Schneider Electric

The Global Cyber Advisor

Invensys Critical Infrastructure & Security Practice

November 2014
Issue 38

this issue

Survey says: power grid, oil and gas production most vulnerable to cyber attack

From www.fiercesmartgrid.com, 11/12/2014

The Department of Homeland Security said that more than 40 percent of industrial cyber attacks in the United States targeted the energy industry in 2012, the last full year reported. "Cyber attacks are a clear and present threat to every industry, in every country throughout the world," said Michael Chertoff, co-founder and executive chairman of the Chertoff Group, and former head of the U.S. Department of Homeland Security. "This threat is real and industries need a proactive and coordinated approach to protect their assets as well as their intellectual property. We have seen a number of attacks to critical industries in areas like the Middle East and the U.S. and these have had major impacts on their operations."

Cyber Security Best Practices

As 2014 comes to a close, it's easy to see that the predictions and warnings from security experts for increased cyber attacks were no joke. Retailers like Neiman Marcus, Aaron Brothers, Michael's, Home Depot and numerous others had credit card systems compromised. A handful of unnamed public works companies were hacked according to the Department of Homeland Security. Restaurants, postal and shipping services (UPS and USPS), and banks were also no exception to this past year's slew of cyber onslaught. It seems no industry was spared from malicious cyber events.

It is easy to get caught up in the doom and gloom of today's cyber news. The good news is there is something you can do—beginning with cyber security best practices. Whether you are embarking on a NERC CIP (fossil power) or NEI 08-09 (nuclear power) compliance program or just looking to strengthen your existing corporate internal policies, cyber security best practices provide a solid foundation to build from.

In many cases, people are unknowingly their own worst enemy, keeping the same password for months or even years or hiding it on a sticky note under their keyboards at work. Additionally, there are a number of cyber security issues that many companies do not address but should. One of these is keeping automatic updates current. One of the largest malware threat vectors is Adobe. If you do not keep your Adobe product current through updates, you are leaving yourself open to malware. These automatic updates apply to operating systems, anti-virus software, and other critical software and hardware that is running on your network.

Unfortunately, there is no "one box does it all" cyber security product on the market. Any comprehensive cyber security solution will address a security-in-depth strategy. This means you cannot just deploy an anti-virus product and be secure or just deploy a firewall and be secure. Cyber security compliance must address the totality of the network and uniqueness of the industry regulations that will be governing the overall acceptance.

Cyber security solutions are cannot just be installed and then left to protect the network in question. Cyber security solutions are only as effective as the management systems used in conjunction with them. Virtually every aspect of a cyber security solution generates logs that must be monitored for events and actions that must be taken. Effective cyber security is an active pursuit—not a passive pastime.

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
November 2014 / Issue 38

Industry News

Cyber attack causes major breach of software controlling critical U.S. infrastructure

From www.waterworld.com, 11/7/2014

The Department of Homeland Security (DHS) recently announced that much of the critical infrastructure in the U.S., including major water and wastewater systems, has been jeopardized by a destructive computer malware program. The "BlackEnergy" virus -- allegedly carried out by Russian-affiliated hackers, according to authorities -- stems from a 2011 hacking campaign and was also used earlier this year against NATO and other organizations in a similar cyber-attack.

ABC News noted that the Trojan horse has breached integral software used to operate a variety of national industrial processes that include water distribution networks, water and wastewater treatment systems, oil and gas pipelines, wind turbines, power grids, and nuclear plants. The malware, although not yet live, can activate anytime and leave these processes susceptible to failure or malfunctioning. For example, it can cause water facilities to flood, generators to power down or pipelines to shut off, posing a high economic and environmental risk to the nation.

