February 2013 / Issue 17

The Global Cyber Advisor

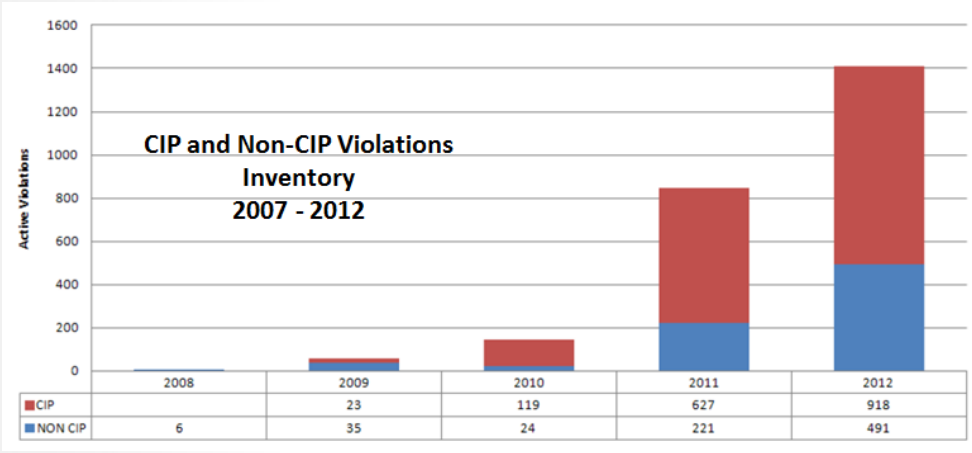
Invensys Critical Infrastructure & Security Practice

this issue

NERC 2012 by the Numbers

With the acceptance of NERC-CIP Version 4 this past year, NERC was as busy as ever tracking violations. In 2012, NERC issued over $5.9MM in violations that averaged over $115K a month. This is a previous trend from 2011 that will continue throughout 2013.

One trend for 2012 not evident in previous years that will surely continue for the foreseeable future was NERC's "Top Enforceable Standards." This year, four of the top five were all CIP standard with only one FERC. Looking at the "CIP and Non-CIP Violations Inventory" graph below, the growth of CIP violations in 2012 definitely accounts for this.



During previous years, the violations were focused on CIP-008 (incident reporting), CIP-003 (security management controls) and CIP-004 (personnel & training). Now the emphasis of NERC is changing, focusing less on the planning activities and more on actual implementation of cyber security solutions. The table below shows the breakdown for 2012.

CIP Std	Total	%
CIP-002 Cyber Asset Identication	21	7.7%
CIP-003 Security Mgt Controls	20	7.3%
CIP-004 Personnel & Training	43	15.8%
CIP-005 Electronic Security Perimeters	46	16.8%
CIP-006 Physical Security	28	10.3%
CIP-007 System Security Mgt	95	34.8%
CIP-008 Incident Reporting and Response	4	1.5%
CIP-009 Recovery Planning	16	5.9%

This is the year of transition for many in the NERC-regulated power industries. There are companies who have seen the refocus of NERC and have begun their cyber security solution rollouts and there are others who are taking a "wait and see" approach. Whether it is addressing cyber security or NERC, a best defense is always a good offense.

Feb. 2013
Cyber Attack Statistics
- **Hackmageddon.com**

Attack Motivations
- 56% Hacktivism
- 26% Cyber Crime
- 9% Cyber Espionage

Top 3 Attack Targets
- 29% Government
- 19% Industry
- 13% Organizations

Top 5 Attack Techniques
- 31% SQL
- 16% DDoS
- 15% Targeted
- 14% Unkown
- 4% Defacement

Industry News

China hackers increasingly focused on U.S. infrastructure

www.securityweek.com, 2/19/2013

A report says China hackers are increasingly focused on companies involved in U.S. critical infrastructure, including electrical power grid, gas lines, and water systems. China's army controls hundreds, if not thousands, of virulent and cutting edge hackers, according to a report by a U.S. Internet security firm that traced a host of cyber attacks to an anonymous building in Shanghai. Mandiant said its hundreds of investigations showed that groups hacking into U.S. newspapers, government agencies, and companies "are based primarily in China and that the Chinese government is aware of them." The 74-page report focused on one group, which it called "APT1" from the initials "Advanced Persistent Threat." The New York Times, citing experts, said the group was targeting crucial infrastructure such as the U.S. energy grid. "We believe that APT1 is able to wage such a long-running and extensive cyber espionage campaign in large part because it receives direct government support," Mandiant said.

