The Global Cyber Advisor

Invensys Critical Infrastructure & Security Practice

December 2014
Issue 39

this issue

- Trends to Expect in 2015
- Industry News
- Cyber News
- Consultant's Corner
- CISP Blog

APAC cyber attacks to rise in 2015

From www.interaksyon.com, 12/3/14

Online users should be more careful and vigilant in 2015 as cyber attacks are expected to increase further in conjunction with expanding Internet adoption in different parts of the world but most especially in the Asia Pacific region, online security company Trend Micro said. In a press statement, Trend Micro said that users "should expect that at least one of their accounts, whether on Web services or online portals will be compromised." The company cited the APAC region, where the Philippines is located, as an attractive target for cyber attacks due to the growing prevalence of social media. Trend Micro urged the public to be more vigilant in their password use and online security to ward off theft of user credentials.

Invensys is becoming Schneider Electric

Trends to Expect in 2015

Now that 2014 has come to a close, security experts are predicting new trends and urging companies to review their cyber security policies and programs to help counteract the expected increase in malicious events. Trend Micro's annual security predictions report forecasts 8 trends for 2015 (trendmicro.com):

1. More cybercriminals will turn to darknets and exclusive-access forums to share and sell crimeware.
2. Increased cyber activity will translate to better, bigger, and more successful hacking tools and attempts.
3. Exploit kits will target Android, as mobile vulnerabilities play a bigger role in device infection.
4. Targeted attacks will become as prevalent as cybercrime.
5. New mobile payment methods will introduce new threats.
6. We will see more attempts to exploit vulnerabilities in open source apps.
7. Technological diversity will save IoE/IoT devices from mass attacks but the same won't be true for the data they process.
8. More severe online banking and other financially motivated threats will surface.

2015 will prove to be yet another challenging year in cyber security. Even though decisions concerning security have usually been driven by compliance, the increased likelihood of cyber attacks have companies realizing that they must protect themselves. As 2014 ends, we must be prepared for the number of cyber attacks and data breaches to escalate. Having a cyber mitigation plan in place as well as implementing a thorough and comprehensive cyber security program is the best defense. Have a plan, take action, monitor, and be vigilant. Happy New Year!

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
December 2014 / Issue 39

Industry News

FBI warns of possible Iranian cyber attack on US defense and energy institutions

From www.jpost.com, 12/13/14

The FBI has warned US businesses to be on the alert for a sophisticated Iranian hacking operation whose targets include defense contractors, energy firms and educational institutions, according to a confidential agency document. The operation is the same as one flagged by cyber security firm Cylance Inc as targeting critical infrastructure organizations worldwide, cyber security experts said. Cylance has said it uncovered more than 50 victims from what it dubbed Operation Cleaver, in 16 countries, including the United States. The FBI's confidential "Flash" report, seen by Reuter, provides technical details about malicious software and techniques used in the attacks, along with advice on thwarting the hackers.

A good cyber defense can protect pharmaceutical and medical device companies

From Schneider Electric, Dec. 2014

The inability to keep data safe can undermine the results of a clinical study and an organization's ability to generate new products and ensure the safety of existing ones. Much of the world's critical infrastructure and vital goods are at significant risk of cyber security threats. Add to this discomforting list of threats to medical devices and pharmaceutical manufacturing. Some companies in different industries underestimate the threat of cyber attacks believing falsely that because their control and monitoring systems are not connected to the Internet, they many not be subject to traditional hacking. "The big theory is that there is no technology connection between us in the plant and others in the outside world so our control systems are safe," said Doug Clifton, global director, critical infrastructure and security practice at Schneider Electric.

China is capable of launching cyber strikes against US power grids

From nationalinterest.org, 12/3/14

Admiral Mike Rogers, head of U.S. Cyber Command and the director of the National Security Agency, told a congressional panel that China and "one or two" other countries would be capable of mounting a cyberattack that could shut down the power grid or other critical infrastructure. In addition, over the last two years, there have been a number of public reports that China-based hackers broke into industrial control systems (ICS). UglyGorilla, one of the five People's Liberation Army hackers indicted by the Department of Justice, reportedly hacked into the computers of a public utility in the northeastern United States, perhaps to map the system in preparation for a future attack.

A cyber attack may have caused a Turkish oil pipeline to catch fire in 2008

From www.slate.com, 12/11/14

In 2008, two years before Stuxnet was noticed, a Turkish oil pipeline mysteriously caught fire without triggering any sensors or alarms. Although Kurdish separatists claimed the attack, according to Bloomberg, a number of U.S. intelligence officials credit Russia, which was opposed to the Baku-Tbilisi-Ceyhan pipeline. Investigators found that the hackers used the security camera system's vulnerable software to gain entrance to the pipeline's control network and get to work. Beyond damaging the pipeline, the attack cost BP, the State Oil Fund of the Republic of Azerbaijan, and others millions of dollars, and also caused thousands of barrels of oil to spill close to a water aquifer. Security experts are increasingly convinced that America needs to prepare for an inevitable cyber attack on its own energy, transport, or financial infrastructure.