Middle East oil and gas industry urged to stay on top of growing cyber security challenges

From www.zawya.com, 11/9/2014

The Middle East's oil and gas industry was praised for its recent cyber security initiatives but urged to maintain vigilant against a rising tide of targeted and fast -changing threats. According to a recent global study by PwC, last year saw a 179 per cent rise in the number of reported cyber-attacks on oil and gas companies, which soared above 6,500 cases. Frost & Sullivan has also reported that cyber security uptake is expected to surge with the passing of national and international legislation and awareness-raising initiatives and that, ultimately, the issue would emerge as "the highest-priority area for oil and gas companies." The oil and gas industry cyber attack playbook could include anything from distributed denial-of-service (DDoS) attacks and phishing/spear-phishing emails to data theft, "zero-day" software assaults, web application exploits, and website defacement.

Nukes getting second-to-last cyber check

From thehill.com, 11/6/2014

The government is putting $12 million toward completing its cybersecurity vetting of nuclear power plants. The Nuclear Regulatory Commission (NRC) has awarded a contract to test nuclear plants' compliance with the final phase of a cyber security program launched in 2009. At the start of the program, nuclear plants were given a generic cyber security template, which they were required to fill in with their own cyber defense tactics. NRC has been periodically checking in since then. This newest round of inspections comes ahead of a final check by the NRC next year.

'Trojan Horse' Bug Lurking in Vital US Computers Since 2011

From abcnews.com, 11/6/2014

A destructive "Trojan Horse" malware program has penetrated the software that runs much of the nation's critical infrastructure and is poised to cause an economic catastrophe, according to the Department of Homeland Security. National Security sources told ABC News there is evidence that the malware was inserted by hackers believed to be sponsored by the Russian government, and is a very serious threat. The hacked software is used to control complex industrial operations like oil and gas pipelines, power transmission grids, water distribution and filtration systems, wind turbines and even some nuclear plants. Shutting down or damaging any of these vital public utilities could severely impact hundreds of thousands of Americans. DHS said in a bulletin that the hacking campaign has been ongoing since 2011, but no attempt has been made to activate the malware to "damage, modify, or otherwise disrupt" the industrial control process. So while U.S. officials recently became aware the penetration, they don't know where or when it may be unleashed.

BlackEnergy malware threat has some uneasy

From powersource.post-gazette.com, 11/11/2014

A malicious software dubbed BlackEnergy has intrigued and frightened cybersecurity experts, in part because of its intent and in part because of its origin. BlackEnergy is designed to target critical energy infrastructure and is believed to have originated with Russian government-sponsored hackers. The Department of Homeland Security's Oct. 29 cyber threat alert was, unfortunately, business as usual for many of the nation's companies. However, with the potential attack on water, electricity and other features of the nation's critical infrastructure linked to Russian cyber criminals, security practices within private companies have become the public's business.

Schneider Electric

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
November 2014 / Issue 38

Cyber News

Major cyber attack will hit in next 11 years

From www.usatoday.com, 11/1/2014

Almost two-third of technology experts expect a "major" cyber attack somewhere in the world that will cause significant loss of life or property losses in the tens of billions of dollars by 2025. A survey released by the Pew Research Center found that many of analysts expect disruption of online systems like banking, energy and health care to become a pillar of warfare and terrorism. The survey asked over 1,600 technology experts whether a major attack that would cause "widespread harm to a nation's security and capacity to defend itself" would be launched within the next 11 years. Sixty-one percent said yes.

Online security experts link more breaches to Russian government

From www.nytimes.com, 11/1/2014

For the second time in four months, researchers at a computer security company are connecting the Russian government to electronic espionage efforts around the world. In a report released by FireEye, a Silicon Valley firm, researchers say hackers working for the Russian government have for seven years been using sophisticated techniques to break into computer networks, including systems run by the government of Georgia, other Eastern European governments and militaries, the North Atlantic Treaty Organization and other European security organizations. The researchers have made the government connection because the malicious software used in the incidents was written during Moscow and St. Petersburg working hours on computers that use Russian language settings and because the targets closely align with Russian intelligence interests.

