHENTICATION AUTHENTICATION OR IDENTITY MANAGEMENT

BUSINESS SUPPORT SYSTEMS OR QUALITY METRICS DEFENSE

LOGISTICS INFORMATION SYSTEMS NON-COMBAT TECHNOLOGIES

A Defense Departmet asset-tracking tool has won the Kantara Initiative's Identity Deployment of the Year award for its innovative use of Web-based technology.

DOD developed the Synchronized Pre-Deployment and Operational Tracker (SPOT) system under a 2005 congressional mandate to better track and manage contractors and assets being deployed abroad with U.S. forces.

“We wanted better contract visibility to allow contacting officers, planners and commanders to see what is available now, down to the job skill level of the people, and how it can be leveraged for greater economy,” said Lt. Col. Richard Faulkner, SPOT program manager.

SPOT went operational in 2007, and has since been serving the State Department and USAID for identifying contract assets abroad.

SPOT is a Web-based enterprise networking solution for precise tracking and management of overseas assets. It was developed and launched by a collaboration between DOD and the Federation for Identity and Cross-Credentialing Systems Inc. (FiXs). It recognizes identity credentials issued by various government entities, as well as compatible certified identity credentials issued by the private sector.