Schneider Electric

The Global Cyber Advisor

Invensys Critical Infrastructure & Security Practice

March 2014
Issue 30

National electric grid remains at significant risk for cyber attack

From www.infosecurity-magazine.com, 3/6/2014

Evidence collected by the U.S. Department of Homeland Security (DHS) suggests that cyber attacks on key energy infrastructure—and on the electricity system in particular—are increasing, both in frequency and sophistication. And worryingly, new research shows that the risk of a successful large-scale cyber attack, or combined cyber and physical attack, on the electric power sector is "significant." Urgent priorities include strengthening existing protections, for the distribution system as well as the bulk power system; enhancing coordination at all levels; and accelerating the development of robust protocols for response and recovery in the event of a successful attack.

this issue

Businesses Worldwide Amp Up Cyber Security

According to a recent report from the Bipartisan Policy Center, a Washington, DC think tank founded by former leaders of the U.S. Senate, the energy sector was the target of more than 150 cyber attacks last year alone. With that in mind, and the likelihood of cyber attacks in 2014 continuing to increase, businesses have begun to grasp the importance of strengthening their cyber security programs and adopting the belief that it is no longer a question of "if" but "when" their systems will be compromised by hackers, and how they will deal with the aftermath of an attack.

With the value of the cyber security market projected to grow to $77 billion this year, many American companies have begun to view cyber attacks as one of the top three business risks. 60 percent of U.S. businesses have increased or plan to increase their cyber security budgets, with many claiming to have been influenced by the recent attacks on banks and retail giants such as Target. 29 percent of respondents estimated a successful cyber attack could cost their organizations more than $75 million, and almost half said it could cost more than $15 million.

Even in the UK, some 60 percent of the UK FTSE 100 companies now highlight cyber security in their annual reports, an increase of 11 percent from 2012, with the most dramatic increases in the healthcare, oil and gas, and consumer goods industries. And in Australia, 64 percent of businesses surveyed said that they had increased their cyber security budgets with the expectation that cyber attacks would increase over the next two years. 55 percent said their greatest concern is the loss of customer data.

Security experts continue to warn that internet security in 2014 will only get worse. According to Trend Micro, "From mobile banking vulnerabilities and targeted attacks, to growing privacy concerns...2014 promises to be a prolific year for cybercrime." A good cyber security program is not just firewalls and anti-virus software, but a combination of things, such as hardware, software solutions, policies and procedures, and employee behavior. The "insider threat" remains one of the largest concerns among companies today, as well as unsecured networks, BYOD, data privacy in the cloud, data regulation, mobile malware.

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
March 2014 / Issue 30

Industry News

LightsOut is latest cyber threat to target energy sector

From www.infosecurity-magazine.com, 3/15/2014

What happens when the energy grid goes down? Well the lights, of course, go out. A fresh advanced persistent threat (APT) targeting the energy sector is thus aptly named LightsOut, and like previous attacks, it used a watering hole method to start its system compromise. LightsOut performs several diagnostic checks on the victim's machine to make sure that it can be exploited. This includes checking the browser and plugin versions. And ultimately, a payload is delivered from the LightsOut Exploit kit, which attempts to drop a malicious JAR file. LightsOut is only the latest watering hole-oriented attack on the sector. Earlier this year it was discovered that "Energetic Bear" was making the rounds, an adversary group with a nexus to the Russian Federation that conducts intelligence collection operations against a variety of global victims, with a primary focus on the energy sector.

Power companies struggle to maintain defenses against cyber attacks

From insurancenewsnet.com, 3/24/2014

When experts rank U.S. industries' abilities to ward off potentially damaging cyber attacks, the electric utilities are normally near the bottom. One of the issues is that there is no sense of alarm. A terrorist group or nation state has heretofore not switched off a power grid. That doesn't mean that they aren't vulnerable, said Curt Aubley, chief technology officer and North American vice president at McAfee. And new smart power grids, which will rely on Internet protocols to connect homes and businesses to the energy plants, may complicate matters. Many of the technicians who operate the SCADA systems are reluctant to update the software because they don't know what the full impact will be on the grids.

