The Global Cyber Advisor

Invensys Critical Infrastructure & Security Practice

February 2014
Issue 29

this issue

AWWA guidance helps water utilities guard against cyber attacks

From www.awwa.org, 2/12/2014

With cyber attacks a growing threat to critical infrastructure systems, the American Water Works Association announced the release of expert guidance on how water utilities can reduce their cyber vulnerabilities. This guidance was prepared to provide water utility managers with a concise set of best practices and standards. It puts forth a transparent and repeatable process for evaluating a utility's process control system. In order to provide the widest benefit, the guidance and tool are free and publicly available.

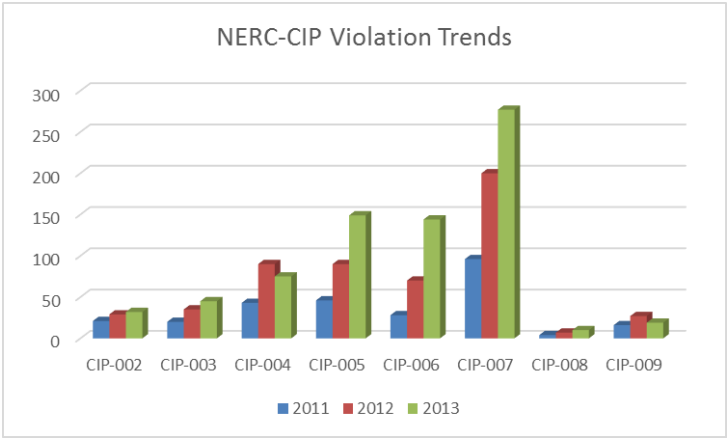
NERC CIP 2014 by the Numbers

It has been one year since we last looked at NERC CIP by the numbers. Since that time, FERC approved Version 5 of the NERC CIP standards. The Version 5 CIP standards differ from Version 4 in that they require that all cyber assets be categorized as Low, Medium, and High impact assets. All cyber assets in the Bulk Electrical System (BES) will now have some level of protection based on the impact level. Additionally, there are 12 new requirements with new cyber security controls. Details can be found on www.nerc.com.

Even with the introduction of CIP Version 5, NERC has been busy tracking violations. From 2011 through 2013, there were $19.3MM in violations. The strongest trend continues to be the dominance of CIP in the mix of standards violations.

	2011	2012	2013
Tot Stds	1372	1101	1065
CIP Stds	274	548	751
% CIP	20%	50%	71%

In 2011, there were 1,372 standards violations, of which 20 percent were CIP. Fast forward to 2013 and on, CIP represents 71 percent of all NERC fines. With the introduction of Version 5 CIP and the new requirements, this trend will only continue into 2014.



The top three CIP standards have not changed much since 2011; however, the focus on CIP is much greater. The top three for 2013 were CIP-007 System Security Management, CIP-005 Electronic Security Perimeter (ESP), and CIP-006 Physical Security.

Just as last year, this year continues to be a transition for many in the NERC regulated power industries. Companies are seeing the increased focus of NERC and have begun their cyber security solution rollouts. However, others are taking a "wait-and-see" approach. Whether it is addressing cyber security best practices or NERC CIP, a best defense is always a good offense.

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
February 2014 / Issue 29

Industry News

Congress moves critical infrastructure cyber security bill

From www.mondaq.com, 2/7/2014

Earlier this month, the House Homeland Security Committee passed a substitute bill for H.R. 3696, the National Cybersecurity and Critical Infrastructure Protection Act of 2013. H.R. 3696 delegates to the Department of Homeland Security the responsibility for civilian cyber security research and development, incident detection and response, and facilitating the exchange of cyber threat information between government and the private sector.

Summit offers chance to cooperate on nuclear cyber security

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

Nations should form an international agreement that forbids cyber attacks against civil nuclear facilities during peacetime, the EastWest Institute says in a new report. "The growth of cyber arsenals and the democratization of access to the technologies of cyber attacks mean that time is increasingly short" to protect nuclear facilities, the report says. "Rather than wait for comprehensive solutions, the EastWest Institute has focused in this report on a specific next step, adoption of a measure of restraint."

Hacks on gas and the grid

From www.forbes.com, 2/12/2014

Natural disasters demonstrate that outages can occur regularly in the United States, particularly in the wake of weather-related events, but there are valid concerns about how computer control of energy generation and distribution might bear the brunt of a significant cyber attack. When the balance between production and consumption tips, the entire power grid is at risk of collapse, as it did in July 2012 in India impacting some 320 million people. The combination of a software vulnerability combined with the capacity for cascading failures is why there should be concern on the cyber security of the power grid.