Power-grid cyber attack seen leaving millions in dark for months

www.bloomberg.com, 2/1/2013

A blackout that swept parts of North America in August 2003, leaving 50 million people in the dark for as long as four days, provides a glimpse of the havoc a cyber attack could inflict on the nation's power grid. Internet-based terrorists would be capable of causing blackouts "on the order of nine to 18 months" by disabling critical systems such as transformers, said Joe Weiss, managing director of Applied Control Solutions LLC, a Cupertino, California-based security consulting company. Energy companies including utilities would have to increase their investment in computer security more than seven fold to reach an ideal level of protection, according to a survey done for Bloomberg Government by the Ponemon Institute LLC,

SCADA, ICS bug brokering mirrors IT vulnerability market

threatpost.com, 2/5/2013

The world of SCADA and industrial control system vulnerabilities is starting to mirror that of IT security, not only in the demonstration and exploitation of zero-day vulnerabilities, but also in the brokering of flaws and exploits between hackers and organizations interested in buying research. At the Kaspersky Security Analyst Summit, two researchers known for finding more than 1,000 vulnerabilities in Internet-facing industrial control systems, demonstrated a zero-day in vendor Tridium's Niagara Framework, which is used to run building maintenance systems including elevators, HVAC, video surveillance systems, and more.

U.S. cyber security debate risks leaving critical infrastructure in the dark

www.forbes.com, 2/26/2013

The generally poor quality of the public policy debate about cyber security in the United States has included a tendency to resist efforts to define key terms clearly, to hype threats, and to conflate a number of different threats and vulnerabilities under the term "cyber war." We saw one potential negative consequence to these tendencies. Just as a number of pieces of legislation addressing the cyber security of critical infrastructure like power and water systems are being introduced into the Congress, the New York Times reports that some lawmakers might be getting cold feet.

Nuclear lab remains vulnerable to cyber strikes, Energy IG says

www.nextgov.com, 2/16/2013

A leading U.S. nuclear arms site has taken significant steps in recent years to defend against strikes on its computer systems, but key weaknesses remain to be fixed, the Energy Department's inspector general said this week. The Los Alamos National Laboratory in New Mexico uses a host of information systems and networks to carry out its duties, which include research and production programs in support of maintaining the nation's nuclear arsenal, Inspector General Gregory Friedman said in a memorandum attached to a cyber security report.

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
February 2013 / Issue 17

Cyber News

Apple admits "widespread cyber security breach" by Chinese hackers

news.yahoo.com, 2/10/2013

In a move that Reuters calls "an unprecedented admission of a widespread cyber security breach," Apple (AAPL) on Tuesday admitted that it was the victim of several attacks by the same group of Chinese hackers who previously targeted Facebook (FB) and other large companies. The hackers were able to infect a "small number" of Mac computers that belonged to Apple employees, although it said that "there was no evidence that any data left Apple."

Chinese hackers compromise NY Times, WSJ to steal sources

www.eweek.com, 2/1/2013

The Journal released few details of its own network compromise on Jan. 31, stating that the FBI has been investigating Chinese attacks on media companies for more than a year. "Evidence shows that infiltration efforts target the monitoring of The Journal's coverage of China and are not an attempt to gain commercial advantage or to misappropriate customer information," said Paula Keve, a spokeswoman for The Journal's parent company, Dow Jones & Co.

U.S. Department of Energy: Which bright spark just hacked us?

www.theregister.com, 2/5/2013

Personal information on several hundred employees at the U.S. Department of Energy has been compromised as the result of a hack attack, according to media reports. The FBI is reportedly investigating the attack, which was detected around late January. According to officials quoted in the Washington Free Beacon, the damage appears to have been limited to 14 servers and 20 desktop workstations at the DoE's HQ. Although the breach might have ultimately been aimed at gaining access to classified systems, early indications are that no classified info was compromised, according to an official letter from the agency to its employees.

