October 2012 / Issue 13

The Cyber Advisor

Invensys Critical Infrastructure & Security Practice

this issue

Social Networking or Social Engineering

Social networking is widely accepted by companies today, with an average of over 80% of U.S. businesses using one or more of the numerous social media sites available (Business Courier 6/21/12) to market their business or transact commerce. According to Symantec's Cybercrime report, cyber criminals have shifted their focus to social networks. Some of the shift can be explained by the lack of security policies most companies have on social networking, unlike network security and website security that is typically managed internally. Security for social networking sites is left up to the social media provider and the person who controls the account for the company or holds the username and password. But what are the real ramifications of a social network security breach to your ICS?

The rapid growth and acceptance of social networking has introduced a new security vector to understand and address. Cyber criminals want the password, and with that information they can not only cause your company irrefutable damage on its social networking sites but also gain access to passwords and usernames that can be used to find system vulnerabilities and gain access to your ICS. Social network attacks are not just limited to bad press; these are cyber attacks and must be identified and treated as such.

Phishing is sending emails in the attempt to acquire information such as usernames, passwords, or other specific information. For example, a cyber criminal sends an email that says, "Send us your username and password to reset your account." It may even appear to come from the correct company or your IT department.

Social Engineering, in the context of security, is the art of manipulating people into performing actions or divulging confidential information. Similar to the above scenario, except now the cyber criminal calls your company after obtaining a phone number or working their way around the switchboard. They claim to be the IT department and have your name and other information from a social network site, and ask for your password and username to reset accounts due to maintenance.

The best prevention for Social Networking cyber crimes is putting in place policies and procedures like the ones below:

- Social media guidelines on site access and who controls usernames and passwords
- Education on cyber security, focusing on social networking and other key topics
- Password change management best practices

An ounce of prevention is worth avoiding the hours spent working on the cure!

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

Attack Motivations
- 57% Cyber Crime
- 35% Hacktivism
- 5% Cyber Warfare
- 2.5% Cyber Espionage

Top 3 Attack Targets
- 30% Government
- 33% Industry
- 10% Education

Top 5 Attack Techniques
- 25% DDoS
- 25% Unknown
- 22% SQL
- 10% Defacement
- 5% Targeted Attacks

Industry News

Next generation cyber attacks target oil and gas SCADA

Pipeline & Gas Journal, 10/2012

Anyone working with SCADA or industrial control systems (ICS) in the oil and gas industry is aware of the pressure to increase productivity and reduce costs through network integration. For example, sharing real-time data from field operations with management is standard practice for most companies. Similarly, the demand for remote support has made many pipeline control systems accessible via Internet-based technologies. These new technologies are enabling companies to implement agile, cost effective business practices. Unfortunately, they also come at a cost—many of the same security vulnerabilities that have plagued business systems now appear in SCADA systems. Pipeline control systems are now exposed to cyber security threats they were never designed for.

Gulf oil industry at risk of cyber attack

FT.com, 10/23/2012

Rising regional political tensions and a flurry of recent cyber attacks have raised fears about the growing use of viruses to target critical national infrastructure in the Middle East. Working with governments and authorities, Kaspersky is aiming to develop a new, industrial-scale operating system with security embedded in the hardware, rather than using security envelopes to protect the systems. Gulf governments are becoming increasingly attuned to the issue of cyber security as the threats proliferate. The United Arab Emirates in September announced the creation of a new agency, the National Security Authority, to implement a national plan to ward off threats to online security.

Electric industry cyber security

ELP.com, 10/2012

Securing electric utility control systems maintains a utility's mission to produce and/or deliver electricity reliably and safely. It is impossible to secure control systems fully; however, these systems can be made more secure to minimize unintentional incidents and "less than nation-state" cyber attacks that could cost hundreds of millions of dollars and lives. The premise for grid reliability is the N-1 criteria, which describes the impact if one element in the system fails or becomes out of service. It is meant to address mechanical or electric failures of equipment or facilities. The N-1 criteria, however, does not address acts of nature, malicious incidents or common cause failures that could affect multiple facilities. Cyber security is a common cause failure that can affect facilities across large geographic areas and can be more severe than acts of nature. Consequently, neighboring utilities might be unable to help because they could be affected, too. In addition, a major cyber attack could affect enough equipment that there would not be adequate replacements, meaning long-term outages from nine to 18 months.

DHS, Energy Dept schedule briefings on cyber attacks

naylornetwork.com, 10/11/2012

Yesterday, the Department of Homeland Security and the Department of Energy released a schedule of classified and unclassified briefings, starting Oct. 17, on the latest cyber attacks targeting energy infrastructure around the world. The DHS Industrial Control Systems Cyber Emergency Response Team, in coordination with DOE, the Transportation Security Administration, and other federal and private sector partners, "has been tracking threats and responding to intrusions into U.S. oil and natural gas, pipeline and electric power organizations at an alarming rate."

Weak cyber security at EPA, says auditors

FierceGovernment.com, 10/18/2012

The Environmental Protection Agency office of inspector general faults the agency for weak network security practices. Auditors say EPA cyber security staff haven't confirmed that corrective actions have been taken to address known weaknesses. Plans of action and milestones "were either not created or were not created until [the] audit was underway."