Attacking ICS systems 'like hacking in the 1980s'

From threatpost.com, 2/11/2014

Here's how nuts the state of building automation security is: Terry McCorkle, an ICS and automation security researcher, was doing an assessment of a building's security and was able to access its automation system over the Internet. He accessed the HVAC system and from there was able to pivot to the lighting and surveillance system. He then found the access control and energy management system and was eventually able to unlock the doors, turn off the IP cameras, open the parking garage door and modify the access-control database. "It's like hacking in the 1980s and 1990s," said Jonathan Pollet, founder of Red Tiger Security. Pollet said that in the PLC and ICS world, what might drive better security is demands from users.

ACC supports introduction of house legislation to extend chemical security regulations

From www.americanchemistry.com, 2/6/2014

House Committee on Homeland Security Chairman Michael McCaul (R-TX), Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies Chairman Patrick Meehan (R-PA), and Representative Gene Green (D-TX) introduced a bipartisan bill this month that will provide for a two-year extension of the Chemical Facility Anti-Terrorism Standards (CFATS) program through authorizing legislation rather than using the appropriations process. "The bill introduced in the House will help ensure the ongoing effort to secure chemical facilities will continue to advance and will provide the regulatory certainty that is vital to the overall success of CFATS."

Risk for CFATS

From www.dhs.gov, 2/12/2014

In Section 550, Congress directed the Department of Homeland Security to identify and secure those chemical facilities that present the greatest security risk. Security risk is a function of the consequence of a successful attack on a facility (consequence), the likelihood that an attack on a facility will be successful (vulnerability), and the intent and capability of an adversary in respect to attacking a facility (threat). Since each chemical facility faces different security challenges, Congress explicitly directed the Department to issue regulations "establishing risk-based performance standards for security chemical facilities." Performance standards are particularly appropriate in a security context because they provide individual facilities the flexibility to address their unique security challenges and helps to increase the overall security of the sector by varying the security practices used by different chemical facilities. Security measures that differ from facility to facility mean that each presents a new and unique problem for an adversary to solve.

Schneider Electric

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
February 2014 / Issue 29

Cyber News

DDoS attacks against datacenters on the rise

From www.networkcomputing.com, 2/6/2014

Despite widespread efforts to curtail them, distributed denial-of-service attacks continue to stake their place among the greatest threats enterprises face today. The likely reason? DDoS attackers -- who increasingly have extortion as their objective -- continue to evolve their strategies, seemingly staying one step ahead of information security teams. According to Arbor Networks' ninth annual Worldwide Infrastructure Security Report, companies surveyed by the security company ranked DDoS attacks against infrastructure as their top concern for 2014.

Target attack shows danger of remotely accessible HVAC systems

From www.computerworld.com, 2/7/2014

The massive Target breach led to revelations that many companies use Internet-connected heating, ventilation, and air conditioning (HVAC) systems without adequate security, giving hackers a potential gateway to key corporate systems, a security firm warned Thursday. Cloud security service provider Qualys said that its researchers have discovered that most of about 55,000 HVAC systems connected to the Internet over the past two years have flaws that can be easily exploited by hackers. HVAC systems connect to networks at various retail companies, government buildings and even hospitals, according to the security firm. Hackers can exploit these systems to gain access to enterprise networks and leapfrog onto other corporate systems, Qualys said.

Cyber attacks fallout could cost the global economy $3 trillion by 2020

From www.techrepublic.com, 2/20/2014

The global economy has yet to mount an adequate defense against the rise of cyber attacks, according to new research. The impact could be $3 trillion in lost productivity and growth.

Cyber security market to hit $77B

From www.federaltimes.com, 2/21/2014

The global cyber security market will be worth $77.7 billion in 2014, according to a new forecast by market research firm ASDReports. The study examined the government, military, critical infrastructure, and private sectors. "Cyber security remains a significant challenge for developed markets, with the capacity to cause significant and embarrassing disruption to a range of modern infrastructures and networked systems," said the study.

360 million account credentials found in the wild

From www.computerworld.com, 2/26/2014

A cyber security company said it has obtained a list of 360 million account credentials for Web services, likely collected through multiple data breaches. Analysts with Hold Security came across the credentials during their work over the last three weeks while studying underground forums where stolen data is for sale, said Alex Holden, CIO with the Wisconsin-based company. "This month has been very fruitful for hackers," he said in a phone interview. One batch of 105 million details included email addresses and corresponding passwords.

Nearly half of companies assume they have been compromised

From www.net-security.org, 2/25/2014

In the first-ever SANS Endpoint Security Survey, SANS surveyed 948 IT Security professionals in the United States to determine how they monitor, assess, protect and investigate their endpoints, including servers. The survey results demonstrated that more and more attacks are bypassing perimeter security, despite the fact that the respondents do not consider the attacks to be sophisticated.

