Schneider Electric

The Global Cyber Advisor

Invensys Critical Infrastructure & Security Practice

September 2014
Issue 36

this issue

Security experts scramble to plug "bash bug" hole

From www.newsmax.com, 9/26/14

A newly-discovered computer security flaw with the alliterative name "the bash bug" leaves a potential security hole in many widely-used operating systems. The bug makes use of a program called a "bash" used in Apple Macintosh, Linux and other operating systems. Most importantly, it is used in the software of the Apache web servers that run at least half the world's websites. It's also used in the software that connects many "smart" home devices to the Internet, including household security systems and even lighting systems. "This vulnerability is potentially a very big deal. It's rated a 10 for severity, meaning it has maximum impact, and "low" for complexity of exploitation – meaning it's pretty easy for attackers to use it," said Tod Beardsley of the security firm Rapid7.

Invensys is becoming Schneider Electric

ISF Maps to NIST Framework

Information Security Forum

The Information Security Forum (ISF), an international organization that is dedicated to investigating, clarifying, and resolving key issues in information security, released a "mapping" document for the NIST Framework earlier this month to be used with the ISF's standard of good practice (known as The Standard). The latest version of The Standard incorporated the NIST Framework's language so members of ISF can "determine which of their current controls satisfy the corresponding control objectives in the NIST Cybersecurity Framework, and thus demonstrate their alignment with it," said Steve Durbin, managing director of ISF. Using these tools together, ISF members are able to show clients and stakeholders that they are working toward a resilient, comprehensive cyber security program.

Released in February this year, the NIST Framework serves as a set of guidelines for businesses and organizations to bolster their cyber security programs, whether they already have a program in place or are working to create one from scratch. The framework's "common language makes use of familiar topics in information security and clearly-expressed control objectives within those topics" (info-securitymagazine.com).

According to ISF, the benefits of using The Standard to understand where your organization's level of compliance with the NIST framework are threefold (fedscoop.com):

- You can rely on a well-established, robust control set with sufficient detail to address the control objectives in the framework.
- The Standard of Good Practice covers not just technical topics, but includes operational and governance controls necessary to maintain a resilient information security program.
- You can assess your existing security arrangements against the Standard of Good Practice controls to determine how well you are currently satisfying the control objectives in the framework.

Though the Framework was released over six months ago, NIST is seeking all public feedback "to strengthen awareness of the framework and to promote its use as a basic, flexible and adaptable tool for managing and reducing cybersecurity risks" (info-securitymagazine.com).

NIST

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
September 2014 / Issue 36

Industry News

Norwegian oil industry hit by cyber attack

From www.energylivenews.com, 9/1/2014

At least 50 companies in Norway's oil and gas industry have been hacked, reports claim. A further 250 firms have also been warned by the nation's prevention unit for cyber attack – National Security Authority (NSM) – as it revealed the news. It is believed a virus has been spread via malware-infected emails sent to "selected individuals in large Norwegian companies." Kjetil Berg Veire, Head of information at the NSM has been quoted as saying: "I can confirm that the Norwegian National Security Authority has revealed a computer espionage operation especially targeted towards businesses within the oil and gas sector, the energy sector and military industry."

What to expect from Europe's NIS Directive

From www.computerweekly.com, 9/15/2014

Cyber security is one of the biggest issues currently facing governments and businesses in the EU and globally. In response to this, the European Parliament adopted a proposal for a Network and Information Security Directive (NIS Directive) in March 2014. The directive, which was originally proposed by the European Commission in 2013, is part of the European Union's cyber security strategy aimed at tackling network and information security incidents and risks across the EU. According to the commission's consultation, 57% of respondents had experienced information security incidents over the previous year, while the UK government recently rated cyber security as a Tier 1 threat to national security along with terrorism.

Asia Pacific region targeted by advanced cyber attacks

From manilastandardtoday.com, 9/13/2014

FIREEYE, Inc., the leader in stopping today's advanced cyber attacks, today announced the release of its Advanced Threat Report for the Asia Pacific region. Detailing malicious activities captured by the FireEye Security Platform throughout the first six months of 2014, the report finds the region more frequently attacked by various advanced persistent threat (APT) actors than the global average. Additionally, the Philippines was the most exposed ASEAN country to advanced persistent threat activity, with significant peaks in the first six months of this year.

Protecting America's power grid: calls for action

From www.cnbc.com, 9/11/2014

Electronic attacks on banks, retailers and oil companies have amplified calls to fortify the U.S.'s aging electric grid, which some believe is more vulnerable than ever to terrorism. For years, the more than 3,000 utilities that provide the United States with electricity have been the focus of security concerns. Yet in the shadow of the 13th anniversary of the Sept. 11 terror attacks, a growing threat from terrorists and multiple assaults on U.S. companies, risks to the energy grid appear to be multiplying. A sophisticated attack on the energy grid "is real and needs to be addressed urgently," said James Woolsey, chairman of the Foundation for the Defense of Democracies, in an interview. "A hacker could very seriously damage the grid."