Energy companies can't get cyber attack insurance because their defenses are too weak

From www.slate.com, 3/1/2014

Lloyd's of London is so concerned about digital security at energy companies that it won't sell most of them insurance, even though there is a growing demand. BBC News reports that Lloyd's underwriters are getting more and more requests for cyber attack insurance from energy groups, but the insurer is unwilling to take the risk after assessing the companies' defenses. That means that the protections currently in place by energy companies must be horribly inadequate. Laila Khudari, an underwriter at a Lloyd's of London syndicate, told BBC News that Lloyd's has negotiated cyber attack insurance with energy companies in the past, but that they aren't qualifying for the multimillion-dollar policies they want now because the defenses they have in place aren't adequate, which has already been reported in other contexts.

Industrial Control Systems (ICS) security market worth $10.33 billion by 2018

From www.itbusinessnet.com, 3/7/2014

The major forces driving the ICS security market are the increased threat of cyber attacks across the energy and power sector, government pressure and security compliance and regulations, threats from terrorist attacks and cyber attacks, lack in comprehensive solutions for ICS security, and insider threats. Companies providing cyber security solutions are looking to gain a better competitive advantage in this growing market, thereby creating comprehensive security solutions and integrated security management platforms for the industries and critical infrastructures. The global ICS security market is estimated to be $7.02 billion in 2013 and is expected to grow to $10.33 billion in 2018.

Report calls for better backstops to protect power grid from cyber attacks

From www.nytimes.com, 3/2/2014

Despite rising anxiety over the possibility of a cyber attack on the power grid, the industry and government are not set up well to counter the threat, according to a report produced by leading energy security experts. Companies are reluctant to share information with one other, a critical step in reducing vulnerability, because they are afraid of being accused of failing to comply with cybersecurity rules, committing antitrust violations or giving away proprietary information, the report found. And the federal rules intended to protect the electric system from cyber attacks are inadequate because they do not give companies an incentive to continually improve and adapt to a changing threat, according to the report.

Schneider Electric teams with McAfee to expand cyber security capabilities

From www.renewgridmag.com, 3/19/2014

Energy management specialist Schneider Electric and McAfee, a part of Intel Security and wholly owned subsidiary of Intel Corp., have come together to provide cyber security solutions for the utility and critical infrastructure market. According to the companies, the collaboration will enable Schneider customers to add tested and certified application whitelisting capabilities in the management of core offerings of water, oil and gas, electric networks, and transportation infrastructures.

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
March 2014 / Issue 30

Cyber News

California launches cyber attack awareness campaign

From www.fiercecio.com, 3/6/2014

In response to growing IT security threats against government agencies, public corporations and private institutions, the State of California has launched a campaign to better educate organizations on the cyber security threats they face and steps they can take to better safeguard themselves. The "Cyber Security in the Golden State" report was jointly issued by the state attorney general's office, the California Chamber of Commerce, and IT security firm Lookout. This is the "first-ever report from any attorney general in the U.S. on cyber security, detailing how essential security is to business in California and across the country," the report noted.

Cyber attacks a growing risk in the Middle East

From www.thenational.ae, 3/4/2014

Businesses in the Middle East are facing a growing risk of cyber attacks, says an annual security report. Total global threats have reached their highest recorded level, increasing 14 per cent from 2012 to last year, according to the Cisco 2014 Annual Security Report. A sample of 30 of the world's largest Fortune 500 companies generated visitor traffic to websites that host malware, with a sharp rise in malware attacks on the Middle East's oil and gas sector. "Organizations across the Middle East and Africa must realize that it is no longer if they will be targeted by cyber attacks, but when," said Rabih Dabboussi, managing director at Cisco UAE. The report says the Middle East and Africa region posts a strong adoption of smart devices, set to grow from 133 million this year to 598 million in 2018. But that also means more complex security threats. Businesses across the Middle East are at high risk, with 65 per cent of employees not understanding the security risks of using personal devices in the workplace, Cisco's recent Middle East ICT Security Study says.

DDoS Cyber Attacks Get Bigger, Smarter, More Damaging

From www.nbcnews.com, 3/5/2014

Distributed Denial of Service (DDoS) attacks have always been among the most common on the Internet, using hijacked and virus-infected computers to target websites until they can no longer cope with the scale of data requested, but recent weeks have seen a string of particularly serious attacks. On February 10, internet security firm Cloudflare says it protected one of its customers from what might be the largest DDoS documented so far. At its height, the near 400 gigabyte per second (gbps) assault was about 30 percent larger than the largest attack documented in 2013, an attempt to knock down antispam website Spamhaus, which is also protected by Cloudflare. A report this month by security firm Prolexic said attacks were up 32 percent in 2013, and a December study by the cyber-security-focused Ponemon Institute showed them now responsible for 18 percent of outages at U.S.-based data centers from just 2 percent in 2010. The average cost of a single outage was $630,000, it said.

