The Global Cyber Advisor

Invensys Critical Infrastructure & Security Practice

May 2014
Issue 32

this issue

97% of companies using network defenses get hacked anyway

From arstechnica.com, 5/20/14

A security study drawing data from more than 1,600 networks over a six-month period found that 97 percent of the networks experienced some form of breach—despite the use of multiple layers of network and computer security software. Each of the networks already had a "defense in depth" architecture, combining firewalls, intrusion detection and prevention systems, and antivirus software. Despite that, the appliances detected over 208,000 malware downloads across the monitored networks, of which 124,000 were unique malware variants.

The Cost of Cyber Security

Cyber security is a growing international concern. Lloyd's of London has rated cyber security number three in threats to the global economy, up from 12th place in just one year, which isn't surprising when 93 percent of large companies and 87 percent of small companies have reported a cyber security breach (a breach does not imply a successful attack). The impact of cyber crime costs the global economy over $500 billion a year, with some estimates as high as $1 trillion. These are staggering figures, yet looking at the breakdown of an average cyber attack, one can see where these dollars come from:

- $11.56 million—average annualized cost of cybercrime incurred by an organization
- 122 successful attacks per week reported by companies
- 32 days—the average time to resolve a cyber attack
- $32,469—cost per day spent resolving a cyber attack

All of these numbers have increased since last year, yet many companies appear to be resolved to this fate. Over 75 percent say they have had or expect to have such an incident that results in negative public opinion. Soft dollars, such as impact to public opinion, are not even factored into the $500 billion number. There are many other soft dollars that have been negatively impacted as the result of a cyber attack, such as loss of reputation, loss or theft of sensitive and confidential information, and potential regulatory fines and/or lawsuits.

Cyber crime is a growing global business. Yet many ask, "what do cyber criminals want from my company?" It's simple—whatever you have. With the growth of Nation-State attacks, cyber espionage, and cyber terrorists, the answer typically lies within your industry. Many Nation-State attacks originate from developing countries that are interested in growing their critical infrastructure (power, chemical, water, oil/gas), so why not look at successful companies and how they design and operate their systems? Cyber espionage is a growing area of corporate theft, because businesses want to know how their competitors are growing their businesses. Cyber terrorism is also becoming more popular, as cyber terrorists often target companies to disrupt their business with a political agenda. To put things in perspective, the chart below from McAfee compares the cost of cyber activity to other criminal actions like piracy, drug trafficking, car crashes, and pilferage.

Putting Malicious Cyber Activity in Context

CRIMINAL ACTION	ESTIMATED COST	PERCENT OF GDP	SOURCE
GLOBAL			
Piracy	$1 billion to $16 billion	0.008% to 0.02%	IMB
Drug Trafficking	$600 billion	5%	UNODC
Global cyber activity	$300 billion to $1 trillion	0.4% to 1.4%	Various
US ONLY			
Car Crashes	$99 billion to $168 billion	0.7% to 1.2%	CDC, AAA
Pilferage	$70 billion to $280 billion	0.5% to 2%	NRF
US- cyber activity	$24 billion to $120 billion	0.2% to 0.8%	Various

From McAfee's Economic Impact of Cyber Crime and Cyber Espionage, July 2013

All industries will fall victim to cyber crimes, but to different extents. The cost of cyber crime will be higher for industries identified as critical infrastructure—energy, utilities, chemical, water, and oil/gas. There is no mistaking it. The direct financial losses associated with a cyber crime can only be equaled by the cost of remediation. The old saying that the best offense is a great defense holds true for cyber security. A comprehensive cyber security strategy will help establish a strong security posture that will in turn moderate the cost of cyber attacks.

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
May 2014 / Issue 32

Industry News

ICS-CERT Confirms Public Utility Compromised Recently

From www.threatpost.com, 5/21/14

Attackers recently compromised a utility in the United States through an Internet-connected system that gave the attackers access to the utility's internal control system network. The utility, which has not been named, had remote access enabled on some of its Internet-connected hosts and the systems were only protected by simple passwords. Officials at the ICS-CERT, an incident response and forensics organization inside the Department of Homeland Security that specializes in ICS and SCADA systems, said this week that the public utility was compromised "when a sophisticated threat actor gained unauthorized access to its control system network." The attacker apparently used a simple bruteforce attack to gain access to the Internet-facing systems at the utility, and then compromised the ICS network.