Cyber News

MiniFlame: Researchers say "extremely targeted" cyber attack hit Lebanon, Iran

abcNews.go.com, 10/15/2012

Researchers said they have identified part of the powerful Flame cyber espionage program as a stand alone, "highly flexible" spy program that centered its attacks on computer systems in Lebanon and Iran. MiniFlame, as cyber experts at Moscow-based Kaspersky Labs dubbed the malware, is an "info stealing" virus designed to hit only a few high-profile targets—perhaps just a few dozen computer systems. Kaspersky researchers said in a blog post they actually discovered MiniFlame in July but at the time believed it to be just a module within Flame. The larger Flame virus was described by researchers as the most sophisticated cyber espionage program ever discovered and was a veritable "tool kit" for cyber spying programs. It could remotely take screenshots of infected computers, record audio conversations that took place in the same room as the computer, intercept keyboard inputs and wipe data on command. Researchers said that the malware infected thousand of computers, mostly in Iran.

Cyber attacks escalate around the globe

NPR.org, 10/16/2012

U.S. officials now believe Iran was responsible for a series of cyber attacks on American banks in September and on major energy firms in Saudi Arabia and Qatar. David Sanger, chief Washington correspondent for The New York Times, talks about the escalating tactics of cyber warfare. Last month, customers of Bank of America, JP Morgan Chase, Wells Fargo, and several other banks were unable to access their bank accounts. Hackers overwhelmed the sites with traffic that made them extremely slow or totally unresponsive. No funds were lost, but it was a nuisance. Months earlier in Saudi Arabia, a virus named Shamoon spread through 30,000 of the computers of Aramco, the world's largest oil company, and erased file after file. Cyber war isn't fiction, it's underway. The U.S. and Israel reportedly launched attacks that set back Iran's nuclear program by a year or maybe more. U.S. officials believe Iran's cyber warfare unit tested U.S. banks last month and the Saudi computers last summer, and last week Defense Secretary Leon Panetta warned of a cyber-Pearl Harbor.

Iran renews Internet attacks on U.S. banks

WSJ.com, 10/16/2012

Iranian hackers renewed a campaign of cyber attacks against U.S. banks this week, targeting Capital One Financial Corp. and BB&T Corp. and openly defying U.S. warnings to halt, U.S. officials and others involved in the investigation into the attacks said. The attacks, which disrupted the banks' websites, showed the ability of the Iranian group to sustain its cyber assault on the nation's largest banks for a fifth week, even as it announced its plans to attack in advance. U.S. officials said the attacks against banks and others against Middle Eastern energy companies were sponsored by the Iranian government and approved at high levels as part of a low-grade cyber war that officials warned could lead to retaliation.

White House confirms "spearphishing" intrusion

News.cnet.com, 10/1/2012

Officials confirmed a report by veteran Pentagon reporter Bill Gertz saying hackers linked to China's government "broke into one of the U.S. government's most sensitive computer networks." The White House has confirmed that one of its internal computer networks—reportedly a military office in charge of the president's communications—had been targeted in a successful "spearphishing" attack. An article published by the conservative FreeBeacon.com Web site said that hackers with ties to China's government had recently breached an unclassified "system used by the White House Military Office for nuclear commands," including the so-called nuclear football.

Consultant's Corner

Staying Ahead of the Curve with Nuclear Cyber Security

U.S. Nuclear Plants have stepped up to the plate and are actively implementing cyber security controls to combat cyber threats. When it comes to cyber security, key areas of focus have been collaboration, leveraging existing programs, standardization, and resource management.

The nuclear industry provides a great collaborative effort through Nuclear Energy Institute (NEI). NEI has several different working groups that allow utilities and vendors to collaborate and approach cyber security systematically and efficiently. Invensys stays intimately involved in NEI and many other key organizations providing useful working groups and sites that provide cyber security guidance.

One area the nuclear industry that saves thousands of man hours is in the efficient performance of cyber security assessments. Sophisticated database tools, like Wiznucleus Cyberwiz-Pro and Lumension Risk Manager, make the assessment process manageable. These tools come pre-loaded with regulatory requirements, interfaces with existing site databases, allow security control responses to be applied to multiple CDAs at once, and provide an efficient process for managing and maintaining cyber security assessments. Implementation of common controls across groups of CDAs can leverage existing programs and greatly reduce the time required to assess the implementation of security controls.

Standardizing and centralizing security solutions implemented across multiple platforms can also increase efficiency. Centralized patching, backups, and signature updates greatly reduce the time and effort required to update systems. Centralized log management (Security Information and Event Management) and intrusion detection system functions also improve efficiency and effectiveness. While it is essential to maintain defense-in-depth, minimizing the number of different types of security controls implemented reduces the cost and complexity to maintain cyber security controls on systems. Consider standardizing the type of language incorporated into procurement contracts to help standardize the security control products purchased.

Developing an effective and maintainable incident response program is another area of focus for establishing efficient use of resources. A comprehensive process, procedure, and knowledgeable set of stakeholders are needed to appropriately respond to an incident. Stakeholders will include maintenance, security, management, ops, engineering, and an expert in incident response. Most plants do not want to invest in keeping staff resources trained in forensic analysis and the use of the tools needed to investigate an incident. This is an area where an external expert can be a more efficient use of resources. It also helps to have someone who can lead an incident response team that is dealing with incident response on a regular basis.

These are just a few tips that can allow nuclear plants to stay ahead of the curve and implement cyber security in an efficient manner. By using online resources and guidance documents, participating in working groups, using effective assessment tools, developing common controls, standardizing security controls and procurement language, implementing centralized log management, and establishing effective incident response procedures, nuclear plants are reducing the amount of cost, effort, and resources needed to implement their cyber security plans.

This months contributor to Consultant's Corner is
Steve Batson, CISSP
Principal, Consultant, Critical Infrastructure & Security Practice
Invensys
stephen.batson@invensys.com

The Cyber Advisor
Invensys Critical Infrastructure & Security Practice
October 2012 / Issue 13

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.

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.

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 help them understand the demands of Control 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 Assessment, Development, Implementation, and Management.

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**