July 2013 / Issue 22

The Cyber Advisor

Invensys Critical Infrastructure & Security Practice

this issue

- What is cyber security?
- Industry News
- Cyber News
- Consultant's Corner

What is cyber security?

What is cyber security? If you ask 100 people, you may be surprised to find that you get 100 different answers. Cyber security has different meanings to everyone; understandably, it depends on the industry you're in, the process control network you run, and the types of regulations that oversee your specific industry. A control system engineer has a distinct definition, but IT experts may have a completely different definition. To add to the confusion, everybody wants to be cyber secure or they have a mandate to be cyber secure, but because their views are all different, it slows down the process to engage in an effective cyber security program.

Regardless of what definition is the most correct, Invensys focuses on clients' needs and what clients believe cyber security means, since there may be a gap between their definition and their specific needs to comply with best practices, corporate policies, and government regulations. It is also important to understand that cyber security is not just a hardware and software solution but rather how these items are implemented and maintained in a comprehensive cyber security program.

The reasons for implementing cyber security can be almost as numerous as there are definitions for the term itself, yet some will insist they have nothing to protect. Many people understand the need for cyber security, but how do we explain to management why we need it? Consider the questions below:

- Are there competitors who would benefit from your intellectual property?
- Are you sure none of your critical systems "touch" the internet?
- Do you rigorously scan all USB drives and ensure they are under constant surveillance while being used on the plant premises?

A comprehensive cyber security solution is based on an assessment of the current network, development of the cyber security solutions that address the client's needs (regulatory or internal), the implementation of the cyber security solution, and most importantly the management of the solution once it's up and running.

At Invensys, cyber security is viewed as a holistic approach. The bottom line is everyone has something they need to protect. Whatever your definition of cyber security is, the Invensys cyber security team can provide you with a comprehensive solution to address your cyber security needs.

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

Attack Motivations
- 62% Cyber Crime
- 26% Hacktivism
- 8% Cyber Espionage

Top 3 Attack Targets
- 26% Industry
- 22% Government
- 10% News

Top 5 Attack Techniques
- 28% SQL
- 18% Unknown
- 14% DDoS
- 11% Targeted Attack
- 7% Account Hijacking

Industry News

Researchers to show new ways to hack oil, gas, and water plants

From www.reuters.com, 7/27/13

Cyber security researchers next week will demonstrate how hackers can potentially wreak havoc on critical U.S. infrastructure, even causing explosions by altering the readings on wireless sensors used by the oil and gas industry. The presentations at the Black Hat conference in Las Vegas showed how key industries remain vulnerable to cyber attacks, in part because companies are reluctant to replace expensive equipment or install new safeguards unless ordered to do so by regulators or offered economic incentives, experts say. "We've got this cancer that is growing inside our critical infrastructure. When are we going to go under the knife instead of letting this fester?" said Patrick C. Miller, founder of the nonprofit Energy Sector Security Consortium. "We need to restructure some regulations and incentives."

Cyber security spending in critical infrastructure to hit $46 billion globally

From biztech2.in.com, 7/18/13

The digitization of critical infrastructures has provided substantial benefits in terms of socio-economic developments—improved productivity, better connectivity, greater efficiencies. Yet some of these attributes also carry significant risks. Always-on Internet connectivity has ushered in a new cyber-age where the stakes are higher. Disruption and destruction through malicious online activities are the new reality: cyber-espionage, cyber-crime, and cyber-terrorism. Despite the seemingly virtual nature of these threats, the physical consequences can be quite tangible. ABI Research estimates that cyber security spending for critical infrastructure will hit $46 billion globally by the end of 2013. Increased spending over the next five years will be driven by a growing number of policies and procedures in education, training, research and development, awareness programs, standardization work, and cooperative frameworks, among other projects.

