May 2012 / Issue 08

The Cyber Advisor

Invensys Critical Infrastructure & Security Practice

this issue

Cyber Security—Best Practices

Cyber attacks, cyber war, and cyber bombs are the lead in for many articles these days. It is easy to get caught up in the doom and gloom if you do not know what do. The good news is there is something to do—start at the beginning with cyber security best practices. Whether you are embarking on a NERC-CIP (fossil power) or NEI 0809 (nuclear power) compliance program or just looking to strengthen your existing corporate internal polices, cyber security best practices provide a solid foundation to build from.

PEOPLE FIRST

People are unknowingly their own worst enemy in many cases. Keeping the same password for months or even years or hiding on a sticky note under their keyboard at work. A few quick changes to a company's password policy can close more than a few security holes. (1) No shared passwords: this a common practice in process automation areas. Each user must have their own unique password. (2) Use complex passwords: utilize a combination of uppercase, lowercase, and symbols. Do not use common words. (3) Change passwords frequently: this helps prevent misuse of passwords. Social media is a rapidly growing trend that has found its way into the work place. Many unsuspecting people who list where they work as part of their social profile also share many personal facts, many of which are used by hackers to gain access into a company. It may surprise you that someone's birthday or their child's name is their work password. This brings us to the next issue: training. People need to be trained not only on social media and passwords but also security issues and practices as they evolve. Just as a company has safety training, they should have security training.

LOW HANGING FRUIT

There are number of cyber security issues that many companies do not address but should. One of these is keeping automatic updates current. One of the largest malware threat vectors is Adobe. Who doesn't use Adobe? If you do not keep your Adobe product current through updates, you are leaving yourself open to malware. These automatic updates apply to operating systems, antivirus software, and other critical software and hardware that is running on your network.

THERE IS NO HOLY GRAIL

Many people like the sound of a single point solution. Unfortunately, there is no "one box does it all" cyber security product on the market. Any comprehensive cyber security solution will address a security in depth strategy. This means you cannot just deploy an antivirus product and be secure or just deploy a firewall and be secure. Cyber security compliance must address the totality of the network and uniqueness of the industry regulations that will be governing the overall acceptance.

CYBER SECURITY IS 24/7/365

Cyber security solutions are not just installed and then left to protect the network in question. Cyber security solutions are only as effective as the management systems used in conjunction with them. Virtually every aspect of a cyber security solution generates logs that must be monitored for events and actions that must be taken.

Effective cyber security is an active pursuit—not a passive pastime.

What a DDOS Attack Can Cost a Company in 2012

Survey of 1,000 IT professionals by Neustar in North America from various Industries found:

- 300 had a DDOS attack
- 35% had an attack last longer than 24hrs
- 11% had an attack last longer than 1 week
- 1 in 10 had an attack last longer than 1 week

The loss of revenues per day:

- 2/3 say $240,000 in losses
- 1/5 say $1.2MM in losses
- Financial service companies report losses up to $10,000 per hour

Industry News

Al Qaeda Video Calls for 'Electronic Jihad' *From ABCNews, 5/22/12*

Al Qaeda may be turning its destructive attention to cyber warfare against the United States. In a chilling video, an al Qaeda operative calls for "electronic jihad" against the United States and compares vulnerabilities in vital American computer networks to the flaws in aviation security before the 9/11 attack. The al Qaeda video calls upon the "covert mujahidin" to launch cyber attacks against the U.S. networks of both government and critical infrastructure, including the electric grid. The video was obtained by the FBI last year and released today by the Senate Committee on Homeland Security and Governmental Affairs. "This is the clearest evidence we've seen that al Qaeda and other terrorist groups want to attack the cyber systems of our critical infrastructure," Homeland Security and Governmental Affairs Committee Chairman Joe Lieberman, I-Conn., said in a statement. "It's clear that al Qaeda is exploring all means to do us harm and this is evidence that our critical infrastructure is a target." Increasing evidence also suggests that Iran is looking to commit cyber attacks against the United States, according to testimony last month before the House Committee on Homeland Security. Iran's sponsorship of terrorist groups takes on a new dimension in cyberspace, where it could develop a powerful cyber weapon and pass it on to a terrorist group. The Homeland Security Committee says the DHS received more than 50,000 reports of cyber intrusions or attempted intrusions since October, an increase of 10,000 reports over the same period the previous year.

