August 2013 / Issue 23

The Global Cyber Advisor

Invensys Critical Infrastructure & Security Practice

this issue

Long Hot Summer

As summer winds down, we find that cyber criminals did not take a vacation. A quick look at statistics shows the amount and frequency of cyber attacks are continuing to rise rather than decrease, with the top five threats being data breaches, malware, DDoS, mobile threats, and industrialization of fraud; and they are all interrelated (Info Security, June 2013).

Although there have been several reported incidents of data breaches, there has been no significant publicized cyber attacks on a U.S. power plant to date. An ever-growing number of utilities are taking steps to mitigate attacks; nevertheless, the industry remains too vulnerable. Utilities remain high-value targets. A targeted attack can cause a disruption in services for a prolonged period, triggering civic and economic unrest.

Of organizations that acknowledged cyber attacks, InfoSec found that the top impacts were:

- Employee downtime/business disruption: 33%
- System downtime: 32%
- Loss/compromise of data: 19%

When organizations were asked to rate their organization's ability to protect endpoints and servers from emerging threats, 66 percent of respondents said between "average" and "non-existent."

Many of these attacks are targeted and originating from nation-states such as Russia and China, according to Massachusetts-based cloud platform provider Akamai. By 2017, the global cyber security market is projected to skyrocket from $63.7 billion in 2011 to $120.1 billion, with an estimated 18 victims per second (go-gulf.com). Symantec's 2013 Internet Security Threat Report states that there was a 42 percent increase in targeted attacks last year with most aimed at industries and corporations with less than 250 employees.

Cyber attacks will continue to be a fact of life; it is important to understand that a "one size fits all" approach of firewalls and anti-virus software is inadequate in addressing potential threats. A best practices cyber security approach that addresses the specific challenges of your sites is the only way to provide a comprehensive security solution that will increase your overall cyber security posture.

August 2013
Cyber Attack Statistics
- Hackmageddon.com

Attack Motivations
- 57% Cyber Crime
- 33% Hacktivism
- 6% Cyber Warfare

Top 3 Attack Targets
- 29% Government
- 26% Industry
- 9% Individual

Top 5 Attack Techniques
- 21% Defacement
- 21% Account Hijacking
- 19% Unknown
- 15% SQL
- 9% DDoS

Industry News

Not cyber myths: hacking oil rigs, water plants, industrial infrastructure

www.networkworld.com, 9/1/2013

If about 55 million people were to suddenly lose power and be plunged into darkness because malware attacked the smart grid, would you rank that as a large-scale cyber attack? It happened a decade ago, according to Eugene Kaspersky of Kaspersky Lab. At the AFCEA Global Intelligence Forum, he said a worm designed to attack Windows systems unexpectedly attacked Unix servers instead, and that malware was responsible for the infamous Northeast blackout of 2003.

Oil, gas field sensors vulnerable to attack via radio waves

www.computerworld.com, 8/25/2013

Sensors widely used in the energy industry to monitor industrial processes are vulnerable to attacks from 40 miles away using radio transmitters, according to alarming new research. Researchers Lucas Apa and Carlos Mario Penagos of IOActive, a computer security firm, say they've found a host of software vulnerabilities in the sensors, which are used to monitor metrics such as temperature and pipeline pressure, that could be fatal if abused by an attacker.

Cyber criminals are targeting you and your utility

chemical-facility-security-news.elp.com, 8/14/2013

"I visited a relative in another state recently and was surprised to find that my debit card didn't work at Target. I knew I had money in my account to cover the transaction, but because it was Sunday, I couldn't call my bank. To expedite my checkout, I gave the cashier my credit card. It was declined, too," a consumer explained. Cyber criminals are part of life. While they can create problems for individuals, their threat to utilities is much worse.

Water sector eyes federal cyber security efforts

www.wateronline.com, 7/31/2013

The water sector is watching closely as the federal government moves forward on plans to bolster cyber security at private and public entities. Federal cyber security legislation won the approval of a key Senate panel in late July. The bill would formally give the National Institute of Standards and Technology (NIST) the authority to create voluntary cyber security guidelines, an undertaking it has already begun.

How cyber security helps to transport gas safely across the continent

www.bulk-solids-handling.com, 8/12/2013

Operating and maintaining a gas pipeline involves numerous safety concerns. A cyber security assessment is one of the solutions that helps to maintain safety parameters—especially when handling explosive and flammable goods such as natural gas. The pipeline organization, which was incorporated in the USA in the early 1900s, is one of the largest combinations of natural gas and electric utility companies. While large interstate natural gas pipelines may serve major wholesale users such as industrial or power generation customers directly, it is the distribution system that actually delivers natural gas to most retail customers, including residential users.

Cyber security in the nuclear power sector

www.power-eng.com, 8/15/2013

In today's digital age, many critical business operations take place in cyberspace, requiring companies to take measures to protect their employees and business infrastructure from cyber attacks. Malicious individuals and groups, whether aiming to steal personal information or to completely destabilize an Internet network or critical infrastructure system, can expose sensitive personal and business information and disrupt critical operations. Critical infrastructure, such as electrical power generation or transmission and distribution systems, experience escalated costs to protect against potential exploitation that could adversely impact operations. The processes and practices designed to protect networks, computer programs, and data from attack, damage, or unauthorized access is known as cyber security.

Cyber News

Cyber security expert: assume you're being hacked right now

www.crn.com, 8/21/2013

When it comes to IT security, it's best to assume hackers or cyber criminals have already penetrated your network, according to cyber security expert Roger Cressey. Unfortunately, Cressey said, the U.S. is still dealing with many of the same problems it saw more than a decade ago, from data beaches to security critical infrastructures. "All of those issues are still relevant today," he said, "which means we have not done a good job of trying to address the fundamental issues that are driving Cyber security."

