September 2013 / Issue 24

The Global Cyber Advisor

Invensys Critical Infrastructure & Security Practice

this issue

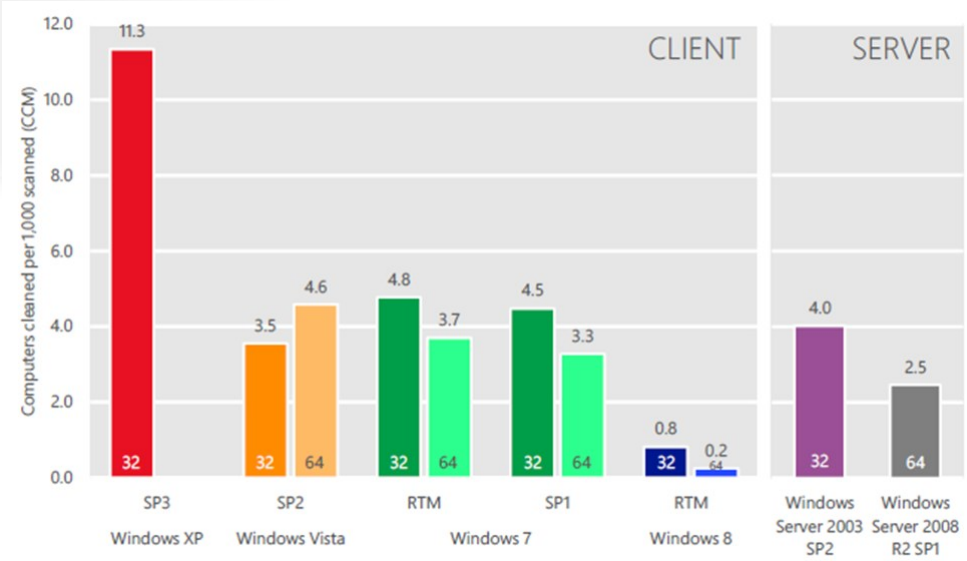
Why Upgrade Your Microsoft OS?

Windows XP Service Pack 3 (SP3) and Server 2003 will go out of support in April 2014 and July 2015 respectively. Microsoft's Support Lifecycle policy, which went into effect in 2002, provides support for Microsoft Business and Developer products for a minimum of ten years.

After April, Windows XP SP3 customers will no longer receive new security updates, non-security hotfixes, free or paid assisted support options or online technical content updates, which means that any new vulnerabilities that are discovered will not be addressed by new security updates from Microsoft.

So what is the major risk of running Windows XP and Server 2003 after their support is discontinued? For one, those who still choose to run these operating systems will be at a severe disadvantage because hackers will likely know more about the vulnerabilities and how to exploit them. And since Windows XP and Server 2003 will no longer be receiving security updates, they will basically have a "zero day" vulnerability forever. Even with anti-virus software, it will be tough to truly know whether hackers have compromised the code.

Of 1.25 billion PCs worldwide running Microsoft, one has to wonder how many are running Windows XP or Server 2003 and how many will have failed to have upgraded or stopped using it by April 2014 and July 2015. According to Microsoft, Server 2003 is 38% more likely to be infected than Server 2008 and Windows XP is 93% more likely to be infected than Windows 8, so an updated operating system is essential in preventing attacks. Just by glancing at Microsoft's chart below, one can see just how vulnerable the older operating systems have become. For more information, read *Microsoft Security Intelligence Report* vol. 13.



REF: *Microsoft SIR,* vol. 13

September 2013 Cyber Attack Statistics - Hackmageddon.com

Attack Motivations
- 49% Cyber Crime
- 35% Hacktivism
- 10% Cyber Warfare

Top 3 Attack Targets
- 26% Government
- 16% Industry
- 10% Individuals

Top 5 Attack Techniques
- 24% Unknown
- 18% DDoS
- 17% Account Hijacking
- 16% Defacement
- 9% SQL

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
September 2013 / Issue 24

Industry News

Stuxnet expert proposes new framework for ICS/SCADA security

From www.darkreading.com, 9/4/13

Critical infrastructure operators that have adopted the security industry's popular risk management mindset are doing it wrong, according to Ralph Langner. Langner, the German security expert who deciphered how Stuxnet targeted the Siemens PLCs in Iran's Natanz nuclear facility, released a proposed cyber security framework for industrial control systems (ICS) that he says is a better fit than the U.S. government's Cyber Security Framework, which is currently in draft form. The so-called Robust ICS Planning and Evaluation, or RIPE, framework takes a different approach to locking down plants, with more of a process-based approach than the risk-based NIST-led Cyber Security Framework. It all starts with these organizations establishing a "security capability," Langner says. "ICS environments are notorious for their lack of enforcing security policies, if such even exist, specifically for contractors. The bigger asset owners in critical infrastructure do have policies for staff, but not for contractors. After Stuxnet, this seems quite negligent," Langner said.