Cyber Attacks on Pipelines linked to China *From HackerNews, 5/16/12*

The spear-phishing attacks laying siege to networks in the natural gas pipeline industry apparently are being carried out by the same group that hacked RSA security last year. The attacks, which have been occurring since this past March, have targeted several of the country's natural gas pipeline companies. According to U.S. officials, it's unclear if a foreign power is trying to map the gas systems or if hackers are attempting to harm the pipelines. A previous attack on the oil and gas sector seemed to originate in China. DHS officials and a spokesman have acknowledged they are working with the FBI to find out who may be behind the intrusions and malicious emails. The Monitor reports that some investigators now believe that the campaign is tied to another attack last year against cyber security company RSA, which the head of the National Security Agency told Congress could be traced back to China. The group responsible for the RSA attacks has also been linked to several previous hacking incidents around the globe. The oil and gas sector has been targeted before. In February 2011 the computer security firm McAfee discovered a computer intrusion labeled "Night Dragon" that was traced to China. As part of that attack, individuals tried to obtain sensitive data and financial documents from the oil and gas companies about bids and future drilling exploration projects.

DHS To Critical Infrastructure Owners: Hold On to Data After Cyber Attack *From ThreatPost, 5/29//12*

The Department of Homeland Security is offering organizations that use industrial control systems advice on mitigating the effects of cyber attacks. Among the agency's recommendations: hold on to data from infected systems and prevent enemies from moving within your organization. DHS's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) published a technical paper on cyber intrusion mitigation strategies on Friday. The document calls on critical infrastructure owners to take a number of steps to thwart attacks or limit the damage they cause among them: improving their ability to collect and retain forensic data, and to detect attempts by attackers to move laterally within their organization. The document, a Technical Information Paper - or TIP, is merely guidance from ICS-CERT to critical infrastructure owners and is targeted at both enterprise and control system networks, DHS said. The agency is responding to a rising drum beat of news about vulnerabilities in SCADA and ICS software and attacks on industrial control systems (ICS) and SCADA systems in the U.S. and abroad. In recent weeks, the agency has warned of cyber threats to organizations that operate gas distribution pipelines.

The Cyber Advisor
Invensys Critical Infrastructure & Security Practice
May 2012 / Issue 08

Cyber News

Researchers identify Stuxnet-like malware called 'Flame'

From Computerworld, 5/28/12

A new, highly sophisticated malware threat that was predominantly used in cyber espionage attacks against targets in the Middle East has been identified and analyzed by researchers from several security companies and organizations. According to the Iranian Computer Emergency Response Team (MAHER), the new piece of malware is called Flame and might be responsible for recent data loss incidents in Iran. There are also reasons to believe that the malware is related to the Stuxnet and Duqu cyber espionage threats, the organization said on Monday. Malware researchers from antivirus firm Kaspersky Lab have also analyzed the malware and found that while it is similar to Stuxnet and Duqu in terms of the geographic propagation and targeting, it has different features and it is, in many ways, more complex than both of those threats. Flame, as the Kaspersky researchers call it, is a very large attack toolkit with many individual modules. It can perform a variety of malicious actions, most of which are related to data theft and cyber espionage. Among other things, it can use a computer's microphone to record conversations, take screenshots of particular applications when in use, record keystrokes, sniff network traffic, and communicate with nearby Bluetooth devices. Flame is much bigger than both Duqu and Stuxnet, which at around 500KB in size were already considered large by security experts. The size of all Flame components combined adds up to over 20MB and one file in particular measures over 6MB alone, Kamluk said. Another interesting aspect of the threat is that some parts of Flame were written in LUA, a programming language that's highly uncommon for malware development.

LUA is often used in the computer gaming industry, but Kaspersky Lab hasn't seen any malware samples before Flame that were written in the language, Kamluk said. Flame spreads to other computers by copying itself to portable USB devices and also by exploiting a now-patched Microsoft Windows printer vulnerability that was also leveraged by Stuxnet.

Spy malware infecting Iranian networks is engineering marvel to behold

From arsTechnica.com, 5/29/12

Malware recently found infecting Middle Eastern networks is so complex and sophisticated that it's probably an advanced cyber-weapon unleashed by a wealthy country to wage a protracted espionage campaign on Iran, researchers from some of the world's leading security companies said. The malware, dubbed "Flame" after one of the dozens of modules available for it, immediately evoked memories of Stuxnet, another piece of advanced malware that disabled uranium centrifuges in Iranian nuclear plants. As sophisticated as Stuxnet and a related piece of espionage software known as Duqu, the latest piece of malware is probably orders of magnitude more sophisticated. When fully installed, its size is a whopping 20MB, and it also uses SQLite databases and dynamically generated code that uses the Lua programming language. Such characteristics suggest the malware, which Kaspersky estimates has been found on about 1,000 computer systems so far, could only have been written by a large team of highly skilled software engineers.

Hacker Group Comes Out of Nowhere to Launch Attacks Against Government Networks

From SecurityWeek.com, 5/4/12

"**The Unknowns**" is gaining attention for a string of attacks against government and private networks, which started back in March. However, there are questions as to whether their recent actions could lead to their downfall. The Unknowns, as the group refers to themselves, entered the public's eye a few weeks ago, and since then they have claimed credit for attacks against Oak Ridge National Labs, NASA, the European Space Agency, the French Ministry of Defense, the U.S. Air Force, Harvard, Bahrain's Ministry of Defense, a French radio station, and the Jordanian Yellow Pages.

