November 2013 / Issue 26

The Global Cyber Advisor

Invensys Critical Infrastructure & Security Practice

this issue

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

Attack Motivations
- 33% Hacktivism
- 63% Cyber Crime
- 4% Cyber Espionage

Top 3 Attack Targets
- 24% Government
- 16% Industry
- 9% Organization

Top 5 Attack Techniques
- 27% Defacement
- 22% Unknown
- 10% Account Hijacking
- 9% DDoS
- 8% SQL

New Stuxnet Revelations

Even though over three years have passed since the Stuxnet virus ravaged Iran's Natanz nuclear facility, new revelations are emerging about the worm, the latest being about the origins of the original Stuxnet variant, a more sophisticated and potentially more powerful worm that infected Iran's nuclear facilities as early as 2007, according to a report from Foreign Policy. This Stuxnet "twin" targeted the centrifuges at the Natanz uranium-enrichment plant and "blocked the outflow of gas from the cascades of centrifuges, causing pressure to build up and the equipment to become damaged. It even masked the attack by looping 21 seconds of the system's sensor values so that the engineers at the facility wouldn't realize anything was wrong." So while the second Stuxnet is considered the first cyber act of force, the new details reveal that the impact of the first virus will be much greater. That's because the initial attack "provided a useful blueprint to future attackers by highlighting the royal road to infiltration of hard targets:" humans working as contractors (*Business Insider*).

The human factor in data breaches due to lack of security awareness or training still remains a top threat among the industry today, with BYOD perpetuating vulnerabilities and cyber risk. As we saw with the eerily similar viruses that followed Stuxnet, USB keys are small but mighty devices that could bring down economically-dependent critical infrastructure, as we saw as Saudi Aramco, where 30,000 workstations were sent offline in August 2012 after a third-party contractor inserted a Shamoon-infected thumb drive into one of the computers. More recently, there was speculation that Russian cosmonauts infected the international space station with USB keys containing malware.

Implementing firewalls and anti-virus software alone does not make you cyber compliant or cyber secure. Computers don't have to be connected to the internet to become infected with malware. Firewalls and anti-virus software are small parts of a larger picture, such as adequate policies and procedures, proper system maintenance, patching at regular intervals, and following industry best practices, including:

- ☑ Establishing end user acceptable use guidelines
- ☑ Managing strict vendor guidelines
- ☑ Managing physical security
- ☑ Purging unnecessary data
- ☑ Enforcing a patch management program
- ☑ Enforcing password requirements and guidelines
- ☑ Maintaining wireless networking policies and procedures
- ☑ Creating an incident response program *before* incidents occur

Compliance is not the same as cyber security; however, a strong cyber security project must begin with a compliance plan to help develop the proper methodology, which can help you conform to regulatory or non-regulatory requirements, industry standards, or company standards. The path to cyber security is through best practices. Compliance can help give you a platform to build a more thorough and customized cyber security strategy to prevent catastrophic cyber attacks.

Industry News

60 percent of Industrial Control industry has not deployed security configuration management

From www.itbusinessnet.com, 11/13/13

Tripwire, Inc. announced the results of research comparing risk-based security management in the industrial sector to that of other industries. The study revealed that the industrial sector is less effective than other industries in deploying risk management controls and communicating effectively about security. Additional findings included:

- Only 40 percent have fully or partially deployed security configuration management
- 75 percent have fully or partially deployed system hardening
- 69 percent said security communications are contained in only one department or line of business
- 67 percent said security communications occur at too low a level
- Only 56 percent listed an openness to challenge assumptions as one of the top three features most critical to the success of a risk-based security management approach

Cyber attack at a major port could cost $1 billion per day

From www.gsnmagazine.com, 11/24/13

At a time when the nation's infrastructure faces a growing threat from cyber attacks, maritime and homeland security officials say they are making significant progress in protecting the nation's ports, which handle more than 2 billion metric tons of cargo annually and are critical to the global economy. Doug Albrecht, director of information management at the Port of Long Beach, said the port blocks about 9 million attacks monthly on its network. But it only takes one successful intrusion to potentially do damage, he said. To combat this threat, port officials teach workers how to recognize methods hackers use to break into the highly-secure networks of ports and other critical infrastructure in the nation. A lot is at stake. A cyber attack that successfully shuts down the ports of Los Angeles and Long Beach would cause $1 billion a day in losses to the national economy.