Schneider Electric accelerates its transformation

From www.plantengineering.com, 5/9/14

As growth in key segments of its U.S. customer base expands, Schneider Electric sees itself as growing and changing after the acquisition of Invensys in 2013. The acquisition of Invensys gave Schneider Electric a strong and complementary portfolio of products in the oil and gas sector. What was less discussed at the time, but an area Laurent Vernerey, the new president and CEO of Schneider Electric's North American operations, thinks is just as crucial, is a competency in cyber security management. "Compliance is a key question," he said "We're seeing a lot more questions about cyber security. That picture has changed significantly. (Invensys) had assembled a team of cyber security experts, and they bring a legacy of what's happening at the compliance level.

China cited in cyber-spying case

From www.securityinfowatch.com, 5/19/14

Attorney General Eric Holder says Chinese military officials hacked into six U.S. nuclear power, metals and solar products industries. Holder says the companies affected are Alcoa World Alumina, Westinghouse Electric Co., Allegheny Technologies, U.S. Steel Corp., United Steelworkers Union, and SolarWorld. The charges contained in a federal indictment are the first U.S. cyber-espionage charges against state actors. The hackers are accused of stealing trade secrets and economic espionage.

300% growth in enterprise attacks across UK and Ireland

From www.net-security.org, 5/1/14

At Infosecurity Europe 2014, FireEye announced the release of its Regional Advanced Threat Report for the United Kingdom and Ireland (UKI). Detailing malicious activities captured by the FireEye Security Platform throughout 2013, the report found that an average of over 70 new infections occurred within enterprises every day and that 12 major UKI verticals were impacted by advanced persistent threat (APT) attacks. Drawing on worldwide data gathered from nearly 40,000 unique cyber attacks (more than 100 per day) and over 22 million malware command and control communications, the Advanced Threat Report provides a look into cyber attacks that routinely bypass traditional defenses such as firewalls, next-generation firewalls, IPS, anti-virus, and security gateways. The United Kingdom was one of the top ten countries in the world exposed to APT attacks when measured by number of unique verticals targeted. The verticals that were most targeted by APT attacks in 2013 were Federal Government, Energy/Utilities/ Petroleum Refining, Financial Services, and Higher Education.

Utilities face growing risk of cyber attack

From www.theglobaandmail.com, 5/7/14

North America's electricity grid is facing increasing risk of cyber attacks from criminals, terrorists and foreign states, and utilities have to devote growing resources to defend the system, a regulators' conference was told this month. The technological modernization of the grid—from smart meters to less-centralized generation—is creating new opportunities for cyber threats to enter the system, and new risk for the utilities. The threats range from nuisance hacking that can disrupt software systems, to attacks on the grid by shadowy, state-backed groups in an effort to steal secrets, sow terror or disable critical infrastructure.

CIP (Critical Infrastructure Protection) market worth $105.95 billion by 2018

From itbusinessnet.com, 5/1/14

MarketsandMarkets forecasts the global critical infrastructure protection market to grow from $63.7 billion in 2013 to $105.9 billion in 2018.

Schneider Electric

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
May 2014 / Issue 32

Cyber News

Hacks on widely used traffic control gear could cause gridlock and chaos

From arstechnica.com, 5/1/14

Hacks that allow spies, villains, or terrorists to manipulate traffic signals may seem like the exclusive province of action movies, but a well-known security researcher says they're not as far-fetched as many people may think. Cesar Cerrudo of security penetration testing firm IOActive said he has identified more than 50,000 devices in New York, Washington DC, Los Angeles, and cities in at least seven countries around the world that can be hacked using inexpensive gear that's easy and—at least in the US—legal to obtain and operate. The equipment Cerrudo used included a drone flying at heights of 650 feet and radio hardware that sells for $100. With more sophisticated transmitters, antennas, and other hardware, he said an attacker could be as far away as two miles from the targeted signals.

