April 2013 / Issue 19

The Global Cyber Advisor

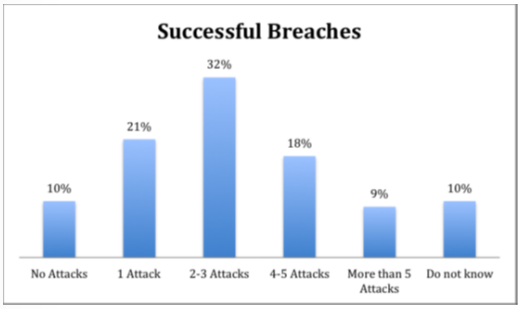
Invensys Critical Infrastructure & Security Practice

this issue

Attitudes Shifting to Continuously Secure

Over the past two years, more companies have changed their attitudes on the need for cyber security. A recent survey by Bit9 reported that 64% of companies believe they will be a target of a cyber attack in the next six months. While this may not be surprising, the reasons for the paradigm shift might. Malware is up over 50% from last year (McAfee) and SQL injections along with remote access remain the top attack vectors for the fourth year running (Trustware). These statistics have been around for years, with many companies taking a "look-and-see" approach. The real driver in the attitude shift towards cyber security is not statistics but rather the unfortunate reality of a security breach.

A Ponemon Research Institute shows that 90% of companies suffered a computer hack in the last 12 months, with some suffering multiple attacks, as seen in the graph below.



Of all the attacks reported, 41% claimed at least half a million U.S. dollars ($500,000) in damages, and some reported they were unable to determine their immediate losses.

Why are these attacks increasing and why are they so successful? One answer may lie in the fact that targeted attacks increased by 42% last year, averaging approximately 116 per day, resulting in data theft and industrial espionage, according to Symantec. A similar study by Ponemon revealed that two-thirds of the companies surveyed believe the increase in cyber attacks is neither due to "media hype" nor perceived weaknesses in their defenses, but rather the result of a growing number of hacktivists. Over 61% of respondents feel that they are most likely to be attacked by Anonymous and/or other hacktivists or Nation-States. A recent Mandiat report exposed just how real this threat is, exposing how Nation-State sponsored organizations like China's APT1 have stolen hundreds of terabytes of data from at least 141 organizations across a diverse set of industries.

The bright side of the attitude shift is a greater understanding of how to implement cyber security effectively. 74% of the same companies who believe they will be the target of a cyber attack also feel that securing end-points such as laptops and desktop computers is ineffective. The majority now believe that the greatest impact on preventing cyber attacks is implementation of best practices and better security policies.

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

Attack Motivations
- 50% Hacktivism
- 40% Cyber Crime
- 7% Cyber Espionage

Top 3 Attack Targets
- 22% Finance
- 25% Government
- 12% News

Top 5 Attack Techniques
- 50% DDoS
- 13% SQL
- 9% Targeted
- 8% Unknown
- 6% Account Hijacking

Industry News

How do utilities prepare for the cyber security executive order?

Gridinsights-energycentral.com, 4/1/2013

President Obama signed an executive order with the intentions of beefing up cyber security protection. The order itself states that "repeated cyber intrusions into critical infrastructure demonstrate the need for improved cyber security. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats." While the order discusses the need to enhance security, make our critical pieces more flexible, and develop just a nicer general interaction between infrastructure sources (read: play nicer), few details are given about what this will all mean for electric utilities, NERC CIP, the programs already in place, or how involved the Department of Homeland Security (DHS), who is leading this push, will become.

Gas pipelines have become a hot topic

readingeagle.com, 4/13/2013

Natural gas pipelines were among the topics that came up this week when three of the four congressmen representing Berks County attended an event held by the Greater Reading Chamber of Commerce & Industry at Met-Ed in Muhlenberg Township. Reps. Joe Pitts and Jim Gerlach, both Chester County Republicans, and Rep. Charlie Dent, a Lehigh County Republican, were there. Rep. Pat Meehan, a Delaware County Republican, couldn't attend. He was at another meeting fulfilling his duties as chairman of a House subcommittee on cyber security. Pipelines are a hot topic in this region because Commonwealth Pipeline wants to build a 30-inch interstate line that could pass through the heart of this county and through Chester County. Texas Eastern Transmission has plans to expand an existing line that runs through Berks.

Cyber security standards for electric grid expanding

www.businessweek.com, 4/18/2013

The U.S. Federal Energy Regulatory Commission proposed to revise its cyber security standards for the nation's electric grid, expanding the rules to more than 60 additional companies. The agency today voted to start the process for updating the existing critical infrastructure protection standards. The revisions are aimed at enhancing the "security posture" of companies that link to the grid, according to a FERC statement. Cyber security is becoming a critical issue for electric utilities as components such as generators, power meters, and appliances are interconnected using the Internet. White House National Security Adviser Thomas Donilon said in a March 11 speech that the U.S. is concerned about "cyber intrusion emanating from China at a very large scale."

FERC reviews grid cyber security protection

www.csmonitor.com, 4/19/2013

A dozen new requirements for cyber security controls would help ensure the protection of the U.S. electrical grid, the Federal Energy Regulatory Commission (FERC) said. FERC announced it was moving to strengthen cyber security standards through 12 requirements under the Critical Infrastructure Protection Reliability Standards.