Coordinated cyber attacks on global critical infrastructure exposed

From www.net-security.org, 12/2/14

Cylance identified coordinated attacks by hackers based in Iran on more than 50 targets in 16 countries around the globe. Victim organizations were found in a variety of critical industries, with most attacks on airlines and airports, energy, oil and gas, telecommunications companies, government agencies and universities. Through custom and publicly available tools that use, among other methods, SQL Injection, spear phishing, water holing attacks and hacking directly through public websites, the attackers were able to extract highly sensitive and confidential materials and compromise networks with persistent presence to such a severity that they have control over networks of victims in 16 countries. Cylance found significant victims in Canada, China, England, France, Germany, India, Israel, Kuwait, Mexico, Pakistan, Qatar, Saudi Arabia, South Korea, Turkey, United Arab Emirates and the United States.

Schneider Electric

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
December 2014 / Issue 39

Cyber News

Cyber attacks, drones increase threats to plane safety

From www.reuters.com, 12/4/14

Cyber attacks and commercial drones pose a growing risk of commercial aeroplane crashes, a major insurer said, running counter to a long-term decline in fatal accidents and insurance premiums. Technical advances in aircraft design and navigation systems have reduced the chance of dying in a plane crash, but the reliance on computers poses new types of risks. "Cyber terrorism may replace the hijacker and bomber and become the weapon of choice on attacks against the aviation community," German insurer Allianz said in a review of aviation safety, publicly expressing concerns that other insurers have discussed in private.

Cyber security attacks targeting healthcare companies

From healthitsecurity.com, 12/3/14

If there weren't enough reasons already for healthcare organizations to have strong cybersecurity measures in place, a recent email phishing scam is targeting numerous organizations, including healthcare companies. More than 100 organizations have been attacked by cybercriminals for over a year, according to a report from FireEye, a security company. FireEye calls the online attackers FIN4, and explains that they don't infect their victims with malware, but instead capture usernames and passwords to victims' email accounts. From there they can read private email exchanges. Approximately two-thirds of the targeted companies are healthcare and pharmaceutical companies, the report explained. However, FIN4 has also targeted publicly traded companies or advisory firms that provide services such as investor relations, legal counsel, and investment banking.

Government and industry gear-up for new generation of cyber security

From www.militaryaerospace.com, 12/9/14

The recent cyber warfare hacker attack on entertainment giant Sony Corp. is yet another stark warning about the dire threats that cyber attacks and hacker terrorism pose to U.S. and allied military forces, public utilities, and commercial business. The severity of the cyber security threat cannot be overstated or overestimated; it's real, it's here, and we're only seeing the beginning of what is to come. The cyber attack on Sony reportedly has compromised the Social Security numbers and phone numbers of Hollywood entertainers, and has led to blackmail threats to coerce the company not to release a major theatrical movie that is nearly complete.

Phishing tops local online fraud cases in 2014

From www.themalaymailonline.com, 12/11/14

Phishing, which involves online banking, accounts for most online fraud with 2,993 incidents reported from January to October this year. Chief Executive Officer of CyberSecurity Malaysia, Dr Amirudin Abdul Wahab, in a statement, said the figure constituted 94 per cent of all 3,190 online frauds reported in the same period. "Clearly, criminals are aiming for financial gains. An average of 12 fraud incidents involving online purchases are reported every month or total 120 incidents from Jan to Oct this year," he said.

Rising cyber attacks prompt more investment in security

From www.gulf-times.com, 12/6/14

Technology firms and critical national infrastructure such as telecommunications networks are among the five major industries that invest heavily on security due to high risks of cyber attacks and threats, a senior official of Qatar-based global telecom company Ooredoo said. Mustapha Huneyd, head of Corporate Information Security, made the statement during a lecture on "Cyber Security Risk Management & Governance in the Telecoms Industry" at the Cyber Security Summit – Middle East. Huneyd said the 2014 Information Security Breaches Survey conducted by advisory firm PwC showed that both telecoms and technology sectors spend 13% of their IT budget on security. The survey revealed that "Large organizations now spend on average 11% of their IT budget on security; small businesses spend even more of their IT budget on security than large ones with an average of almost 15% of their IT budget" – the highest level ever recorded.

Schneider Electric

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
December 2014 / Issue 39

Indicators of Compromise and Effective Incident Handling: Part 1

Every day, the media issues a new warning of emerging threats to our cyber security and nearly as often we are hearing of how some organization has experienced a breach. By now most of us are running secured systems (or at least we all should be) that are segmented from the internet in some fashion with anti-virus and anti-malware programs installed on all applicable machines, using some type of encryption for communications, etc. But the question is what can be done when there is a suspected compromise? Lets begin with defining what constitutes a compromise and what "indicators" should in turn begin the enactment your incident handling process.

