November 2012 / Issue 14

The Cyber Advisor

Invensys Critical Infrastructure & Security Practice

this issue

Nov. 2012
Cyber Attack Statistics
- **Hackmageddon.com**

Attack Motivations
- 60% Hacktivism
- 40% Cyber Crime

Top 3 Attack Targets
- 24% Government
- 20% Industry
- 15% Torrent Sites

Top 5 Attack Techniques
- 33% SQL
- 33% Defacement
- 21% DDoS
- 7% SQLi/XSS/FPD
- 2% Other

BYOD or BYOT

Bring Your Own Device (BYOD) has been gaining in popularity for years, driven in part by the prevalence of next generation mobile devices. Many companies have embraced BYOD as a cost savings program, letting the employees foot the bill for the latest smartphone or tablet technology. Too few companies have explored the all-too-real security consequences of permitting such a practice without proper policies and safeguards in place, making it, in many cases, Bring Your Own Threat (BYOT).

Most companies have gone to great expense to secure their DCS networks and critical assets, with many more companies enforcing policies and procedures about what programs can be run on what computers and treating USB thumb drives with the utmost scrutiny. In short, companies continue to go to great lengths to secure their assets. But what about those unsecure assets like BYOD? The majority of the devices in question are wireless and access the internet using existing plant spectrum, bandwidth, and the companies' network. There is inherent security risk in providing access to unsecure devices. The security is made only more complex when you do not know how these devices have been used.

- 65% do not use any type of security solution
- 46% of people who use a device for work allow someone else to use it
- 45% access internet via unsecure Wi-Fi
- 35% have had their device lost or stolen
- 31% open text messages from anonymous senders

It should come as little surprise that McAfee's 2Q 2012 Threat Report focused on mobile malware. The report found the biggest increase in malware samples detected in the last four years—a 1.5 million increase since 1Q 2012—the bulk of the malware exploiting the various new mobile platform OS as well as SMS-sending malware, mobile botnets, spyware, and destructive Trojans.

While much has been done to keep unknown entities from gaining access into your control systems, what about the threats that are already on your plant site? Even if these devices are only allowed in the break rooms, not knowing how or where they were used can still compromise your network once they connect to the Internet. Once connected, they are like a rogue device, with no controlled security. While BYOD does have its advantages, it is another cyber security threat vector that must be addressed. Like the USB thumb drive, BYOD is here to stay. With BYOD, you must always link responsibly.

Industry News

Hackers steal and publish e-mails from UN Nuclear Agency

News.cnet.com 11/27/2012

Hackers have made their way into one of the servers of the United Nations' International Atomic Energy Agency, according to Reuters. The agency confirmed that the hackers stole information and published it online. "The IAEA deeply regrets this publication of information stolen from an old server that was shut down some time ago," agency spokesperson Gill Tudor told Reuters. "The IAEA's technical and security teams are continuing to analyze the situation and do everything possible to help ensure that no further information is vulnerable."

Stuxnet Hit 4 Oil Companies

www.isssource.com 11/15/2012

Major U.S. oil companies already facing increasingly sophisticated cyber attacks by China have also been infected by the Stuxnet virus, which has attacked countries around the globe, including Germany, Indonesia, and Kazakhstan. U.S. intelligence sources said victims of the Stuxnet virus include Baker Hughes, ConocoPhillips, Marathon, and Chevron, who was the first of the group to declare earlier this month it had been attacked by the virus.

U.S. electric power grid "inherently vulnerable" to terrorist attacks

www.homelandsecuritynewswire.com 11/16/2012

The U.S. electric power delivery system is vulnerable to terrorist attacks that could cause much more damage to the system than natural disasters such as Hurricane Sandy, blacking out large regions of the country for weeks or months, and costing many billions of dollars, says a newly released report by the National Research Council. According to the report, the security of the U.S. electric power system is in urgent need of attention. The power grid is inherently vulnerable physically because it is spread across hundreds of miles, and many key facilities are unguarded.