Federal Reserve confirms its Web site was hacked

www.cnet.com, 2/5/2013

The wave of high-level cyber attacks continues as the Federal Reserve confirmed that one of its internal Web sites was hacked, according to Reuters. "The Federal Reserve system is aware that information was obtained by exploiting a temporary vulnerability in a website vendor product," a Fed spokeswoman told Reuters. "Exposure was fixed shortly after discovery and is no longer an issue. This incident did not affect critical operations of the Federal Reserve system."

Microsoft joins list of companies recently hacked

news.yahoo.com, 2/22/2013

Microsoft has joined the list of prominent technology companies confirming they have been hit by a recent computer hacking attack. In a blog posting Friday, Microsoft said it had found no evidence that any customer data had been heisted. Microsoft Corp. gave few other details about the break-in, except to say that was it similar to a hacking attack that online social networking leader Facebook Inc. disclosed last week. Facebook had said its investigation had discovered other companies had been hacked, but didn't identify the other victims.

Hackers target Twitter, could affect 250,000 user accounts

news.yahoo.com, 2/1/2013

Anonymous hackers attacked Twitter this week and may have gained access to passwords and other information for as many as 250,000 user accounts, the microblog revealed late on Friday. Twitter said in a blog post that the passwords were encrypted and that it had already reset them as a "precautionary measure," and that it was in the process of notifying affected users. The blog post noted recent revelations of large-scale cyber attacks against the New York Times and the Wall Street Journal, but unlike the two news organizations, Twitter did not provide any detail on the origin or methodology of the attacks.

Consultant's Corner

USB Sticks and the Spread of Malware

Malware has continually been on the rise over the past several years. Kindsight Security Labs' 2012 malware reports discovered the following:

- The infection rate of home networks teetered between 11% and 14% in 2012
- Mac Flashback malware topped the list of Top 20 Home Network Infections for four weeks straight, "infecting 10% of home networks with Mac computers" during the month of April alone
- The ZeroAccess bot distributed malware responsible for ad-click fraud that subsequently eats up bandwith, infecting over 2 million users, with 685,000 in the United States alone
- The amount of Android malware samples increased 300% in 2Q/2012 and continues to rise

Kaspersky Lab identified the top 20 countries where web resources are seeded with malware, with the United States ranking #1, with 413,622,459 attacks. Malware has become a serious problem and will continue to increase, so although you may keep your networks updated with the most current patches, firewalls, and anti-virus software, have you considered the risks of using USB drives?

USB drives can be easily lost, stolen, or fail without warning, causing users to lose invaluable amounts of data. Anti-virus firm Sophos discovered that 66% of USB drives lost by railroad commuters were infected with malware; similarly, one cyber criminal purposely planted "lost" USB drives in a company parking lot, hoping employees might plug them into company computers and allow him to steal confidential information. Even the U.S. Army has fallen victim to the hazards of removable media, and unauthorized use has led to over 70 percent of their cyber security breaches. An entire power plant was taken offline for three weeks after a third-party contractor plugged a USB stick into one of the company's critical systems (SC Magazine, January 18, 2013).

USB drives are a double-edged sword; even though they are convenient in industry for quickly transferring software and data between workstations, how do you secure and control that data? How do you really know for sure USB sticks are secure?

The security control of USB drives in the industrial environment has as much to do with the application they are being utilized in as where they are utilized. In some cases, USB drives are no longer required since a centralized patch management solution was installed as part of the overall cyber security solution.

In other cases where USB drives are required, policies can be created and managed using host intrusion detection (HIDS) and data loss prevention (DLP) software solutions.

This month's contributor to Consultant's Corner is
Carrie Straka
Consultant, Critical Infrastructure & Security Practice, Invensys
carrie.straka@invensys.com

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
February 2013 / Issue 17

Invensys 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, Implement and Management.

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.

invensys™

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

5601 Granite Pkwy. Suite 1000 Plano, TX 75024 ▪ P 214.295.6365 ▪ F 888.758.7675 ▪ **iom.invensys.com**