Energy quote of the day: 'grid jihad'

From theenergycollective.com, 9/6/2014

The suggestion that ISIS-related militants could team up with Mexican drug cartels to disable the US power grid for an extended period of time seems a bit alarmist, but worth noting, particularly in light of 2 recent substation attacks in California. US power grid vulnerability, be it from cyber attack or direct assault, has been widely reported and it appears steps are being taken to strengthen security, though threats certainly remain. "Inadequate grid security, a porous U.S.-Mexico border, and fragile transmission systems make the electric grid a target for ISIS," said Peter Pry, one of the nation's leading experts on the grid, according to the Washington Examiner. Experts quoted in the article claim that if the grid were down for a year 9 out of 10 Americans "would likely perish." The likelihood of the entire power grid being down for a year seems rather low, but probably not impossible.

Schneider Electric

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
September 2014 / Issue 36

Cyber News

Government hackers try to crack HealthCare.gov

From newsfactor.com, 9/24/2014

The government's own watchdogs tried to hack into HealthCare.gov earlier this year and found what they termed a critical vulnerability -- but also came away with respect for some of the health insurance site's security features. Those are among the conclusions of a report released earlier this month by the Health and Human Services Department inspector general, who focuses on health care fraud. So-called "white hat" or ethical hackers from the inspector general's office found a weakness, but when they attempted to exploit it like a malicious hacker would, they were blocked by the system's defenses. However, the report concludes that more work needs to be done to bolster security.

Inside hackers seen as $40 billion threat for employers

From www.newsmax.com, 9/26/14

Fired from a job as a technology contractor for a Toyota Motor Corp. factory in Kentucky, Ibrahimshah Shahulhameed went home, logged into the company's computer network and attacked it with programming commands. It took the automaker months to fix the damage and landed Shahulhameed in prison. He is appealing the conviction. While attention has been drawn recently to outsiders suspected of attacking companies such as Home Depot Inc. and JPMorgan Chase & Co., Shahulhameed's case illustrates the growing threat from within. U.S. companies and organizations suffered $40 billion in losses from unauthorized use of computers by employees last year, according to SpectorSoft Corp. based in Vero Beach, Florida, which develops software that companies can use to monitor Internet activity of their workers.

FBI probes possible Russian cyber attack on major US banks

From www.hstoday.us, 9/3/2014

The FBI and US Secret Service are investigating a significant breach of corporate computer security at J.P. Morgan Chase & Co., the largest bank by assets in the United States, and several other unnamed financial institutions. The attack possibly was carried out by hackers with ties to Russia. "We are working with the United States Secret Service to determine the scope of recently reported cyber-attacks against several American financial institutions," FBI spokesman Joshua Campbell said in a statement. Although the extent of the attack remains unknown, highly skilled hackers allegedly infiltrated the bank and compromised gigabytes of data after slowly siphoning customer data from the company's corporate network over the course of a three month period. The hackers used layer upon layer of malware custom-built for J.P. Morgan's website.

Cyber threats among greatest national security dangers

From ibnlive.in.com, 9/10/2014

Terming cyber threats as one of the greatest national security dangers, the US has said the Obama administration has significantly enhanced the government's capabilities to address this challenge. "Cyber threats pose one of the greatest national security dangers that the United States faces, ranging from vulnerabilities in our critical infrastructure to identity theft from credit card information," White House Press Secretary Josh Earnest said. He said the Obama administration had significantly enhanced the government's capabilities by forging relationships with private sectors to prevent and mitigate the cyber incidents while increasing efforts to prosecute cyber criminals.

Belden research reveals Dragonfly malware likely targets pharmaceutical companies

From www.marketwatch.com, 9/15/2014

Belden Inc., a global leader in signal transmission solutions for mission-critical applications, released new research that shows the recently revealed Dragonfly (Havex) malware is likely targeting the pharmaceutical sector, not the energy sector as previously believed. Until now, advanced cyber attacks against industry have focused on the critical energy and chemical sectors. Manufacturing management teams are advised to update their risk assessments and ensure that their cyber security defenses can withstand what are clearly highly coordinated attacks by teams of professional hackers.

Schneider Electric

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
September 2014 / Issue 36

What's New in Windows Server 2012 and R2 Active Directory

You can divide the "What's New" categories in Windows Server 2012 Active Directory into two parts: “New Features” and “Improved Features.” We will cover the items that apply to both versions first and then review the items that apply to R2 version only. Either way, you're going to like what you see.