Hospital agrees to pay $750,000 over data breech allegation

From SCMagazine.com, 5/25/12

A Massachusetts hospital has agreed to settle in court to the sum of $750,000 over allegations concerning its failure to protect sensitive patient data. According to a statement released by the Massachusetts Attorney General's (AG) office, a consent judgment approved in Suffolk Superior Court involving South Shore Hospital includes a $250,000 civil penalty and a payment of $225,000 to be used to create awareness concerning data security.

Consultant's Corner

Passwords: a weak link in the chain

The other day, I was reading an article by a reformed hacker who was telling his secrets for "gaining access" to company networks. Much to my surprise, and I will assume yours, he focused on passwords. Here was his recipe, plus a little social research thanks to Facebook:

1. Your partner, child, or pet's name, possibly followed by a 0 or 1
2. The last 4 digits of your social security number
3. 123 or 1234 or 123456
4. "password"
5. Your city, or college, football team name
6. Date of birth – yours, your partner's or your child's
7. "god"
8. "letmein"
9. "money"
10. "love"

Believe it or not, this person claims a 20% success rate. I am sure some of you already see your own password in the list. This got me thinking—with all the money being spent by corporations on sophisticated hardware and software, just how much attention is being paid to the selection of passwords that are entrusted to us?

The solution to this dilemma is twofold; first, knowledge of why I need such long passwords, and secondly, discipline to change them and to change them frequently.

What many people do not understand is the impact that password length has on security. Add to that mix all characters—alphanumeric, special characters, and upper and lower case letters. You have just exponentially increased the difficulty to hack your password. Adding just one capital letter and one asterisk would change the processing time for an 8 character password from 2.4 days to 2.1 centuries—that is a huge improvement.

These are my top 10 tips for passwords.

1. Follow your network administrator's guidelines on changing your passwords!
2. When given the choice on length of password, always opt for the longer password string.
3. Do not choose passwords that are common to you or a reflection of who you are, as they are easy to guess. But do create passwords that you can remember.
4. Do not write your password down on a sticky note and put it behind your monitor or under your keyboard.
5. Randomly substitute numbers and characters for letters, like the letter *o* for zero (*0*).
6. Randomly substitute special characters for letters or numbers, like @ for the letter *a*.
7. Change default passwords that come on every device. These passwords are published on the internet.
8. Use the Microsoft password strength checker at https://www.microsoft.com/en-gb/security/pc-security/password-checker.aspx.
9. Use common sense; if a contract crew has been working in the area, change your passwords.
10. Change your passwords frequently.

This months contributor to Consultant's Corner is
Tom Jackson
Principal, Critical Infrastructure & Security Practice
Invensys
Tom.Jackson@Invensys.com

Consultant's Corner

Tim Johnson, CISSP —CISP Principal Consultant

"Centralized Anti-Virus DAT repository deployments enable quick and reliable Anti-Virus updates for Stand Alone Control Systems."

Doug Clifton, CISSP — Dir. CISP

"It's significantly less expensive to purchase Managed Security Services than to hire new staff with Security Experience."

Steve Batson, CISSP — CISP Principal Consultant

"Implementing common security controls across disparate systems can greatly reduce the cost of security and maintenance."

Michael Martinez — CISP Principal Consultant

"Being regulatory compliant does not ensure being secure. Cyber Security is a ongoing life cycle."

Tom Jackson — CISP Principal Consultant

"According to Kaspersky Labs, applications like Adobe are primary targets for hackers to deliver viruses. Implementing patch management and update services is an effective fix."

Meet the CISP team and learn more about Cyber Security at http://www.real-time-answers.com/cyber-security/

Cyber Security for the Nuclear Industry »
Focusing on 10 CFR 73.54 and NEI 08-09 Reg. guide 5.71, learn more about cyber security in the nuclear industry.

Cyber Security for Power Generation »
As more and more electric power plants begin their NERC CIP compliance plan, many are left trying to understand where to start. See which areas require special attention.

Cyber Security Compliance »
Cyber compliant does not necessarily mean cyber secure. Identify the keys common to both.

Cyber Security Threats »
Cyber attacks are increasing. A continuous state of preparedness is required.

Cyber Security Life Cycle »
Cyber security cannot be maintained from a one-time initiative. Learn about a methodology designed to keep your site cyber secure well into the future.

Cyber Security Consulting Advantage »
Security and compliance take a tremendous amount of effort. Help is available to get secure and compliant … and stay that way.

The Cyber Advisor
Invensys Critical Infrastructure & Security Practice
May 2012 / Issue 08

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**