Info about Zero-Day SCADA flaws offered for sale

www.net-security.org, 11/21/2012

Following in the footsteps of French Vupen Security, Malta-based start-up ReVuln has also decided to sell information about zero-day vulnerabilities to companies and governments instead of sharing it with the developers of the flawed software and hardware. In a recently released video, the company showcased a number of zero-day exploits for SCADA systems and claimed that all the vulnerabilities affect the server-side and are remotely exploitable. According to the company, they discovered vulnerabilities in products by General Electric, Schneider Electric, Kaskad, ABB/Rockwell, Eaton, Siemens, and other well known SCADA/HMI vendors.

More Flame Modules Could Be Lurking

ThreatPost.com, 11/16/2012

After years of research and investigation into the cyber-espionage attacks that began with the discovery of Stuxnet and continued with Flame, Duqu, and Gauss, there are still many details that are unknown. While researchers have a pretty good handle on many of the tools' capabilities, experts say that there may be other modules from these weapons still in circulation that have yet to be discovered. Researchers believe that many of these recent attacks are connected, whether through code re-use, similar targets, or other factors, and think that several of them may have been the work of the same team, or at least related groups. Each of the tools seemed to have a different purpose, with Stuxnet targeting a uranium enrichment facility in Iran, for example, and Gauss being used to monitor financial transactions in specific banks. And while much has been learned about the attackers' methods and their target base, researchers say that there may well be pieces of the attack tools that are yet unknown and are still in operation right now.

Cybergeddon now? Industrial control systems targeted

SecurityTube.net, 11/5/2012

Security researcher Reid Wightman from the firm ioActive has found an undocumented back door in CoDeSys, the management software used by 261 different manufacturers of ICS devices. The back door gives full access without requiring authentication and has prompted ICS-CERT to issue an alert. They've discussed ICS before, including the Stuxnet operation against Iran's uranium enrichment program, how an air gap doesn't work to protect networks any more, and even war studies academic Thomas Rid reckons that cyberwar will not happen. But hackers are getting smarter and, by the time you read this, it's likely that a module to detect Wightman's newly discovered vulnerability will have already found its way into automated hacking tools. Doesn't this change the balance of power?

Cyber News

Digitally signed ransomware lurking in the wild

Www.net-security.org, 11/23/2012

Trend Micro researchers have spotted two ransomware variants bearing the same (probably stolen) digital signature in order to fool users into running the files. Other than that, the malware acts like any other ransomware: it blocks the victim's computer and shows messages that seem to come either from the FBI or the UK's Police Central e-crime Unit: "Users may encounter these files by visiting malicious sites or sites exploiting a Java vulnerability," say the researchers.

Attackers Had Access for Months in South Carolina Data Breach

ThreatPost.com, 11/21/2012

Attackers had two months of unfettered access to South Carolina's Department of Revenue systems in a classic targeted attack that began with a phishing email and ended with the loss of electronic tax return data, payment cards, and personal information on 3.8 million files, possibly dating back to 1998. Governor Haley said her administration could have done more to prevent the breach, and that she had accepted the resignation of DOR director Jim Etter. Haley pointed in particular to the lack of two-factor authentication securing access to sensitive systems, and the lack of encryption on the Social Security numbers stolen in the attack. Like most executives, Haley admitted a false sense of security in that the state's systems were compliant with IRS standards that did not mandate encryption of Social Security numbers.

65% Of Organizations Experience Three DDoS Attacks A Year

DarkReading.com, 11/13/2012

Despite the increasing sophistication and severity of cyber attacks, a survey of more than 700 senior IT professionals reveals that organizations are surprisingly unarmed to deal with today's threat landscape. In a recent report titled "Cyber Security on the Offense: A Study of IT Security Experts," the Ponemon Institute and Radware®, found that while 65% of organizations experienced an average of three distributed denial-of-service (DDoS) attacks in the past 12 months, less than half reported being vigilant in monitoring for attacks—much less putting into practice proactive and preventative measures to protect their organizations. "The reality is that cyber threats are outpacing security professionals, leaving most organizations vulnerable and unprepared."

Cyber attacks against Lockheed have "increased dramatically"

News.Cnet.com, 11/12/2012

Cyber attacks against Lockheed Martin—one of the largest defense contractors for the U.S. government—have stepped up significantly in both pace and savvy, according to Reuters. "The number of campaigns has increased dramatically over the last several years," Lockheed vice president and chief information security officer Chandra McMahon said in a news conference, according to Reuters. "The pace has picked up."

