The Global Cyber Advisor

Invensys Critical Infrastructure & Security Practice

July 2014
Issue 34

this issue

Reports reveal ongoing cyber attacks on U.S. and European energy sector

From www.washingtonpost.com, 7/1/2014

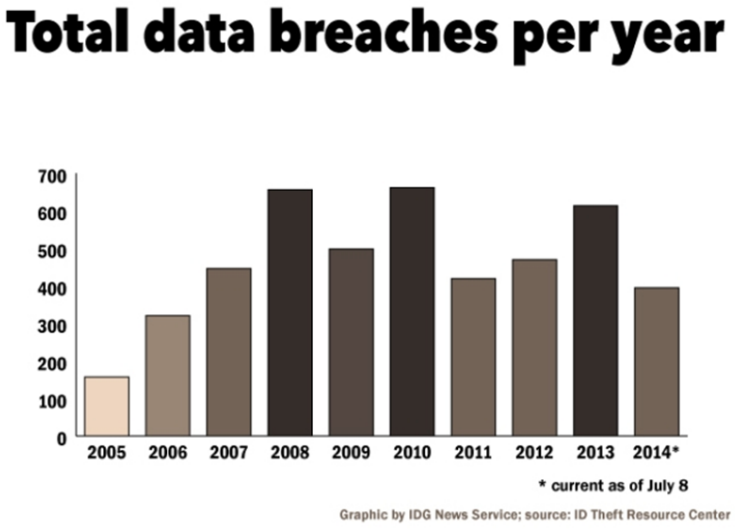
Hackers likely linked to a foreign government have targeted U.S. and European energy sector companies in an escalating industrial espionage campaign, according to reports from private cyber security researchers. The report prompted the Department of Homeland Security to issue an alert. The group, dubbed "Energetic Bear" or "Dragonfly" by different security firms, has targeted primarily oil and gas companies but also health care, government and defense contractors. The attacks include phishing scams in which malicious links were sent via mass e-mails. In others, the hackers infected Web sites their targets visited often, tricking them into downloading malware that gave hackers access to their computers.

Invensys is becoming Schneider Electric

The Biggest Data Breaches of 2014

Now that we are more than halfway through 2014—a year many security researchers predicted to have an increased onslaught of cyber attacks—reports are surfacing that detail some of the largest breaches that have occurred just over the last seven months. According to the Identity Theft Resource Center, there has been a 21 percent increase in the number of data breaches, at a current total of 395, and that number doesn't include unreported attacks. This year's World Economic Forum ranked cyber attacks among the top 5 global risks in terms of likelihood in its annual report (weforum.org). And research from Arbor Networks states that "the number of DDoS events topping 20Gbps in the first half of 2014 are double that of 2013" (forbes.com). Some security researchers speculate that hackers are not the only threat; poor security practices and simple mistakes are quickly becoming just as hazardous. Some of the biggest data breaches of 2014 (computerworld.com) include:

- Retail giant Michael's, whose sales systems were compromised with malware that resulted in exposure of up to 2.6 million credit card numbers and their expiration dates
- eBay, whose majority of its 145 million members had personal information compromised, such as birthdates, addresses, phone numbers, and passwords
- Montana Department of Public Health and Human Services, when names, birthdates, and Social Security numbers of 1.3 million people were accessed after a server was compromised
- Variable Annuity Life Insurance Co., after a former employee was caught with a USB drive that contained full and partial Social Security numbers of its 774,723 customers
- Spec's, a Texas wine retail chain, which lost information belonging to as many as 550,000 customers, including bank information, driver's licenses, and credit and debit card numbers after a 17-month-long attack on their network
- P.F. Chang's, whose point-of-sale machines were hacked, credit and debit card information obtained, and then sold for between $18 and $140 per record (forbes.com)



The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
July 2014 / Issue 34

Industry News

Modern electric grid fights cyber vulnerabilities

From www.emergencymgmt.com, 7/23/2014

The recent push to modernize the electric grid has increased communication between utilities and consumers, enhanced reliability and created more opportunities for green energy producers. But it also has raised the risk of cyber attacks. New technology, while largely beneficial for utility companies and their consumers, has created millions of new access points that make the grid vulnerable. Utility companies are spending millions annually in cyber security costs, and the trend will continue with investments in smart meters and other technology meant to bring the electric grid up to date.