Critical infrastructure risk still high

From www.csoonline.com, 9/23/13

Cyber attacks on the nation's critical infrastructure (CI) are up—way up, particularly in the energy sector. The Department of Homeland Security's (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) reported earlier this year that there were a third more cyber incidents (111) reported by the energy sector in the six-month reporting period ending in May than in the previous 12 months (81). But so far, the power grid, transportation, water, and other control systems don't seem to be going down in any catastrophic way. And an executive order in February 2013 from President Obama calls for frameworks for the protection of CI to be implemented by February 2014. Does that mean the multiple warnings about catastrophic damage to U.S. industrial control systems (ICS) from cyber attacks are overblown?

Oil pipelines monitored for safety

From www.tulsaworld.com, 9/1/13

An array of computer monitors blinks with charts and graphs in a dark room at the south Tulsa headquarters of Explorer Pipeline. Employees are looking for even the slightest changes in pressure, outflow, anything that would indicate even the smallest discrepancy. Above the monitors on the wall is a sign: *When in doubt, shut it down.* "It's always easier to be proactive and shut down than it is to regret it later on," said Dave Ysebaert, president and CEO of Tulsa -based Explorer Pipeline. "The worst thing you can do is notice something and there was a leak and you were just pumping along and adding to it." Companies responsible for the transportation infrastructure of volatile crude and refined petroleum products take measures to protect their infrastructure and the public safety, Ysebaert said. But incidents do occur. Just this year in Oklahoma, there have been 81 incidents involving crude oil at well sites, pipelines, or other modes of transportation, according to the National Response Center database.

Energy department spends $30 million to bolster utility cyber security tools

From www.computerworld.com, 9/20/13

The Department of Energy (DOE) today awarded $30 million to 11 security vendors to develop technology the agency says will better protect the nation's electric grid, oil, and gas infrastructure from cyber attacks. The projects, which will combine power system engineering and cyber security, will include testing of the new products to demonstrate their effectiveness and interoperability, the DOE said. While the DOE's investment is welcomed, a survey of U.S. utilities in May shows what many utilities are up against. That survey, called "Electric Grid Vulnerability," said more than a dozen utilities claimed cyber attacks were daily or constant. The survey was commissioned by U.S. Democratic Representatives Edward J. Markey and Henry A. Waxman, who are members of the U.S. House Energy and Commerce Subcommittee.

Cyber News

Voluntary cyber incident reporting from the private sector better than mandatory, says report

From www.fiercegovernmanet.com, 9/24/13

Establishing voluntary mechanisms for private sector reporting of cyber security incidents is a better option than requiring mandatory reporting, concludes a Rand Corp. report commissioned by the European Parliament. Mandatory reporting might even undermine the objective of better security by setting an expectation that cyber security incidents will be treated as separate from other types of risk that critical infrastructure providers face, the report adds. The European Commission in February 2013 unveiled a proposal for network and information security that would, among other things, require operators from the energy, finance, healthcare, transport, and Internet sectors to report cyber security incidents to newly designated "competent authorities" designated at a national level.

Brute-force malware targets email and FTP servers

From www.infoworld.com, 9/20/13

A piece of malware designed to launch brute-force password-guessing attacks against websites built with popular content management systems like WordPress and Joomla is now being used to also attack email and FTP servers. The malware is known as Fort Disco and was documented in August by researchers from DDoS mitigation vendor Arbor Networks, who estimated that it had infected over 25,000 Windows computers and had been used to guess administrator account passwords on over 6,000 WordPress, Joomla, and Datalife Engine websites. Once it infects a computer, the malware periodically connects to a command and control server to retrieve instructions, which usually include a list of thousands of websites to target and a password that should be tried to access their administrator accounts.