Oil and gas industry urged to focus on cyber security

From www.mywesttexas.com 7/11/13

From producing wells to tank batteries to pipelines, computer networks are playing an increasingly important role in the operations of the nation's oil and gas industry. Because of that increasing importance, the Obama administration is urging the industry to strengthen its cyber security capabilities. To that end, U.S. Secretary of Energy Ernest Moniz has announced a new public private partnership comprised of the Energy Department, industry experts, the Department of Homeland Security, and other stakeholders. This partnership will create tools to help operators assess their cyber security capabilities and prioritize their actions and investments to improve security.

Brute-force cyber attacks on critical infrastructure intensify

From www.securitymagazine.com 7/12/13

The Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) warned that attacks against critical infrastructure are growing, with more than 200 brute-force cyber attack incidents reported between October and May, surpassing the 198 total attacks in all of FY 2012. According to a ComputerWorld article, the newly issued report states that more than half of the attacks were against the energy sector—49 malicious IPs attacked natural gas companies across the Midwest and Plains. A further 17 percent of attacks targeted the manufacturing sector.

Cyber attacks targeted key components of natural gas pipeline systems

From ThreatPost, 7/1/13

The Department of Homeland Security's ICS-CERT publicly revealed information on a series of attacks that targeted gas compressor station operators earlier this year. According to ICS-CERT, on February 22, 2013, it received a report from a gas compressor station owner about an increase in brute force attempts to access its process control network. Based on analysis by ICS-CERT, the attacks were originally traced back to 10 IP addresses. However, after other critical infrastructure asset owners were notified, it was discovered that similar brute force attempts to compromise their networks also occurred. Those new reports yielded 39 additional IP addresses where attacks appeared to originate from.

Cyber News

Cyber attacks account for up to $1 trillion in global losses

From www.cnet.com, 7/22/13

While still costly, cyber attacks might not be depleting government cash at the rate previously thought. A new joint report released Monday by security firm McAfee and the Center for Strategic and International Studies has lowered the estimate from $1 trillion in global annual losses to a range of $300 billion to $1 trillion. The report's authors say that estimating the annual costs of cyber attacks is extremely difficult because some companies hide their losses, while others don't even know the value of what has been stolen from them. In the new report, the authors look at losses in six categories: the loss of intellectual property, cybercrime, loss of business information, service disruptions, the cost of securing networks, and reputational damage to a hacked company.

Cyber security collaboration in Europe

From www.net-security.org, 7/10/13

The EU agency ENISA is supporting the development of standards for products and services in cyber security by signing a collaboration agreement with two of the major standardization bodies in the EU, the European Committee for Standardization (CEN) and the European Committee for Electrotechnical Standardization (CENELEC). The cooperation agreement has the objective of contributing more effectively to understanding and resolving Network and Information Security issues related to standardization, in particular in different ICT sectors that are of relevance for ENISA.

Current cybercrime market is all about cybercrime-as-a-service

From www.net-scurity.com, 7/2/13

The cybercrime market is constantly evolving, and it is currently full of knowledgeable individuals who have focused on their core competencies to offer services to those who lack the skills, patience, or time to make what they want or need for their criminal exploits. "The marketplace contains many stakeholders, ranging from formal, legitimate organizations selling vulnerabilities to parties that meet their strict eligibility criteria to underground websites that allow individuals to offer illegal services," says McAfee CTO Raj Samani and Senior Threat Research Engineer François Paget in their latest white paper titled Cybercrime Exposed.

Phishing attacks rise, evolve

From www.securityweek.com, 7/1/13

Say the word phishing, and there are people who would probably begin to think back to a quiet day on a boat. But the kind of phishing that begins with a "ph" is far from relaxing, and it is on the rise. According to a new report from Kaspersky Lab entitled "The Evolution of Phishing Attacks: 2011-2013," an estimated 37.3 million Internet users were hit by phishers between 2012 and 2013. That represents an 87 percent increase from between 2011 and 2012, with most of the users being targeted residing in Russia, the U.K., India, Vietnam, and the U.S. The top two ways that phishing attacks are spread are through the Internet (87.91 percent) and email (12.09 percent).