Energy sector leaders still not taking cyber threats seriously

From www.nationaldefensemagazine.com, 7/15/2014

Companies and organizations in the energy sector remain vulnerable to cyber attacks, which could result in the loss of intellectual property and leave critical infrastructure prone to damage, according to a recently released study. Many of the world's utility, oil and gas, energy and manufacturing companies have immature cyber security programs, according to a survey sponsored by Unisys and conducted by the Ponemon Institute. It polled 599 info-tech executives in 13 countries. Most respondents reported that security programs in their companies were unorganized and ill-equipped to handle network and other kinds of computer intrusions.

Preparing for cyber warfare

From www.chicagotribune.com, 7/22/2014

Recently, emboldened Russian hackers breached the systems of power plants across the United States and Western Europe. In June, Chinese hackers attempted to gain access to several U.S. power plant operation control systems. And in May, the Department of Homeland Security announced hackers had actually gained control of a mechanical device at an unnamed U.S. energy facility. These brazen cyber attacks on a critical infrastructure have raised new alarms within the information and homeland security sectors. Following other recent high profile data breaches at private companies such as Target, Michaels, and eBay, and the digital bomb that was left in NASDAQ in 2011, the question is being raised – is America prepped to handle a contemporary cyber war?

US unprepared for cyber attack

From www.globalpost.com, 7/23/2014

The United States has failed to sufficiently adapt to new cyber-security threats, exposing itself to potential terror strikes as devastating as September 11, authors of the report on the 2001 attacks warned. In July 2004, the independent 9/11 commission issued a comprehensive, nearly 600-page report with numerous recommendations for upgrading the US security apparatus to avoid a new catastrophe. A decade later the commission's former members have released a blunt follow-up, pointing out gaps in US security that increase the risk of cyber attacks on infrastructure, including energy, transport and finance systems, and the theft of intellectual property from the private sector. After exhaustive meetings with national security officials, "every single one of them said we're not doing what we should be doing to protect ourselves against cyber security" threats, former 9/11 commission co-chair Tom Kean told a House homeland security panel.

Two-thirds of energy and manufacturing firms hit by cyber attacks

From www.powermag.com, 7/10/2014

A report released July 10 found alarming gaps in the security of the world's critical infrastructure. Key findings from the report include:

- 67% of respondents say their companies have had at least one security compromise that led to the loss of confidential information or disruption to operations over the past 12 months.
- 57% of respondents say that cyber threats are putting industrial control systems and supervisory control and data acquisition systems at greater risk.
- 54% of respondents say upgrading legacy systems to the next improved security state may result in sacrificing mission-critical security.
- 34% of respondents say their companies do not get real-time alerts, threat analysis, and threat prioritization intelligence that can be used to stop or minimize the impact of a cyber attack.
- 83% of respondents say their companies have not fully deployed their information technology security programs.

Schneider Electric

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
July 2014 / Issue 34

Cyber News

Hacking experts build device to protect cars from cyber attacks

From www.chicagotribune.com, 7/23/2014

Two security experts who a year ago exposed methods for hacking the Toyota Prius and Ford Escape say they have developed technology that would keep automobiles safe from cyber attacks. At last summer's Def Con hacking conference in Las Vegas, the two researchers, Chris Valasek and Charlie Miller, described ways to launch dangerous attacks, including manipulating the brakes of the moving Prius and the Ford Escape. Valasek, director of vehicle security research at the consulting firm IOActive, told Reuters that he and Miller will show off a prototype vehicle "intrusion prevention device" at next month's Black Hat hacking conference in Las Vegas. They built the device with about $150 in electronics parts, though the real "secret sauce" is a set of computer algorithms that listen to traffic in a car's network to understand how things are supposed to work. When an attack occurs, the device identifies traffic anomalies and blocks rogue activity, Valasek said.