A "compromised computer" can be defined as any computing asset whose confidentially, integrity, or availability has been adversely impacted, either intentionally or unintentionally, by an untrusted source (either internal or external to the resource in question). This can occur through either some type of manual interaction with the target machine or via some type of automation, i.e. an infected web page that automatically installs malicious code on the target machine. One example of a compromise would be someone who attempts to gain unauthorized access to the target asset by impersonating a legitimate user or by conducting a brute force password attack. Alternatively, a target computer that becomes infected with some type of virus, worm, Trojan, or other malicious software could be considered compromised, depending on the circumstances. This all depends on where in the organization the machine is located, what other assets it has access to, the business purpose of the machine, the users logged in, etc. However, if the malicious software is detected and removed via traditional measures, i.e. AV software, in a timely manner, then it will more than likely not constitute a compromise. However, if the infection is widespread or other symptoms begin to appear, then the best judgment of your security/network team will need to be used as to whether or not to classify this as an incident and enact the incident handling process. Some of the more common indicators of a compromise are as follows:

- The target machine has began exhibiting unusual outbound network traffic such as DNS request anomalies and geographic irregularities
- The target machine is showing anomalies in privileged user account activity and multiple failed login attempts for non-existent user accounts
- The target machine exhibits sudden and unexplainable performance degradation along with suspicious registry and system file changes
- The appearance of inexplicable and unexpected system patching along with the sudden appearance of large amounts of data in the wrong places
- A complaint is received from a third party in regards to suspicious activity originating from your organization (such as excessive amounts of questionable email activity from a mail server)

If any or all of these indicators are discovered it is essential to the organization that they immediately begin a thorough investigation into the source and cause of the infection or hire an experienced third party to do so on your behalf. If an investigation is not commenced immediately, utilizing time proven industry standards, not only can loss of data and access to critical systems be diminished, but it can also cause irreparable brand damage as well. Confidence in your company's ability to provide its given services/products in a timely manner is of utmost importance to you and your customers, and without access to critical systems and data this could be virtually impossible. The next part of this article will discuss the importance of having an effective Incident Handling process.

This month's contributor to Consultant's Corner is Paul Pelletier
Consultant, Critical Infrastructure & Security Practice, Invensys
paul.pelletierl@schneider-electric.com

Schneider Electric

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
December 2014 / Issue 39

Most Popular Blog Posts This Month

Sony Paralyzed By Computer Hacker Attack With Ominous Message (November 24, 2014)
Things have come to a standstill at Sony today, after the computers in New York and around the world were infiltrated by a hacker. As a precaution, computers in Los Angeles were shut down while the corporation deals with the breach. It has basically brought the whole global corporation to an electronic standstill.

10 ways to protect your Devices and Data (November 19, 2014)
Gee, it used to be just your desk computer that needed protection from cyber thugs. Now, your connected thermostat, egg tray monitor, teen's smartphone, garage door opener, even baby monitor, are all game for cyber creeps.

Automakers aim to drive away car computer hackers (December 4, 2014)
Against the team of hackers, the poor car stood no chance. Meticulously overwhelming its computer networks, the hackers showed that - given time - they would be able to pop the trunk and start the windshield wipers, cut the brakes or lock them up, and even kill the engine. Their motives were not malicious. These hackers worked on behalf of the U.S. military, which along with the auto industry is scrambling to fortify the cyber defenses of commercially available cars before criminals and even terrorists penetrate them.

Companies Should Assume Cyber Attackers Are Already Inside (December 12, 2014)
Companies seeking to shield valuable data from criminals and government spying should assume the attackers have already penetrated their systems and adjust defensive strategies, security firms McAfee and Symantec Corp. said. "You must assume something is going on and you have to start looking for it," Patty Hatter, chief information officer and senior vice president of operations at Intel Corp.'s McAfee, said today at the Bloomberg Enterprise Technology Summit in London.

Featured Post: A Good Cyber Defense Can Protect Pharmaceutical and Medical Device Companies

The inability to keep data safe can undermine the results of a clinical study and an organization's ability to generate new products and ensure the safety of existing ones. Much of the world's critical infrastructure and vital goods are at significant risk of cyber security threats. Add to this discomforting list of threats to medical devices and pharmaceutical manufacturing.

Some companies in different industries underestimate the threat of cyber attacks believing falsely that because their control and monitoring systems are not connected to the Internet, they many not be subject to traditional hacking. "The big theory is that there is no technology connection between us in the plant and others in the outside world so our control systems are safe," said Doug Clifton, global director, critical infrastructure and security practice at Schneider Electric. Read the full article here.

Visit us on Blogger!

Schneider Electric

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
December 2014 / Issue 39

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.

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**