Mobile attacks will continue to increase and grow more sophisticated

From www.securityweek.com, 7/1/13

A new report from Juniper Networks outlines the trends and the year-over-year growth of the mobile malware market, including the fact that criminals are making a tidy profit as a result of their efforts. Monitoring from March 2012 until March 2013, Juniper charted the growth in the mobile malware market, and noticed a few patterns—most notably the fact that criminals have turned the process into a vast money making enterprise. The number of mobile threats grew rapidly during the monitoring period—spiking an astounding 614% to 276,259 malicious apps in all, which the company says proves that criminals are showing a major interest in mobile development.

Attackers embedding backdoors into image files

From www.networkworld.com, 7/21/13

Researchers at Sucuri, a firm focused on website security awareness and attack recovery, have discovered attackers using a known but rather uncommon method of maintaining access to an already compromised server: They're hiding backdoors inside the headers of legitimate image files. Daniel Cid, Sucuri's CTO, told CSO in an interview that the company has discovered more than a dozen sites.

Consultant's Corner

Network Management

Periodically, we encounter entities using non-managed switching equipment for their plant control networks. Plant control networks are loosely defined as utility networks that support ancillary connectivity to control system platforms. These networks are not the control system backbone that transmits the process adjustments or receives the data from the instrumentation. The main reason for the unmanaged equipment is convenience and cost.

While the equipment is convenient and inexpensive, it has no capability to provide visibility into what is occurring on the network. Additionally, since the equipment can't be managed, it can't be secured. Having unmanaged equipment makes it impossible to secure the interior because the physical ports can't be disabled if they're not in use. This provides a potential vector for an inadvertent introduction of a virus. Human nature is to connect to port if it is available.

Visibility is usually provided by Simple Network Management Protocol (SNMP) and an SNMP Element Manager. The Element Manager is a computer that can query manageable equipment to collect statistical information. This can be percentage utilization of a particular port or something like CPU utilization. The element manager polls the equipment at a regular interval and usually presents the information in a graphical form. The graphical form can usually be mapped out in hourly, daily, or monthly increments. This can show what normal looks like. Is it high utilization because there is a virus or is it the daily back up of the system attached to a particular port?

There are several versions of SNMP—Version 1, Version 2c, and Version 3. Version 1 and Version 2c pass in clear text on the wire and can be seen with a network sniffer. Version 1 and 2c use SNMP communities. The default SNMP communities shipped by most manufacturers are Public and Private. These two communities should always be changed. The Public community provides read-only access, which can be used to enumerate the environment and hosts. The Private community can be used to configure the equipment using an SNMP set. Version 3 uses encryption in conjunction with privilege levels; since the traffic is encrypted it is not easily intercepted. SNMP version 3 should be used in lieu of the older standards when it is available on the equipment. SNMP also sends traps, which is usually an adverse event such as the wrong SNMP community being used to poll the equipment, a power supply failure, or excessive errors on a particular interface.

The other protocol typically used to gain insight is syslog. Syslog sends messages, usually to the same SNMP element manager. These messages are event related, i.e. user A logged in to the equipment at 8:40 and at 8:41 configured port 4. It follows that you probably want to create unique users on the equipment so that you can determine whether the appropriate individual is configuring the equipment rather than using a generic administrative account that might be used by an individual who might not necessarily be associated with your company. Syslog has 7 category levels, 0 – 2 usually require immediate action. Typically, alerts can be configured on syslog traffic and on the SNMP traps so that an individual can take action.

This months contributor to Consultant's Corner is
David Milne
Consultant, Critical Infrastructure & Security Practice
Invensys
david.milne@invensys.com

The Cyber Advisor
Invensys Critical Infrastructure & Security Practice
July 2013 / Issue 22

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 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 help them understand the demands of Control 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 actively participate 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 Assessment, Development, Implementation, 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.

Join us on Blogger

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**