New Features

- **GUI for Recycle Bin:** Microsoft introduced the Active Directory Recycle Bin in Windows Server 2008 R2, but it was limited by its Windows PowerShell-only exposure. This time it gets a GUI.
- **UI for Fine-Grained Password Policies:** Also gaining a GUI are fine-grained password policies.
- **Dynamic Access Control (DAC):** Windows Server 2008 R2 brought the File Classification Infrastructure (FCI). This version's DAC adds far greater functionality to the (optional) second layer of FCI resource authorization.
- **Windows PowerShell History Viewer:** You see the Windows PowerShell commands that correspond to actions you perform in the Active Directory Administrative Center UI.
- **Windows PowerShell Cmdlets for Active Directory Replication and Topology:** More cmdlets.
- **Active Directory-Based Activation (ADBA):** The good: ADBA eliminates the need for a Key Management Service server. The bad: Only forthcoming Windows 8 computers can leverage ADBA.
- **Flexible Authentication Secure Tunneling (FAST):** The nickname for FAST is "Kerberos armoring," if that tells you anything. It isn't enabled by default and requires clients that support it.

- ## Improved Features

Virtual Snapshot and Cloning Support: Active Directory and hypervisor snapshots didn't mix before. Now they do, if your hypervisor supports VM Generation ID.

- **ADPREP Integrated into DC Promotion:** DCPromo is done when you add the Active Directory Role to Windows Server 2012.
- **Active Directory Federation Services (ADFS) Now In-Box:** Adding ADFS no longer requires a separate installation. ADFS also gains multiple improvements. Watch this space, because you'll be seeing and using more ADFS in the years to come.
- **Domain Join via DirectAccess:** Computers can now be domain-joined over the Internet. You'll need DirectAccess first. Trust me, you'll want it.
- **Kerberos Constrained Delegation (KCD) Across Domains:** Another one of those capabilities you've probably never used, but probably will in the future. KCD was first introduced in Windows Server 2003. Now it can span domains.
- **Group Managed Service Accounts (GMSAs):** MSAs in Windows Server 2008 R2 made administering service accounts easier. GMSAs in this version extend their support to clustered and load-balanced services.

Additional R2 Items

In Windows Server 2012 R2, Active Directory has been enhanced with the following value propositions to allow IT risk management while also enabling IT to empower their users to be productive from a variety of devices:

- IT administrators can allow devices to be associated with the company’s Active Directory and use this association as a seamless second factor authentication.
- Enable users to use single sign-on (SSO) from devices that are associated with the company’s Active Directory.
- Enable users to connect to applications and services from anywhere with the Web Application Proxy feature.
- Manage the risk of users working from anywhere, accessing protected data from their devices, with Multi-Factor Access Control and Multi-Factor Authentication (MFA).

While individually these new features might not seem like a lot, as a group they improve the usability and security of Active Directory. As members of the CISP team, this should give a broad overview of what we may encounter in the field and can be used as a guide in future service offerings.

This month’s contributor to Consultant’s Corner is Terry Mixon
Consultant, Critical Infrastructure & Security Practice, Invensys
terry.mixon@schneider-electric.com

Schneider Electric

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
September 2014 / Issue 36

Most Popular Blog Posts This Month

Shopping Online May Actually Be Safer Than Shopping In Person (September 19, 2014)
The list of major retailers that have been hacked keeps growing. But while tens of millions of people have seen their credit card numbers fall into the hands of hackers, online shoppers at those stores appear safe. In recent breaches at Target, Neiman Marcus and, most recently, Home Depot, the retailers said online customers were not affected. The hacks raise a curious question at a time when danger seems to lurk on every corner of the Internet: Is it actually safer to shop online than in person?

Russian hackers publish nearly 5 million Gmail passwords (September 12, 2014)
Nearly 5 million Gmail passwords were published on a Russian-language bitcoin security forum on Tuesday, according to a report from The Daily Dot. The publisher, known as "tvskit," claimed 60 percent of the 4,930,000 leaked usernames and passwords are valid.

Hackers Fire Warning Shot at Healthcare.gov (September 8, 2014)
Hackers breached security at the website of the government's health insurance marketplace, HealthCare.gov, but did not steal any personal information on consumers, Obama administration officials said.

Massively Distributed Citadel Malware Targets Middle Eastern Petrochemical Organizations (September 25, 2014)
Recently, IBM Trusteer researchers identified targeted cyber attacks on several Middle Eastern petrochemical companies. They have identified a campaign in which attackers are using a variant of the evasive Citadel malware. Citadel was originally created for the purpose of stealing money from banks and has been massively distributed on users' PCs around the world.

Your Password Laziness Makes Life So Much Easier For Russian Hackers (September 9, 2014)
A gang of Russian hackers recently stole more than 1 billion usernames and passwords, and they likely got help from an unlikely accomplice: you.

Featured Post: Seven safety tips from hackers

It's easy to get hacked. And yes, it can happen to you. Click here to read safety tips from hackers.

Visit us on Blogger!

Schneider Electric

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
September 2014 / Issue 36

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**