Out-of-date, vulnerable browsers put users at risk

www.computerworld.com, 11/9/2012

Is your browser up to date? According to the results of a new survey from security software vendor Kaspersky, nearly a quarter of the browsers currently in use are out of date. Surfing the Web with a vulnerable browser is a recipe for disaster. The Web browser has evolved to become the primary software used on many PCs. People access their email, surf websites, create documents and spreadsheets, access cloud-based file storage and sharing sites, and share with others on social networking sites—all through the browser. Attackers know this as well, which is why it is exceptionally risky to use a browser with known vulnerabilities.

Consultant's Corner

Security Appliances

In today's cyber security landscape, a firewall is considered a paramount first line of defense in securing your networks. Many Distributed Control Systems, SCADA, Automation, and Process networks sit behind these devices that empower the nation's critical infrastructure. While attacks on secure networks have increased in frequency and sophistication, firewalls have developed into security appliances capable of fulfilling multiple roles in defending networks. The current generation of security appliances offers the following technologies to enhance your cyber security solution:

- **Zone Segregation**
  Security appliances have the capability to segregate multiple networks into virtual zones within the device. This allows isolation of networks and the ability to control what flows in and out of the zones in great detail.

- **Rules and Policies**
  In addition to controlling traffic flows between zones, policies support the configuration of anti-virus, traffic inspection, logging, and specific ports and services to further define what is permissible data traversing your network.

- **Multi-Layer Operation**
  Security appliances have the capability of operating in a transparent mode or routed mode. In transparent mode, the device passes traffic at layer 2 and downstream nodes are unaware of the device. This allows the device to be implemented with a simple configuration and provides traffic logging and alerting. In routed mode, the device operates as a traditional firewall and router would, allowing segregation of network segments directly connected to the unit. Routing, NAT, or a combination of the two can be used to manage traffic paths.

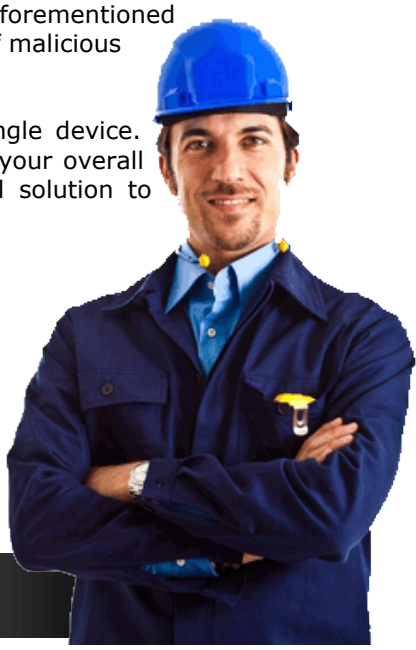
- **Failover and Load Balancing**
  Most security appliances support high availability configurations. Traditionally, devices can be physically paired for stateful failover or configured independently for load balancing and failover purposes. To further enhance failover capabilities, monitors, triggers, and configuration integrity checks can be enabled.

- **Anti-Virus and Traffic Inspection**
  Security appliances possess the capability to inspect data streams for virus, Trojan, and worm signatures. Many appliances also feature traffic inspection at upper OSI layers as well as compressed data for attack signatures and behaviors. This feature allows the device to filter and alert on suspect traffic such as port scans, network mapping, and compressed payloads.

- **Logging and Alerting**
  While logging and alerting are certainly not new features, when paired with the aforementioned technologies they become an essential component of early detection and suppression of malicious data in your environment.

Current generation security appliances have many features and technologies built into a single device. However, these devices should still be treated as point solutions and play an integral part of your overall cyber security program. A best practice layered approach should be a tiered, policy-based solution to ensure that the integrity of your cyber assets are protected and monitored.

This month's contributor to Consultant's Corner is
Gary Richardson
Consultant, Critical Infrastructure & Security Practice, Invensys
gary.richardson@invensys.com



The Cyber Advisor
Invensys Critical Infrastructure & Security Practice
November 2012 / Issue 14

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**