Chemical industry offers improvements to chemical security regulations

www.ameriacnchemistry.com, 4/1/2013

The Department of Homeland Security (DHS) has made notable progress on implementing the Chemical Facility Anti-Terrorism Standards (CFATS) program, but there is still room for improvement. That's according Timothy J. Scott, Chief Security Officer and Corporate Director Emergency Services and Security at The Dow Chemical Company, who testified before the House Subcommittee on Environment and the Economy today. Testifying on behalf of the American Chemistry Council (ACC), Scott said chemical security remains a top priority for ACC's members, who continue to make significant investments in security measures to safeguard their facilities. He also noted that ACC continues to support effective federal regulation of chemical security and that DHS has made measurable improvements in the implementation of CFATS despite early difficulties.

Cyber News

Global nature of advanced cyber attacks

news.cnet.com, 4/24/2013

FireEye released a report that provides insight into the global nature of malware communication activity related to sophisticated cyber attacks. "The threat landscape has evolved, as cyber threats have outpaced traditional signature-based security defenses, such as anti-virus, and permeated around the world, enabling cybercriminals to easily evade detection and establish connection inside the perimeter of major organizations," said FireEye CEO David DeWalt.

96% of state-backed cyber spying traced to China

www.net-security.org, 4/23/2013

New statistics contained in Verizon's Data Breach Investigation Report 2012 found that 19 percent of all attacks were carried out by agents acting on behalf of their government. Researchers recorded more cyber espionage incidents than ever before although the majority of attacks were carried out by criminals looking to make money. Bosses will be comforted by the finding that "external actors" were responsible for the majority of data breaches, with 92 percent of all incidents involving an attack from someone working outside the organization.

Cyber attacks growing more sophisticated

www.eweek.com, 4/23/2013

Technology organizations are among the most frequently attacked by cyber criminals and the majority of Advanced Persistent Threat (APT) attacks—89 percent—are associated with tools developed and disseminated by Chinese hacker groups, according to cyber security specialist FireEye's "The Advanced Cyber Attack Landscape" report. The report found 184 nations house communication hubs, or command and-control (CnC) servers, with Asia and Eastern Europe accounting for the majority of activity. CnC servers are used heavily during the life cycle of an attack to maintain communication with an infected machine by way of callbacks, enabling the attacker to download and modify malware to evade detection, extract data, or expand an attack within a target organization.

8 in 10 companies suffered web-borne attacks

www.net-security.org, 4/1/2013

The vast majority of organizations that allow employees to freely access the Web are experiencing high rates of malware threats, including phishing attacks, spyware, keyloggers, and hacked passwords, according to Webroot. The study, which surveyed Web security decision -makers in the United States and United Kingdom, found an overwhelming 79 percent of companies experienced Web-borne attacks in 2012. These incidents continue to represent a significant threat to corporate brands.

World's biggest DDoS that almost broke the Internet

Thehacknews.com, 4/1/2013

The last week of March saw probably the largest distributed denial-of-service (DDoS) attack ever. A massive 300Gbps was thrown against Internet blacklist maintainer Spamhaus' website, but the anti-spam organization CloudFlare was able to recover from the attack and get its core services back up and running.

Malware attacks occur every three minutes

www.net-security.org, 4/4/2013

Malware activity has become so pervasive that organizations experience a malicious email file attachment or Web link as well as malware communication that evades legacy defenses up to once every three minutes, according to FireEye. "The high rate at which cyber attacks are happening illustrates the allure of malware," said Zheng Bu, senior director of research. "Today, malware writers spend enormous effort on developing evasion techniques that bypass legacy security systems. Unless enterprises take steps to modernize their security strategy, most organizations are sitting ducks."

Consultant's Corner

Continuously Secure: Network Switch Security—Protecting Layer 2

Network switches in a Distributed Control System (DCS) network play a vital role interconnecting digital assets that comprise a DCS network. Network switches not only interconnect devices in redundant and mesh networks, but also decide alternate communications paths and control much of the information flowing across the network. The DCS would not function properly or would be at risk if the network switch were to be compromised by an intruder.

Configuring network switch security not only helps eliminate the possibility of compromise, but proper settings can help minimize unwanted network traffic caused by a failing network device.

Network switch security should address the following:

1. **Access Control**
    a. Physical Access – Place switches in locked cabinets or controlled areas while password protecting console access.
    b. Logical Access – Manage the switches on a management network rather than the DCS network.
    c. Role-Based Access – Similar to access on a DCS; not all users require administrative rights to the switch.
2. **Patch Management**
    a. Test Software Patches – Test patches to ensure security is not degraded due to a software upgrade
    b. Deploy Software Patches – Vendors provide software patches to address flaws in their software that could lead to a compromise.
3. **Configuration Control**
    a. Create a repeatable checklist to provide for configuration continuity.
    b. Disable ports, use port security, and configure enhanced security features.
4. **Monitoring**
    a. Set up logging on the network switch to aid in detecting malicious activity.
    b. Ensure logging provides detailed information that can assist in after-the-fact investigations.

Protecting network switches from compromise will help ensure that the DCS is able to perform as expected. A secure network switch will help provide high availability and the self-healing network performance that is expected out of DCS networks. In support of continuous cyber security, the Invensys Critical Infrastructure and Security Practice (CISP) team can perform assessments and configuration hardening on network switches.

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

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
April 2013 / Issue 19

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**