India 2nd most vulnerable country to cyber attacks

From www.newindianexpress.com, 7/19/2014

While China has 25 million cyber warriors who are extensively engaged in various activities, India lags far behind with only 22,075 cyber security professionals, minister for IT and panchayat raj KT Rama Rao said. Speaking at the inauguration of a cyber security conference titled 'Counter Measures to Face the Threats,' Rao said Kaspersky Labs had placed India as the second most vulnerable country to cyber attacks.

Europe cyber security market is expected to reach $19 billion in 2019

From www.streetinsider.com, 7/25/2014

The Europe Cyber Security report defines and segments the cyber security solutions market in Europe with analysis and forecast of revenue. This market is estimated to grow from around $13.53 billion in 2014 to $19.07 billion by 2019, at a CAGR of 7.10% from 2014 to 2019.

House passes bills to strengthen U.S. cyber security efforts

From www.businessinsurance.com, 7/30/2014

The House of Representatives has approved three bipartisan bills intended to strengthen efforts to combat cyber attacks on the critical infrastructure. The bills are:

- H.R. 3696, the National Cybersecurity and Critical Infrastructure Protection Act, which requires the Secretary of Homeland Security to conduct cyber security activities including "shared situational awareness" among federal entities to prevent, mitigate, respond to and recover from cyber incidents.
- H.R. 2952, the Critical Infrastructure Research and Development Advancement Act, which amends the Homeland Security Act of 2002 to improve laws relating to the advancement of security technologies for critical infrastructure protection.
- H.R. 3107, the Homeland Security Cybersecurity Boots-on-the Ground Act, which assesses the readiness and capacity of the Department of Homeland Security to meet its "cyber security mission."

Suspected Chinese cyber attack forces NRC security overhaul

From ottawacitizen.com, 7/29/2014

The National Research Council has launched a massive, year-long security overhaul of its computer systems after a series of cyber attacks believed to have come from China. The Communications Security Establishment Canada "detected and confirmed a cyber intrusion on the IT infrastructure of the National Research Council of Canada," the science and tech research organization said in a statement. "Following assessments by NRC and its security partners, action has been taken to contain and address this security breach, including protecting its information holdings and notifying the privacy commissioner. NRC has also taken steps to inform its clients and stakeholders about this situation." It says it will undertake a major overhaul of its computer security: "This could take approximately one year."

Schneider Electric

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
July 2014 / Issue 34

Security Program Assessment

Information security is the process by which an organization protects and secures systems, media, and facilities that process and maintain information vital to operations. On a broad scale, the control system industry has a primary role in protecting the nation's critical infrastructure. The security of control systems and information is essential to maintain control system safety, soundness, and reliability. Control system owners' information assurance programs must have strong Senior Management level support. In addition, a clear integration of security activities and controls must compliment control system processes. Organizations often inaccurately perceive information security as the state or condition of controls at a point in time. Security is an ongoing process, whereby the condition of a Manufacturing Institution's controls is just one indicator of their overall security posture. Other indicators include their ability to continually assess the security posture and react appropriately in the face of rapidly changing threats, technologies, and business conditions. A Manufacturing Institution establishes and maintains a truly effective information assurance program when they continuously integrate processes, people, and technology to mitigate risk in accordance with risk assessment and acceptable risk tolerance levels. They protect information by instituting security processes that identify risks, form a strategy to manage the risks, implement the strategy, test the implementation, and monitor the environment to control the risks. Manufacturing Institution's information assurance program could be evaluated using a simple tool known as Quality Management Maturity Grid which was outlined in Philip Crosby's book "Quality is Free." The evaluation examines stages of maturity using five stages of security maturity: uncertainty, awakening, enlightenment, wisdom, and benevolence. When combined, they reveal an enterprise's overall information security program maturity.