War and terrorism will start taking place as cyber attacks

From www.pfhub.com, 11/1/2014

Major attacks are coming to some part of the world in the next decade that will wreak havoc of epic proportions and cause an immense sum of life and tens of billions of dollars in damage. This may sound like a warning for a nuclear threat, but in fact, according to a new study, cyber attacks will be the cause of this destruction. A new study released by the Pew Research Center entitled “Digital Life in 2025” discovered that two-thirds of more than 1,600 technology experts are in agreement that cyber attacks will produce disruptions in various spheres of everyday life, such as banking, energy and healthcare, which all three will become a considerable element to war and terrorism.

The bill for cyber security: $57,600 a year

From www.businessweek.com, 11/1/2014

Hackers have made the Internet a scary place to do business, as recent headlines attest. Big companies have been hacked. Small companies have been hacked. As the Pew Research Internet Project reported last month, cyber attacks are likely to get worse. How much should a small business spend to protect against cyber villains? While the answer will vary, depending on the type of business—not to mention the relative optimism of its owner— Eric Montague, president of Executech, an IT firm in South Jordan, Utah, offers a useful baseline: Some $57,600 a year for a 50-employee company.

State Dept. restores email after cyber attack

From thehill.com, 11/18/2014

The State Department said its external email system was back up Tuesday following a cyber breach.The department took the system offline Friday in order to bolster security measures following a breach discovered late last month. It called the move an update that was part of a "scheduled outage." "I can report that our external email services from our main unclassified system are now operating normally," State Department spokesman Jeff Rathke said.

Postal Service Hit By Cyber Attack

From abcnews.com, 11/10/2014

The U.S. Postal Service said it has been the victim of “a cyber-security intrusion” that exposed the personal information of some 800,000 employees. The FBI is investigating the source of the attack, but a source briefed on the incident told ABC News it appears to have originated in China and has been going on for the last two months. The USPS said on its website that the intrusion “is limited in scope and all operations of the Postal Service are functioning normally.” Employee information, like names, addresses and Social Security numbers, may have been compromised, the USPS said.

Schneider Electric

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
November 2014 / Issue 38

Are Firewalls and Anti-Virus Products Relics of the Past?

With data diodes and whitelisting, are firewalls and anti-virus products the "dinosaurs" of the security industry? What are data diodes and whitelisting?

Data diodes are devices that ensure that network traffic does not occur in both directions over physical network media between a trusted and untrusted network. They also tend to involve servers that simulate the two-way traffic that some systems need and interact with them. The servers then send only the data that matters over the diode. These solutions are very secure as they stop things at the physical media, but just like with new modern medicines, there are several "side effects:"

- The servers involved need the necessary "plugin" to simulate the two-way traffic needed by some applications.
- Deployment can become expensive if you have business needs for limited two-way traffic between your trusted ICS network and the untrusted corporate network. In some cases you would need four or more pieces of equipment to avoid having a person or specialized solution "flip a switch" every time two-way communication is needed:
    - A "sender" on the trusted network
    - A "receiver" on the untrusted network
    - A "sender" on the untrusted network
    - A "receiver" on the trusted network
- Some applications refuse to work with this technology, so additional software may have to be purchased and alternate communication paths established to "tunnel" this information.

Whitelisting involves taking a profile of a PC to determine all the software and scripts running on it. Once this profile or "snapshot" is taken, no other applications introduced to the PC can be run unless they are "profiled". On the surface this sounds like a stop-all to viruses and malware, but once again there can be "side effects:"

- "Profiling" a PC can be a lengthy and sometimes inaccurate process:
    - It is best to know when scheduled tasks are set to run on a PC. Sometimes these scheduled tasks run on an infrequent basis and must be captured in the whitelisting profile so they are not forbidden to run. What makes this tricky is sometimes applications have poorly documented or hidden scheduled tasks that you may not be aware of.
    - Setting a PC "profiling" window can be a delicate balancing act. If it is too short, you don't capture needed applications in the profile. If it is too long, you run the risk of approving rogue applications you don't want in the profile or even viruses and malware.
    - Setting a PC to ask for approval to add every new running application to the whitelist profile can become overwhelming. While it may be the more accurate method of approving applications (asking for approval instead of carte-blanche approving), it would require a large amount of administrative overhead for someone to review and approve all application whitelisting requests.

