May 2013 / Issue 20

The Global Cyber Advisor

Invensys Critical Infrastructure & Security Practice

this issue

CFATS and Cyber Security

Critical infrastructure and cyber security go hand-in-hand these days. There is a plethora of regulatory acronyms from the various government agencies that oversee them. Federal Energy Regulatory Commission (FERC) has their agency, the North American Electric Reliability Corp (NERC), which oversees cyber security standards for the power generation sector, Critical Infrastructure Protection (CIP), and is commonly referred to as NERC-CIP. The Nuclear Regulatory Commission (NRC) has their body of cyber security standards overseen by the Nuclear Energy Institute (NEI), the current version being NEI 08-09.

Yet there is one other government agency, the Department of Homeland Security (DHS). The DHS has identified 16 industrial sectors as "Critical Infrastructure," which they define as *"…the backbone of our nation's economy, security and health. We know it as the power we use in our homes, the water we drink, the transportation that moves us, and the communication systems we rely on to stay in touch with friends and family. Critical infrastructure are the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."*

One of these defined industries is the Chemical sector. The DHS has developed the Chemical Facility Anti-Terrorism Standard, more commonly referred to as CFATS, to provide security guidance. The initial CFATS regulations, which currently cover over 6,000 operations, came into effect on June 8, 2007 and have slowly morphed into a larger and more comprehensive body of work that now includes cyber security. To lead this effort, the National Cyber Security Division (NCSD) of the DHS established the Control Systems Security Program (CSSP). The goal of the CSSP is to reduce the cyber threat to industrial control systems by coordinating the efforts of stakeholders in government and private industry. These elements draw heavily from the NIST and ISO security standards and initially are focusing on a "best practice" approach. DHS defines cyber security as "the electronic protection of critical cyber assets: systems and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of mission-critical services."

Cyber security measures include

- Strategy
- Information classification and role-based access
- Defense-in-depth: layering of security zones
- Risk assessments
- Vulnerability mitigation
- System/disaster recovery
- Performance measurement implementation

The cyber realm is incredibly dynamic, with threats and technology constantly changing, forcing the evolution of standards like CFATS and once again highlighting the need for comprehensive security programs.

May 2013
Cyber Attack Statistics
- Hackmageddon.com

Attack Motivations
- 56% Hacktivism
- 43% Cyber Crime
- 1% Cyber Espionage

Top 3 Attack Targets
- 32% Finance
- 14% Industry
- 11% Government

Top 5 Attack Techniques
- 35% DDoS
- 18% Unknown
- 14% SQL
- 13% Account Hijacking
- 5% DNS Hijacking

Industry News

Power company targeted by 10,000 cyber attacks per month

arstechnica.com, 5/22/2013

A congressional survey of utility companies has revealed that the country's electric grid faces constant assault from hackers, with one power company reporting a whopping 10,000 attempted cyber attacks per month. US Reps. Edward Markey (D MA) and Henry Waxman (D-CA) sent 15 questions to more than 150 utilities and received replies from 112 of them. Only 53 of those actually answered all the questions—the others provided incomplete responses or only "a few paragraphs containing non-specific information" without answering any of the questions. The electric grid is the target of numerous and daily cyber attacks.

- More than a dozen utilities reported "daily," "constant," or "frequent" attempted cyber attacks ranging from phishing to malware infection to unfriendly probes.
- One utility reported that it was the target of approximately 10,000 attempted cyber attacks each month.
- More than one public power provider reported being under a "constant state of 'attack' from malware and entities seeking to gain access to internal systems."
- A Northeastern power provider said that it was "under constant cyber attack from cyber criminals including malware and the general threat from the Internet."
- A Midwestern power provider said that it was "subject to ongoing malicious cyber and physical activity" and that they saw probes on their network looking for vulnerabilities in their systems and applications on a daily basis. "Much of this activity is automated and dynamic in nature—able to adapt to what is discovered during its probing process."