Uncertainty

The lowest stage of information security program maturity, uncertainty, is characterized by a total lack of understanding of information security. Although system integrity and availability requirements may be understood, failures to live up to these reliability requirements are viewed as system engineering failures rather than security incidents.

Awakening

The second stage of information security program maturity, awakening, is characterized by both the realization that information security engineering may be of value and the inability to provide money or time to support information security activities. Security is viewed as a commodity that can be bought on the open market. Management allocates funds to procure systems or products with high-reliability components rather than determine their actual reliability needs. As a result, management often overspends by buying equipment that far exceeds its requirements.

Enlightenment

The third stage of information security program maturity, enlightenment, is characterized by both the realization that a companywide industrial control system security infrastructure is necessary and that resources must be allocated to support industrial control system activities.

Wisdom

The fourth stage of information security program maturity, wisdom, is characterized by an information security program that more closely reflects the enterprise's environment and responds to the Manufacturing Institution's evolving industrial control system needs.

Benevolence

The fifth stage of information security program maturity, benevolence, is characterized by continual information security process improvement through research and participation and the sharing of knowledge in public and professional forums.

Manufacturing Institution network infrastructure and need for information security has grown from an islanded industrial control workgroup located in a single location into a multi-site wide area network (WAN) requiring servers, routers, firewalls, and other technologies. To offset the risk of today's industrial control systems, Manufacturing Institutions must identify which phase of the security model they are currently at and allocate the appropriate resourcing, funding, and commitment to move their industrial control system's cyber security program to maturity.

This month's contributors to Consultant's Corner are Tim Johnson and Michael Martinez
Consultants, Critical Infrastructure & Security Practice, Invensys
tim.johnson.us@schneider-electric.com
michael.martinez@schneider-electric.com

Schneider Electric

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
July 2014 / Issue 34

Most Popular Blog Posts This Month

Chinese hackers target think tanks instead of U.S. tech firms – to protect oil interests (July 10, 2014)
China's Deep Panda hacking crew, considered one of the world's best for its skilled insertion of malware into adversaries' data streams, has apparently changed its snooping habits. Deep Panda has switched its focus, at least temporarily, from American technology giants and financial targets to major U.S. think tanks who employ former ranking government officials.

Internet of Things Has Security Vulnerabilities (July 2, 2014)
Back in the old days, people worried about their computers getting hacked. Today, they worry about their refrigerators being hacked.

Bank-stealing virus returns after crackdown (July 16, 2014)
Malicious software used to steal millions from bank accounts has re-emerged a month after US authorities broke up a major hacker network using the scheme, security researchers say.

Is Your Car Vulnerable to Hackers? (July 21, 2014)
By 2017, more than 60% of cars will be connected to the Internet, literally creating a moving target for cyber criminals.

Are Digital Retailers Focusing Their Security in the Wrong Place? (July 7, 2014)
High-profile data breaches have plagued retail this year — Target, Neiman Marcus, Michael's and other U.S. retailers have seen headlines about their woes splashed across both digital and print media. In Target's case, the breach of 40 million credit cards and 70 million personally identifiable information (PII) database records led the CIO and then the CEO to resign. Could retailers be focusing their security efforts in the wrong areas?

Featured Post: Phishing Alert – 8 Tips to Protect Yourself from Attacks

It's as easy for hackers to phish out your personal data as it is to sit in a canoe on a still pond, cast the bait and wait for the fish to bite. Click here to read about tips to protect yourself from attacks. Click here to read about tips to protect yourself from attacks.

Visit us on Blogger!

Schneider Electric

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
July 2014 / Issue 34

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**