Industrial Control Systems requirements defined by new cyber security standard

www.waterworld.com, 8/20/2013

A new ISA99 standard addresses risks arising from the growing use of business information technology (IT) cyber security solutions to address industrial automation and control systems (IACS) cyber security in complex and dangerous manufacturing and processing applications. The ISA-62443 series of standards, being developed by the ISA99 committee of the International Society of Automation (ISA) and adopted globally by the International Electrotechnical Commission (IEC), is designed to provide a flexible framework to address and mitigate current and future vulnerabilities in IACS.

Hacktivism: The real threat

www.inforisktoday.com, 8/7/2013

DDoS attacks launched by hacktivists are often seen as little more than an interruption in services for an organization, but Terry Ray of Imperva highlights a greater worry hidden behind the attacks. "The reality is [distributed-denial-of-service attacks] are just the front end, if you will, of hacktivism," says Ray, vice president of worldwide security engineering for web application security provider Imperva.

The Rise of Critical Infrastructure Attacks: Understanding the Privileged Connection and Common Thread

www.intelligentutility.com, 8/1/62013

Over the past two years, an alarming number of headline-grabbing cyber attacks, viruses, and data breaches have targeted critical infrastructure—Stuxnet, Flame, Shamoon, and Red October to name just a few. These attacks have kept many organizations dealing in critical infrastructure on high alert. Recently, for example, researchers uncovered that the industrial control system used to manage Google's Australian offices had several security vulnerabilities that would enable hackers to adjust the heating and cooling controls in their offices (which could potentially damage equipment sensitive to heat and humidity). Subsequent research showed that hundreds of businesses across Australia are just as susceptible to attack—they have similar vulnerabilities in their building control systems as well.

India's national cyber security policy

isikkim.com, 8/14/2013

In order to deal with cyber security in an effective and holistic manner, the Department of Electronics and Information Technology has put in place a comprehensive national cyber security strategy. Accordingly, it is following an integrated approach with a series of legal, technical, and administrative steps to ensure that necessary systems are in place to address the growing threat of cyber attacks in the country. Cyber Regulation Advisory Committee reconstituted and notified under Section 88 of Information Technology (Amendment) Act, 2008. The First meeting of the Committee was held on November 29, 2012.

Cyber security council launched in Lithuania

www.lithuniatribune.com, 8/9/2013

Lithuania's Cyber Security Council held its first meeting earlier this month and discussed protection of the critical information infrastructure, the Interior Ministry said. Participants of the meeting shared opinions about identification of Lithuania's critical information infrastructure, consolidation of cyber security capacities, and technological solutions for protecting the Lithuanian cyber space against outside attacks.

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
August 2013 / Issue 23

Consultant's Corner

Keeping the Holes Plugged

In March 2013, Todd Wheeler gave some excellent guidance in selecting a patch management tool. That said, one of our team's most common quotes is:

> *Cyber security is so much more than firewalls and anti-virus software. All successful security solutions are part of an overall program that addresses who will manage, maintain, and upgrade the solution for its lifetime. The latest and greatest technology can't really just be dropped in and expected to perform—you must match it with your plans and strategy. The message is: consider what the needs are, develop a program, and* ***then*** *determine the technical controls.*

If you've started to delve into patch management due to regulatory requirements like NERC, or just as a good business "best practice," you probably became quickly overwhelmed. In fact, you have probably felt like a person on a cold night with a blanket that is too small. You pull the blanket up to keep your chest warm but then your feet get cold. You pull the blanket down to get your feet warm, but then your chest gets cold. There is constantly a "hole" that you can't plug to keep yourself warm. The same is true with patch management. Just when you think you have a good handle on Microsoft patches and have that automated, you have to deal with device firmware (PLCs, network equipment, network-connected peripherals) and the whole myriad of other software on the market. It also doesn't help when many vendors list updates but are not forthcoming in saying which updates are security-related or not.

So, how do you deal with all this "patching uncertainty?" First, keep it simple and look at the title of what you are doing: patch management, not patching perfection. Patch management is all about prioritizing and managing risk. Before patching your environment, you need to establish a patch management *program* to help you evaluate, prioritize, test, and deploy patches. In some cases, you may even determine not to deploy a patch and rely on other security controls (i.e. compensating measures), such as the anti-virus software and firewall solutions you have in place to mitigate that risk.

How does this approach line up with regulatory requirements? In the case of NERC CIP, it fits in perfectly. For example, the title of NERC CIP 007 R3 Version 4 is "Security Patch Management," which immediately tells you that your primary focus should be on "security" patches, not every patch ever created. In fact, this NERC CIP standard only requires three key things:

1. Evaluate *security* patches within 30 days of their publication
2. Document the implementation of patches (note that no timeframe is given for *when* you have to deploy the patch)
3. Document compensating measures applied to mitigate risk when the patch is not installed

This gives power generation facilities the flexibility they need to develop a patch management program that includes adequate time to prioritize, test, and deploy patches without the patch itself becoming a threat to reliability of the electrical grid. If installing a patch threatens reliability, then a generation facility can schedule the patch at a time that minimizes that risk or decide not to deploy it.

This is just the beginning of establishing a patch management program. Other items such as scope of equipment and software for patching must be determined. The Invensys Critical Infrastructure and Security Practice has the skills and the resources to help our clients, no matter what industry. We are structured to help with an establishment of an entire cyber security program, not just patch management.

This month's contributor to Consultant's Corner is
Charles Smith
Consultant, Critical Infrastructure & Security Practice, Invensys
charles.smith@invensys.com

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
August 2013 / Issue 23

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**