U.S. power companies under frequent cyber attacks

www.computerworld.com, 5/21/2013

A survey of U.S. utilities shows many are facing frequent cyber attacks that could threaten a highly interdependent power grid supplying more than 300 million people, according to a congressional report. More than a dozen utilities said cyber attacks were daily or constant, according to the survey, commissioned by U.S. Democratic Representatives Edward J. Markey and Henry A. Waxman. The 35-page report on the survey, called "Electric Grid Vulnerability," was released on Tuesday. The report is in response to widespread concerns that hackers could damage parts of the U.S. power grid, causing widespread outages and prolonged economic effects.

CFATS Fact Sheet Update

chemical-facility-security-news.blogspot.com, 5/8/2013

The DHS Infrastructure Security Compliance Division (ISCD) published a new version of their CFATS Fact Sheet with up-to-date inspection information on the Critical Infrastructure: Chemical Security web page. It is the April version of the fact sheet, but the following numbers have changed (April numbers and change in numbers in parentheses):

- 44,000 (same) preliminary assessments were reviewed by DHS from facilities with chemicals of interest
- 4,351 (4,382; - 31) facilities are currently covered by CFATS
- Over 3,000 (2,900; +100) facilities voluntarily removed, reduced, or modified their holdings of chemicals of interest
- 1,242 (1,202; +40) visits to assist facilities with CFATS compliance
- 380 (280; +100) Security Plans authorized
- 85 (53; +32) Security Plans approved following an on-site inspection

Iran fingered for attacks on U.S. power grid

www.theregister.co.uk, 5/27/2013

Iranian hackers are launching state sanctioned attacks on U.S. energy firms and hope to sabotage critical infrastructure by targeting industrial control systems, according to American officials. The attacks on oil, gas, and power firms have so far concentrated on accruing information on how their systems work – a likely first step in a coordinated campaign that would eventually result in attacks aimed at disrupting or destroying such infrastructure. The prospect of such attacks has senior American officials more worried than the espionage-related incursions which Chinese state sponsored attackers have been blamed for, according to the Wall Street Journal. "This is representative of stepped-up cyber activity by the Iranian regime. The more they do this, the more our concerns grow."

Cyber News

ICS cyber security is still not understood by the IT community—and it is hurting critical infrastructure

community.controlglobal.com, 5/20/2013

Cheri McGuire, Symantec's Vice President of Global Government Affairs and Cyber Security Policy testified to the Senate Judiciary Subcommittee on a Crime and Terrorism hearing. She stated: "In my testimony today, I will provide the Subcommittee with our latest analysis of the threat landscape as detailed in the just-released Symantec Internet Security Threat Report (ISTR), Volume 18. Last year, we saw a significant increase in targeted attacks—up 42 percent from 2011, and it is almost certain that this trend will continue in the coming years.

Only 36% of small firms apply security patches. No wonder cyber crooks are stealing from them

nakedsecurity.sophos.com, 5/24/2013

Small businesses are under constant attack from malware, scams, and online fraud. They are not only losing money directly to fraud, but also in costs associated with maintaining security. Small businesses are simply woefully under-prepared to keep their assets safe. Despite reorganization and redirected priorities, the police can still do little to help. On the plus side, 49% of businesses suffered no fraud losses at all, and only around 7% lost more than £5000. 10% reported incidents of card fraud, including "card not present" problems associated with online trading. Such issues, along with the costs and complexity of PCI-DSS compliance, have apparently discouraged many businesses from operating online at all. 20% report "virus" infections, with a further 8% spotting hacking or other "electronic intrusion," and that's only those that knew about the issues—73% claimed they had had no problems.

APT1 is back, attacks many of the initial U.S. corporate targets

www.net-securityweek.orf, 5/21/2013

In a report that the cyber security firm published in February and that tied the group to Unit 61398 of the People's Liberation Army, they expressed the belief that the group will simply change their attack techniques and continue to do what they did best: compromising business systems of (mostly) U.S. companies and stealing intellectual property.