Cyber attacks to escalate over next decade

From www.computerweekly.com, 9/24/13

Medical implants, cars, and critical infrastructure such as gas pipelines could be at risk from cyber attacks by the end of the decade. Explosive growth in the number of devices connected to the internet will open up new threats to people and infrastructure, a study backed by police and businesses claims. The study, carried out by Europol's European Cybercrime Centre, along with the International Cyber Security Protection Alliance (ICSPA—a body which brings together law enforcement organizations and technology companies—predicts a huge growth in virtual reality technologies.

Attackers sharpen skills: what that means for CISOs

From www.net-security.org, 9/24/13

In late September, IBM revealed the results of its X-Force 2013 Mid-Year Trend and Risk Report, which shows that Chief Information Security Officers (CISOs) must increase their knowledge of the evolving vulnerability and attack landscape, such as mobile and social technologies, to more effectively combat emerging security threats. For CISOs, it's no surprise that tried and true attack tactics can cause the most damage to an enterprise. Known vulnerabilities left unpatched in Web applications and server and endpoint software create opportunities for attacks to occur. These unpatched applications and software continue to be facilitators of breaches year after year. However, the latest X-Force report also recognizes that attackers are improving their skills, which allows them to increase their return on exploitation. These attackers are capitalizing on users' trust when it comes to new vectors like social media, mobile technology, and waterhole attacks.

Consultant's Corner

Transporting Data Securely

In our January 2013 newsletter, Stephen Santee gave some excellent guidance in setting up a Mobile Media program. This was followed up in February 2013 with Carrie Straka providing statistics of the dangers of malware and mobile media. However, what is a way to securely transport data and protect it in case the medium of transport is compromised? The answer is encryption. There are many types and levels of encryption available. Once the type and level of encryption are selected, there are several ways to transport your data using encryption. They include but are not limited to:

Secured Tunnel

This method is used when you have a lot of data going back and forth over an unsecured network such as the internet. It creates a private "tunnel" of information between communicating parties. This is mainly used by people that work in a home office and have a need to connect back to a corporate network.

Example Technology: Virtual Private Networking (VPN)
Possible Drawbacks: (Depending on how it is implemented) Slows down overall communication; a limited number of connections can be made

Secured Email

This method is used when you need to send secure messages over an unsecured network. This allows the entire email, including attachments, to be protected. This is commonly used to share information securely between two companies that have a non-disclosure agreement in place or between executives within the same company.

Example Technology: PGP Email Plug-in for Microsoft Outlook
Possible Drawbacks: Both parties must be using the same software and method of encryption as solutions are not standardized well

Secured Files

This method is used when protected information is contained with files. These files, once protected, can be transported by any normal means.

Example Technologies: Microsoft Document Encryption, Adobe Document Encryption, Compressed Files Encryption (zip, rar, etc.)
Possible Drawbacks: (Depending on how it is implemented) Can be easy to break in and steal information; Parties communicating must share and keep up with encryption password

Secured Transfer

This method is used when you have bursts of data to transport over an unsecured network such as the internet. It creates a private "tunnel" of information between communicating parties. This is mainly used to upload and download files on an as-needed basis.

Example Technologies: Secure copy (SCP), FTP over SSL (FTPS), SSH file transfer protocol (SFTP), FTP over SSH
Possible Drawbacks: Both parties must be using the same software and method of encryption as solutions are not standardized well.

Secured Media

This method is used when you cannot transport data over a network and it must be physically transported. The media is protected so that if it is lost, no data can be recovered without the appropriate passcode or key.

Example Technologies: IronKey, McAfee Encrypted Drive, Encrypted USB Flash Key with PIN access
Possible Drawbacks: Most solutions require software to either be installed or temporarily executed to encrypt and decrypt data; this software may not work on all platforms (ex. Windows, Linux, Mac, etc.). Other solutions that have a physical keypad overcome this limitation but require the user to remember and transport a PIN safely.

The Invensys Critical Infrastructure and Security Practice has the skills and the resources to help our clients no matter what industry. We are structured to help with the selection of appropriate encryption and transport method for all your Critical Infrastructure data needs.

This month's contributor to Consultant's Corner is
Charles Smith
Consultant, Critical Infrastructure & Security Practice, Invensys
charles.smith@invensys.com

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
September 2013 / Issue 24

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.

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, Implement 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**