Chinese military is targeting critical U.S. infrastructure for cyber attacks

From www.oodaloop.com, 11/10/2013

"The Chinese government is directing and executing a large-scale cyber espionage campaign against the United States, and to date has successfully targeted the networks of US government and private organizations, including those of DoD, defense contractors, and private firms," a report from the U.S.-China Economic and Security Review Commission said. "These activities are designed to achieve a number of broad economic and strategic objectives, such as gathering intelligence, providing Chinese firms with an advantage over its competitors worldwide, advancing long-term research and development objectives, and gaining information that could enable future military operations."

Stuxnet also infected the internal network of a Russian nuclear plant

From thehackernews.com, 11/10/2013

Eugene Kaspersky, CEO of Kaspersky security firm, revealed that Stuxnet had badly infected the internal network of a Russian nuclear plant, according to the information he obtained from an unnamed staffer at the Nuclear Plant. During a presentation given at the Canberra Press Club, Kaspersky provided an overview on the security of cyberspace, in particular highlighting the effect of the activities of state-sponsored espionage and cyber crime. The malware Stuxnet is widely considered to have been developed by the US Government in a joint work with Israel cyber units as a means to disrupt Iran's nuclear enrichment plans. After its disclosure, it's raised the debate on the use of software and malicious application in information warfare, and every government is investing to improve its cyber capabilities working on both Defense and Offense sides. In this case, Stuxnet had infected the internal network of a Russian nuclear plant, exactly in the same way it compromised the control system in Iranian nuclear facilities in Natanz.

Persian Gulf oil industry 'vulnerable to cyber attacks'

From www.upi.com, 11/20/2013

Middle East oil and gas companies need to beef up their defenses against cyber attacks, security specialists say, with the Persian Gulf particularly vulnerable because of the high concentration of energy resources in the turbulent region. One of the industry's main vulnerabilities against what British cyber security experts called "an invisible enemy" is its reliance on outdated computer technology that can be easily penetrated. Cyber attacks on the industry's infrastructure are projected to cost damages totaling nearly $2 billion by 2018.

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
November 2013 / Issue 26

Cyber News

Repeated attacks hijack huge chunks of Internet traffic

From arstechnica.com, 11/20/2013

Huge chunks of Internet traffic belonging to financial institutions, government agencies, and network service providers have repeatedly been diverted to distant locations under unexplained circumstances that are stoking suspicions the traffic may be surreptitiously monitored or modified before being passed along to its final destination. Researchers from network intelligence firm Renesys made that sobering assessment in a blog post published earlier this month. Since February, they have observed 38 distinct events in which large blocks of traffic have been improperly redirected to routers at Belarusian or Icelandic service providers. The hacks, which exploit implicit trust placed in the border gateway protocol used to exchange data between large service providers, affected "major financial institutions, governments, and network service providers" in the US, South Korea, Germany, the Czech Republic, Lithuania, Libya, and Iran.

Vast majority of employees use unauthorized file sharing services

From www.securityweek.com, 11/6/13

According to a recent survey conducted by Workshare, most employees (81%) access work documents on the go, but most (72%) are using unauthorized file-sharing services. The survey revealed that:

- 72% of those questioned had not received authorization from their IT department to use their consumer-based file sharing application, up from 66% in 2012.
- Over half (62%) of knowledge workers use their personal devices for work.
- The majority (69%) of these workers also use free file sharing services to collaborate and access shared documents

US charges 5 more in $45M global cybercrime scheme

From news.cnet.com, 11/18/2013

Five more people have been arrested in connection with a global cybercrime ring blamed for the theft of $45 million from banks around the world in a matter of hours. The five men join eight other men who were indicted in May with participating in a scheme to rob thousands of ATMs using bogus magnetic strip cards. One of those original named defendants—believed to be the ringleader of the cell—was murdered in the Dominican Republic in April. Using data stolen during hacks into two credit card processors, the ring made more than 40,500 withdrawals in 27 countries during two sprees in December and February, prosecutors said. The defendants eliminated the withdrawal limits from accounts during the intrusions and then fanned out across multiple cities with old hotel keys or expired credit cards encoded with the correct account information and access codes to quickly drain ATMs. The new defendants face up to seven-and-a-half years in prison, as well as forfeiture and fines of up to $250,000.