Ukraine hit by cyber attacks, MPs' phones blocked

From www.smh.com.au, 3/5/2014

Ukraine's telecommunications system has come under attack, with equipment installed in Russian-controlled Crimea used to interfere with the mobile phones of members of parliament. Some internet and telephone services were severed after Russian forces seized control of airfields and key installations in Ukraine's Crimea region on Friday, but now government officials were being targeted, said Valentyn Nalivaichenko, the head of Ukraine's SBU security service. "At the entrance to [telco] Ukrtelecom in Crimea, illegally and in violation of all commercial contracts, was installed equipment that blocks my phone as well as the phones of other deputies, regardless of their political affiliation," he said.

Baroness fires cyber attack warning

From www.yorkshirepost.co.uk, 3/7/2014

BRITAIN must be braced for a cyber attack aimed at crippling its military, industry, and energy supplies during times of crisis, according to the former chairman of the Joint Intelligence Committee. Baroness Pauline Neville-Jones delivered a stark warning about the scale of the threat from cyber criminals when she spoke in Yorkshire last night. The Baroness, who was delivering the annual public lecture at The Grammar School at Leeds, said the command and control structures of Britain's armed forces must be secured from "penetration and interference." She said, "The Russians attacked the electronically run government services of Estonia over a trade disagreement; they disabled some of the capability of the Georgian armed forces when they invaded South Ossetia and I expect they will be doing the same to the Ukrainian armed forces."

Businesses brace for increase in number of cyber attacks in 2014

From formtek.com, 3/14/2014

Analysts are predicting that in 2014 the number of cyber attacks attempted will only grow in number. Security provider McAfee predicts that "the poor cyber security foundations of many companies will continue to create an environment of high motivation, high opportunity for the attacker in 2014. Businesses need to understand that lax cyber security could have significant implications on their company data, operations and financial viability." The analyst firm VisionGain estimates that the value of the global cybersecurity market in 2014 will reach nearly $77 billion.

Schneider Electric

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
March 2014 / Issue 30

Remote Connectivity in SCADA and Control Systems

In recent years, with the prevalence of new technology, plug and play, and networked devices, remote connectivity is becoming a much more common and convenient feature for administering a plant's SCADA or control systems. Unfortunately, along with this convenience comes a host of new cyber security issues. Recent studies have found thousands of internet-facing SCADA or control system devices that could be exploited from anywhere in the world. To ensure that a business is not susceptible to this, proper network and device configuration is incredibly important.

One of the simplest ways to deal with remote connectivity vulnerabilities is to close off the control networks and remove any connections from other networks or the internet from them. However, doing this removes a lot of functionality that operation and maintenance staff have likely come to rely on. To securely allow remote connections, what is known as a De-Militarized Zone (DMZ) can be set up, which will create a buffer network between a control system network and a corporate network, which can allow for a secure connection between these two networks. Generally, this is achieved through the use of a "jump" server. Users on the corporate network connect to the jump server, which will then allow connectivity to the assets on the control network. By utilizing a properly configured DMZ, an outside attacker has to go through multiple layers of complex security to access your assets, while still allowing employees to use these remote features in a secure manner.

In addition to using a DMZ, proper configuration of SCADA and control system devices is very important. In the default configuration, most SCADA or control system devices are susceptible to a wide range of attacks, the simplest of those is through the use of the default administrator user name and password, which are easily found on the internet. Properly hardening these devices, which includes updating user accounts, patching the device, and disabling any unnecessary features, can greatly increase the security posture of a SCADA or control system.

Taking the precautions of using a DMZ and properly configuring SCADA and control system devices can prevent a remote attacker from compromising these systems. Completing a project to properly configure a SCADA or control system and to implement a DMZ, a company can ensure that it's most important industrial assets are protected, while still allowing the convenience of modern remote connectivity for authorized users. For assistance in developing and deploying these types of solutions, the Invensys CISP team has completed both of these hardening activities at numerous sites across many industries.

This month's contributor to Consultant's Corner is Gary Kneeland
Consultant, Critical Infrastructure & Security Practice, Invensys
gary.kneeland@invensys.com

Schneider Electric

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
March 2014 / Issue 30

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.

Industry Knowledge

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

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.

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,

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!

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**