In summary, while data diodes and whitelisting are valuable tools in your security toolbox, for some customers the administrative cost of owning these technologies could be very high. Through a measured, risk management approach, your site may serve well with a firewall and anti-virus without data diodes and whitelisting.

This month's contributor to Consultant's Corner is Charles Smith
Consultant, Critical Infrastructure & Security Practice, Invensys
charles.smith@schneider-electric.com

Schneider Electric

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
November 2014 / Issue 38

Most Popular Blog Posts This Month

New York financial regulator pushes banks to plug gaps in cyber security (October 27, 2014)
Following the massive cyber attack on the biggest U.S. bank JPMorgan Chase & Co (JPM.N) disclosed in August, and other financial institutions, government authorities in United States are pushing financial institutions and brokerage houses to close glaring gaps in cyber security.

12 percent of businesses have no cyber attack defenses (November 7, 2014)
Twelve percent of financial executives surveyed said their companies have no cyber attack defense plans. Other findings from the Association for Financial Professionals survey:

- 62 percent of businesses have been subject to a cyber attack or an attempted attack during the last year.
- 71 percent of companies have increased spending to combat attacks, with 25 percent increasing it by at least 50 percent.
- 15 percent have increased their cyber insurance.
- 31 percent carry no cyber insurance.

Add data breaches to holiday shopping stress (November 4, 2014)
With the holiday shopping season on the horizon, many retailers soon will be dishing out deals and special promotions to get shoppers in the spending spirit. But what consumers seem to really want for Christmas this year is to keep their personal financial information out of the hands of hackers. CreditCards.com, a credit-card comparison website, recently conducted a survey of 865 credit and debit card holders, and 45 percent said they would not shop this holiday season at retail chains that had been affected by major data breaches.

10 ways to protect your devices and data (November 19, 2014)
Gee, it used to be just your desk computer that needed protection from cyber thugs. Now, your connected thermostat, egg tray monitor, teen's smartphone, garage door opener, even baby monitor, are all game for cyber creeps.

Featured Post: Small firms also face cyber attack

It's not just big businesses such as JPMorgan Chase, Target, Neiman Marcus and Home Depot that are hacked. Small companies suffer from intrusions into their computer systems, too. The costs associated with computer and website attacks can run well into the thousands – and even millions – of dollars for a small company. Many small businesses have been attacked – 44 percent, according to a 2013 survey by the National Small Business Association, an advocacy group. Those companies had costs averaging $8,700. Click here to read the full story.

Visit us on Blogger!

Schneider Electric

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
November 2014 / Issue 38

Critical Infrastructure and Security Practice (CISP)

Invensys CISP has capability in establishing, implementing and maintaining industry best practices to meet the demands for government regulations (NERC-CIP, NEI 08-09, CFATS), industry requirements and company compliance requirements. Attributes of Invensys CISP Critical Infrastructure Consulting include:

Hardware Independence

CISP can work with any type of control system or type of technology a customer prefers for the security environment.

Regulation Knowledge

CISP has a number of subject matter experts who understand a whole host of regulatory requirements as well as active participation in a number of industry and government groups.

Technical Knowledge

The same CISP personnel who have regulatory knowledge are also well versed in the latest security policies, procedures, and technologies for intrusion detection and prevention, firewalls, DCS, and network architecture.

Join us on Blogger!

Industry Knowledge

CISP has a number of resources that understand the demands of Controls Networks and the requirements for continued uptime.

Proven Methodology

CISP follows a proven life cycle methodology to support the implementation of a comprehensive successful cyber security program. Attributes of the life cycle approach are Assessments, Development, Implement and Management.

Schneider Electric

For additional information please visit us at
http://iom.invensys.com/CyberSecurity

1820 Preston Park Blvd. Suite 1900 Plano, TX 75093 ▪ P 469.365.6400 ▪ F 888.758.7675 ▪ **iom.invensys.com**