2014 starts with record-breaking malware traffic

From www.net-security.org, 5/7/14

During the first quarter of 2014, AppRiver screened more than 14 billion messages, nearly 10.9 billion of which were spam and another 490 million that contained malware. Once again, the United States was the leading country of origin for spam email messages, and Europe logged the second-highest total with Spain, Germany and Italy making up the top three countries. January was a record-breaking month for malware traffic since 2008, with one in every 10 pieces of email being malicious.

Average corporate cost of data breach up to $3.5m

From www.ibamag.com, 5/8/14

According to a recently released study from the Ponemon Institute, the average cost of a corporate data breach is up to $3.5 million—a 15% increase since last year. And if it helps to boil that down to per-record cost, researchers associated with the ninth annual Cost of Data Breach Study: Global Study found that each stolen record containing confidential information costs a company an average $145. That's up 9% since last year.

Cyber-alert stats paint stark picture

From www.financierworldwide.com, 5/15/14

The average US firm faces 10,000 potential cyber-security alerts daily, more than any IT team can possibly process, according to an analysis of web traffic by threat protection and containment firm, Damballa. The Damballa State of Infections Report Q1 2014 culled information from ISP and mobile traffic, as well as its own customers, finding that the busiest networks generated up to 150,000 alerts. While the report makes clear that a large number of these alerts are innocent, the problem lies in the sheer volume of alerts that firms face. Large multinational firms with a global reach face up to 97 active infected devices per day, according to the report, a relatively small amount. However, the manual work required to actually find infections is the number one security challenge. An overload of security alerts aids cybercriminals such as those who attacked firms in the US retail sector during 2013. During the time of its three-month security breach, Neiman Marcus experienced 30,000 security alerts. Sifting the alerts that indicated criminal activity from false positives and innocent but anomalous behavior, extending the period in which the firm was under attack.

63% of orgs believe they can't stop data theft

From www.net-security.org, 5/1/14

Websense released the first report of the Ponemon Institute survey, "Exposing the Cybersecurity Cracks: A Global Perspective," which gives new insight into why cybercriminals have a foothold in the broader enterprise. The new survey of nearly 5,000 global IT security professionals reveals a deficit in enterprise security systems. The findings reveal:

- 57 percent of respondents do not think their organization is protected from advanced cyber attacks and 63 percent doubt they can stop the exfiltration of confidential information
- 69 percent believe cyber security threats sometimes fall through the cracks of their companies' existing security systems
- 44 percent of companies experienced one or more substantial cyber attacks in the past year
- 59 percent of companies do not have adequate intelligence or are unsure about attempted attacks and their impact

Schneider Electric

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
May 2014 / Issue 32

Using Security Best Practices

As networked information systems become more essential to modern life, the need for securing availability, integrity, and confidentiality for our cyber asset critical infrastructure becomes increasingly urgent for our country. In other words, the nation's capability for cyber asset protection lags significantly behind our nation's networking capability because nearly every day new threats and attacks are discovered and launched, providing cyber attackers the opportunity to inflict damage to our national and economic security. At this time, there are two primary approaches: security to meet compliance and security using best practices.

General Best Practices Recommendations

These general Security Best Practices are a first step toward providing specific audit guidelines that CISOs, CIOs, IGs, and the US-CERT can adopt to ensure these agency systems have the baseline security controls in place that are most critical. These Security Best Practice recommendations take advantage of the knowledge gained in analyzing the myriad of attacks being actively and successfully launched against federal systems and our nation's industrial base systems and identifying the key controls most critical for stopping those attacks. This effort also takes advantage of the success and insights from the development and usage of standardized concepts for identifying, communicating, and documenting security-relevant characteristics/data.

- Inventory of authorized and unauthorized hardware.
- Inventory of authorized and unauthorized software; enforcement of white lists of authorized software.
- Secure configurations for hardware and software on laptops, workstations, and servers.
- Secure configurations of network devices such as firewalls, routers, and switches.
- Boundary Defense.
- Maintenance, Monitoring and Analysis of Complete Audit Logs.
- Application Software Security.
- Controlled Use of Administrative Privileges.
- Controlled Access Based On Need to Know.
- Continuous Vulnerability Testing and Remediation.
- Dormant Account Monitoring and Control.
- Anti-Malware Defenses.
- Limitation and Control of Ports, Protocols and Services.
- Wireless Device Control.
- Data Leakage Protection.