90% of workers in Britain cannot resist clicking on a link

From www.net-security.org, 11/20/13

90% of UK workers surveyed have clicked on a web link embedded in an email with two-thirds (66%) admitting they very rarely first check to ensure the link is genuine. The study identified three types of clicking behavior:

- Compulsive clickers: 46% of surveyed workers fall into the Compulsive Clickers category. According to the research, 24–30 year olds are most likely to click on an unverified web link with 60% admitting that they always or often click.
- Cautious clickers: 44% of those surveyed are Cautious Clickers who only occasionally click on a web link sent to them and when they do, 23% of them will check to see if the link is genuine. The most cautious are those in the 55+ age rage (47%).
- Never clicks: Only 10% of those surveyed are in the Never Clicks category who say they would never click on a web link received via an email.

HealthCare.gov targeted by more than a dozen hacking attempts

From arstechnica.com, 11/14/2013

Hackers have attempted more than a dozen attacks on HealthCare.gov, according to published news reports citing a top US official. All of the attacks failed and remain under investigation, including the recent discovery of software designed to overload HealthCare.gov with more traffic than it could handle. There is no evidence that the DIY denial-of-service tool was ever actively used. 16 reports from HHS are under investigation as well as one open source report about a denial of service.

Consultant's Corner

A Holistic Approach to Cyber Security

"Phishing" or "Spear Phishing" attacks have received a lot of attention over the past several years. "Spear Phishing" is especially effective since these emails are directed at individuals whom the attacker has some knowledge of, such as the intended victim's line of work, company, or personal interest. Companies have started informing employees of the tactics used by attackers and as a result, attackers are starting to use different methods, such as watering hole attacks. The attack might be an infected webpage intended to deliver malware, a link on the webpage designed to erroneously redirect the user to a compromised website, or free software that contains malicious code. The goal of all these different attacks is to obtain access to the user's workstation. A compromised workstation at work is preferable, but a compromised company laptop or home PC that is used to connect to a company network through a VPN tunnel is just as good. After all, chances are the targeted user visits the same websites at home as they do at work.

A holistic approach to cyber security is the best defense against attacks like these. A site cyber security assessment is a great starting point for any company, since a thorough site assessment will focus on all aspects of the company's security posture. Security best practices should be emphasized in any regulated or non-regulated environment. Assessments may be for a particular Process Network with limited assets to an entire site with multiple Process Networks. The following list includes some high-level areas that should be examined during a site assessment:

Security Policies and Procedures
These are the documents that govern the corporate and industrial environment. These documents should be reviewed for thoroughness and possible gaps.

Security Awareness and Training
Security awareness could come in the form of emails containing security awareness posters or alerting employees to potential cyber threats. Most companies have generic cyber security training for all employees. Job-specific training is even more effective.

Company Personnel and Contractors
Interviews with company personnel and contractors establish a real baseline for cyber security awareness and helps determine the level of compliance with company policies and procedures.

Cyber Asset Identification
A list of critical assets and their support systems should be created and compared against existing documentation.

Systems Management
This includes contingency planning, patch management, and configuration control (physical and logical).

Physical Security
Physical access to the critical assets should be restricted to authorized personnel.

Electronic Security
This category would include firewall and IPS rules, access control list, network configurations, and anti-malware software.

Stopping all attacks at the first or second level is unlikely. This is why properly identifying and protecting critical assets and their support systems is crucial. A policy stating that only corporate-owned laptops may VPN to the business network may help minimize the risk. Another control would be a jump server placed between the business network and process network. The cyber security landscape is constantly changing. The only way to effectively defend against attacks is to apply cyber security in a holistic fashion.

This month's contributor to Consultant's Corner is
Stephen Santee
Consultant, Critical Infrastructure & Security Practice, Invensys
stephen.santee@invensys.com

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
November 2013 / Issue 26

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.

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.

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**