Most attacks are external, but never underestimate the insider threat

www.securityweek.com, 5/1/2013

Earlier this month, U.S. Army MP William Millay was sentenced to 16 years in prison for attempting to sell classified military information to the Russians, according to a story posted on the Federal Bureau of Investigation website this week. Millay wasn't motivated by any political or moral outrage; he was willing to sell secret defense documents just for the money, the FBI said. "This case really drives home the point that the insider threat is alive and well," Special Agent Sam Johnson, the supervisor in charge of the national security squad in Anchorage, Alaska, said in the FBI post. In 2011, Millay began talking to and soliciting help from other military personnel regarding selling classified defense information to the Russians. Many of the people he talked to didn't take him seriously, but some realized he was serious, special agent Derrick Criswell said in the story. "No one came forward to report his activity," Criswell said.

71 percent of applications use components with severe or critical security flaws

www.securityweek.com, 5/1/2013

A significant portion of software is assembled using open source components and frameworks downloaded from public repositories, according to a software development survey. At least 80 percent of modern software being developed can be traced back to open source components and publicly available frameworks, Sonatype said in its annual Open Source Development Survey released Tuesday. Around 76 percent of respondents in the survey said they have no control over what components get used in software development projects.

Consultant's Corner

Minimize Downtime Through Effective Backups

Modern organizations put more and more emphasis on using computer solutions for day-to-day problems. Whether it is payroll, operating door controllers, or controlling turbine assemblies, all these systems rely on computer systems that have been configured to work in their specific environment. Because of these configuration differences, replacing one of these systems in the event of a failure is not as simple as buying a new one off the shelf. Reproducing a configuration of a system without good backups can take huge amounts of time, and also introduce errors into the system that were not originally there. In some cases, the time lost while these systems are being replaced can shut down a production line or power plant for extended periods of time, costing companies millions of dollars. All of these reasons and more are why effective backups are important for any computer system in an industrial environment.

Keep it simple

The first requirement for effective backups is to make them as simple as possible to execute. If the backup procedure for a system requires a technician to go to the machine, plug in a laptop, and manually execute a backup that takes 4 hours to complete, this not only wastes time, but could lead to human errors while performing the backup activities. There are many software suites available now that will automatically perform backups of other systems, either locally or to network drives, and are highly customizable in how these backups are performed. Using one of these software suites to automate the backup process can make them easier and more reliable.

Determine the frequency and types of backups to occur

The second requirement for effective backups is to identify what frequency backups need to occur at and what types of backups need to occur. To evaluate how often backups need to occur, you must first know how often changes are occurring on a system. A controller for an emergency fire protection system may not be used often, and backups every month or every quarter is sufficient; however, for a payroll system that is being changed on a daily basis, incremental backups every day would be more appropriate. Determining the frequency of backups will assure that backups are current and usable, but keep resource usage at a minimum and keep costs down.

Store backup files offsite

The third requirement for effective backups is to have offsite storage locations for the backup files. If a company has up-to-date backups, but they are all in the same building as the servers when a flood or fire occurs, they are of no use. Because most backup software solutions allow network backups, consider other locations on the company's WAN that can house the backups more safely. Storing backups at a corporate location that is offsite from your industrial complex can save a company when large scale disasters strike, such as flood and fire.

Use a test system to ensure smooth recovery

Finally, once a company has backups created for their systems, they must test that they can actually recover from these backups. Using a test system to attempt and recover from these backups can ensure that when the time comes to use system backups, it goes smoothly. Creating and testing a disaster recovery plan can help make recovery as smooth and painless as possible, and with the help of good backups, can prevent extended downtime to a company's critical infrastructure.

This month's contributor to Consultant's Corner is
Gary Kneeland
Consultant, Critical Infrastructure & Security Practice, Invensys
gary.kneeland@invensys.com

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
May 2013 / Issue 20

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.

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.

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**