Industry-Specific Best Practices Recommendations

This reference list provides a non-prioritized list of the top ten most common and threatening vulnerabilities to control systems in the Electric Sector based on the combined expertise of the NERC Control System Security Working Group (CSSWG) members. The information presented in this section is specific to the Power Generation Industry and is further limited to only the cyber assets directly related to power generation.

- Inadequate Policies, Procedures, and Culture Governing Control System Security.
- Inadequately Designed Control System Networks That Lack Sufficient Defense-In-Depth Mechanisms.
- Remote Access to the Control System without Appropriate Access Control.
- Auditable System Administration Mechanisms (System Updates, User Metrics, etc.) are Not Part of Control System Implementation.
- Inadequately Secured Wireless Communication.
- Use of a Non-Dedicated Communications Channel for Command and Control, such as Internet Based SCADA, and/or Inappropriate Use of Control System Network Bandwidth for Non-Control Purposes (e.g., VOIP).
- Lack of Quick and Easy Tools to Detect And Report on Anomalous or Inappropriate Activity. Inadequate or Non-Existent Forensic and Audit Methods.
- Installation of Inappropriate Applications on Critical Control System Host Computers.
- Software Used in Control Systems is Not Adequately Scrutinized.
- Control Systems Command and Control Data Not Authenticated.

By implementing best practices as a company's security guidance, companies will have a solid foundation to build upon. This solid foundation will provide for definable audits and network measurements while giving employees a stable work environment. When companies deploy security programs to meet regulations, these companies tend to sway back and forth changing company security requirements, standards and employee expectations as regulations requirements change. This approach leaves information technology professionals and employees frustrated and resisting security implementations.

Companies must start with and maintain a consistent methodology that only comes with using Best Practices as the foundation for a security program to protect and truly be successful.

This month's contributor to Consultant's Corner is Tim Johnson
Principal Consultant, Critical Infrastructure & Security Practice, Invensys
tim.johnson.us@schneider-electric.com

Schneider Electric

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
May 2014 / Issue 32

Most Popular Blog Posts This Month

Schneider Electric accelerates its transformation (May 13, 2014)
As growth in key segments of its U.S. customer base expands, Schneider Electric sees itself as growing and changing after the acquisition of Invensys in 2013. The acquisition of Invensys gave Schneider Electric a strong and complementary portfolio of products in the oil and gas sector. What was less discussed at the time, but an area Laurent Vernerey, the new president and CEO of Schneider Electric's North American operations, thinks is just as crucial, is a competency in cybersecurity management. "Compliance is a key question," he said "We're seeing a lot more questions about cybersecurity. That picture has changed significantly. (Invensys) had assembled a team of cybersecurity experts, and they bring a legacy of what's happening at the compliance level.

USB sticks bring down 2 U.S. power plants (January 22, 2013)
Two U.S. power plants were affected from malware unknowingly transferred from USB sticks.

Microsoft rushes to fix Internet Explorer browser after attacks; no fix for XP users (May 1, 2014)
Microsoft Corp is rushing to fix a bug in its widely used Internet Explorer web browser after a computer security firm disclosed the flaw over the weekend, saying hackers have already exploited it in attacks on some United States companies.

Hackers find first post-retirement Windows XP-related vulnerability (April 30, 2014)
Microsoft told customers that cyber criminals are exploiting an unpatched and critical vulnerability in Internet Explorer using "drive-by" attacks.

U.S. eyeing charges in foreign cyber-espionage case (May 19, 2014)
The United States is preparing to announce criminal charges against Chinese military officials in an international cyber-espionage case, a government official said.

Featured Post: Meet the Invensys Cyber Security Team

Cyber Security Consulting Advantage
Assessing cyber assets requires adequate resources and a thorough understanding of the industry-specific regulatory requirements. In this video, the Invensys cyber security consultant team sums up the areas where many sites look for guidance to augment their current capabilities. Security and compliance take a tremendous amount of effort. Help is available to become secure and compliant… and stay that way.

Visit us on Blogger!

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
May 2014 / Issue 32

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