Dan Kaplan, Executive Editor

May 08, 2009

The energy sector needs information sharing, too

Share this article:

- facebook
- twitter
- linkedin
- google
- Comments
- Email
- Print

If there was one buzzword during the recent RSA Conference that permeated across the session halls at the Moscone Center (and likely even reached the bar at the W), it was information sharing.

The concept is pretty simple, really. For a discipline as young but profoundly complicated as information security to succeed, communication is key. Because, in the end, information systems all touch each other and, really, we're all in this together.

(Insert image of IT admins sitting around a campfire singing "Kumbaya.")

Of course, getting people into a room and talking about breaches they've had or threats they've seen is inherently complex because of things like fear of punishment, competition, and classified documents.

But mostly everyone has recognized that information sharing is an absolute must if America is to keep up with the sophistication of hackers, some of whom are state-sponsored and thereby threatening the very foundation of the country as a whole.

Perhaps in no other industry is protecting the networks as fundamentally important to the nation's day-to-day living than the electric grid. But as we know, this sector is far from immune from the wrath of cybercriminals, as SCADA control systems are now being built on top of traditional operations systems, such as Windows or Linux, which contain IP-based components.

In other words, the networks tasked with keeping the lights on are susceptible to the same types of attacks that can impact an average business.

One organization has been quietly meeting over the last several years to make sure these critical systems stay protected. Now, they're ready to let everyone know about them.

The Energy Sector Security Consortium, or EnergySec, is made up of about 75 of the power sector's 1,800 asset owners - but now they are trying to "scale" out and reach a wide audience. (Scalability: another RSA buzzword, by the way).

The goal of the organization is to, you guessed it, share information. But here's why they may succeed at it.

According to Chris Jager, the group's chairman, and Seth Bromberger, its director, the energy sector doesn't compete - therefore, asset owners are more likely to collaborate. And with no fear of sanctions, they may be more willing to volunteer the type of information that could prevent another power company from suffering the same type of attack.

Jager says the energy industry has had a tough time responding to today's security threats because many of the publicized events have been based on unnamed sources and classified information. EnergySec, however, wants it members to feel comfortable detailing specifics of a breach so that the group can better arm its members with information.

"We're not interested in putting any names in lights," he says. "It's more like these types of incidents have occurred and this is how you should mitigate your exposure."

And EnergySec can also value the government by providing them with real-time and historical data that they can use to "validate or nullify some of the assertions they're making concerning threats and vulnerability," Jager says.

If there is any industry that needs some cold, hard facts about hacker attempts, it's energy. And it sounds as if EnergySec is going to help sound the alarm on an increasingly worrying situation.

"There are people poking at these networks," Jager says. "That's real."