SEC plans roundtable on cyber security

From www.thenews.com, 2/16/2014

The Securities and Exchange Commission said that it plans to hold a roundtable next month to discuss cyber security, after massive retailer breaches refocused the attention of the business community and policymakers on the area. The SEC said that it would hold the event on March 26 to talk about the challenges cyber threats pose for market participants and public companies. Recent breaches at Target Corp and Neiman Marcus have sparked concern from lawmakers and revived a long-running spat among retailers and banks over who should bear the cost of consumer losses and technology investments to improve security.

Schneider Electric

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
February 2014 / Issue 29

Choking on Data

Ever hear the phrase "Choking on data, starving for information?" I credit my exposure to this phrase during a meeting I had with my new Vice President as a fresh-out-of-college employee. He discussed and displayed a massive amount of spreadsheet business data and pointed out how over time management becomes unenthusiastic to data with large quantities of generic numbers. He then switched over to a single bar chart that showed a summarization of the futile numbers with attractive colors and easy-to-view upper and lower limits. His next statement—"Now this is information!"—created a preservation I embrace daily about how data becomes valuable to an organization as information.

Meaningful information is a challenge for any department, organization, or compliance program. When management commits to spend large sums of capital and investments into a security or compliance program, they enjoy seeing ROI in attractive meaningful information. This is where a SIEM (Security Information and Event Management) solution can help correlate an organization's appetite for information and the harsh quantities of collected signal data. "We have no need for a SIEM," you say? Well, let's take a quick look at some data.

A typical Windows 8 user login will generate six (6) Windows Security events in less than a second, not including access to network resources such as mapped printers and network drives. Now, take this number and multiple it by each station on your network (let's say 100 workstations) during a peak working hour (8am to 9am). That is over 2,160,000 events in 1 hour (6 events x 60 seconds x 60 minutes)! Now you can start to imagine how quickly your organization can be choking on data. Try factoring in security appliances (firewalls, VPNs, proxies, IDS/IPSs) and your ability to analyze data goes from excruciating to borderline impossible. Furthermore, what happens in the event of an unauthorized or unsanctioned security event? Did you get an alert? How do you correlate/relate events from multiple devices scattered across your network? How does your organization take this massive amount of data and make it meaningful information? Do you have a single dashboard to view categorize this data? Enter the SIEM. A SIEM can be an appliance (server), customized software, or vendor service that combines the collection of information and designated events or alerts from multiple data sources. It silently listens to data collection sources, such as services, Workstations, Servers, Firewalls, IPS/IDS, etc. for event data. This event data can consist of almost any instance generated by applications, security, and hardware. With a SIEM, data is analyzed and correlated in real time, which can be displayed via a dashboard, acted upon via scripts or alerts, and stored for compliance or historical information.

Visibility/Reaction

Using the 2,160,000 event example above, let's say you wanted to know how many failed logins occurred this morning from all of your 100 stations. You also want to know if any of these events occurred from your outside VPN IP address range. A SIEM would take these events and correlate them with all of your data sources (firewalls, IPS/IDS, Active Directory), and generate a dashboard to show you all failed logins during the specific time frame and relate them to all VPN logins. You can then further filter the data down to the single event or even the entire communication channel, such as outside IP addresses, VPN addresses, permitted/denied firewall sessions, SSO, or authenticating workstation. With a SIEM, you can even perform additional actions such as banning the IP address/range, adding an email/text alert, sandboxing, or executing customized scripts.

Compliance

From a compliance perspective, you can create customized dashboards, reports, or correlations to categorize and display all relevant data in conjunction with your compliance program. A SIEM can serve as compliance evidence and a change management information historian. Some SIEMs, such as McAfee's ESM Nitro, contain prebuilt compliance views for NERC/CIP, PCI, SOX, HIPAA, 27002, FISMA, and others. These dashboards/views will drastically reduce information gathering and decrease required man power during those stressful audit times.

Vulnerability Views

Vulnerability assessment data can also be imported into a SIEM. Popular vulnerability scanning software (think Rapid7's Metasploit Pro, NeXpose, or Nessus) can be directly imported into a SIEM. With vulnerability scan data, you can easily create automated scans, imports, and dashboards for those critical Electronic Security Perimeter devices and remote access servers. When used with a defense-in-depth program, these intermediary devices become critical gateways to a facility's operations or an organization's intellectual property.

In short, a SIEM can drastically reduce man hours, monitoring costs, forensic data gathering, and compliance fines by providing a synergy for a mass majority of your infrastructure. This remarkable transformation of incomprehensible data into meaningful information will not only keep you from choking, but it will also fill your appetite for information.

This month's contributor to Consultant's Corner is Roy Solis
Consultant, Critical Infrastructure & Security Practice, Invensys
roy.solis@invensys.com

Schneider Electric

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
February 2014 / Issue 29

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