The Global Cyber Advisor

by the Cyber Security Services Group

Schneider Electric

March 2015
Volume 42

this issue

N Korea denies hacking nuclear plants in S Korea (APAC)

From www.outlookindia.com, 3/26/2015

North Korea denied involvement in cyber attacks on South Korea's nuclear power plant operator, accusing Seoul of fabricating a story to shift the blame for high cross-border tensions. Last December hackers published designs, manuals and other information about South Korean reactors on Twitter, along with personal information about workers at their operating company. The leaks prompted the South to heighten cyber security and launch an investigation involving experts, government officials and state prosecutors. Pyongyang's state Internet research institute insisted North Korea had never been involved in any cyber attacks on the South.

The Difference Between Compliance and Cyber Security

Trying to understand the difference between compliance solutions and cyber security solutions can be very confusing. Every discussion on cyber security is interlaced with compliance elements and cyber security solution features, which is compounded by the number of standards on the topics that primarily address compliance, so it is no wonder that many people confuse cyber security compliance with being cyber secure. Cyber security compliance, while complementary to cyber security solutions, is not the same as being cyber secure.

So, what is compliance? Compliance is defined by the laws, regulations, and governing bodies. These standards generally contain a list of requirements that must be met in order to declare the user as compliant. Further, being compliant requires the processes, tools, and organizations to sustain the program in a manner that can be audited. Basically, you must be able to display the actions and evidence required to show that you meet the requirements.

Any comprehensive cyber security initiative begins with a compliance assessment program and is monitored throughout its lifecycle. When executed properly, the outcome of the compliance program is the remediation checkpoints that drive the cyber security solutions.

The compliance process provides an overview of gaps, risks, and statuses as set forth by the regulation used (i.e. NERC CIP, NEI 08-09). This information is used to define assets that will need to be secured within the infrastructure and the extent of the security controls that must be applied. The deployment of the required security controls should always adhere to cyber security best practices.

Just because you are compliant to a cyber security standard or regulation doesn't mean you are 100% cyber secure. True security is a comprehensive program of compliance, cyber security solutions, and an organizational awareness of the risks and benefits of the technologies deployed in our modern industrial control systems.

Cyber Security Services by Schneider Electric

March 2015 / Volume 42

Cyber Central

How We Do It: Cyber Security Lifecycle Methodology

Part 2 of 4

Last month, we introduced our Cyber Security Lifecycle Methodology, focusing on Stage 1, the assessment.

Stage 1: Assess

CISP works with the customer to assess their current network to help identify problems and develop requirements.

This month we will look at Stage 2, the Development phase.

Stage 2: Develop

After the Assessment phase is completed, the next stage is the development phase. As the name implies, the Cyber Security Services team uses the assessment and the customer's requirements to develop a program unique to their needs. Prior to jumping right into network designs, it is important to develop a program that addresses not just the technology but also the timing. Our typical client does not always have the necessary downtime to implement all the changes that are required. In these cases, we can work with clients on a technology roadmap to the defined solution priority based on time windows. We understand the nature of our clients' industries and that "rebooting" the network is not always an option.

With project timing addressed, we can move onto network design. Here, we defer to our clients' preferences for hardware (switches, firewalls, etc.) and software (anti-virus, malware prevention, etc.). In situations where the client does not have a preferred vendor, we recommend one of the "best-in-class" vendors we typically work with. The conclusion of the Development stage is a truly comprehensive cyber security solution that addresses not just the client's unique needs but also their timeline as well as internal corporate mandates, such as preferred vendors.

Next month, we will discuss Stage 3: Implement.

Schneider Electric

The Global Cyber Advisor
Cyber Security Services
March 2015 / Volume 42

Industry News

More data from South Korea nuclear power operator leaked (APAC)

From www.reuters.com, 3/12/3015

A hacker believed to be behind cyber attacks on South Korea's sole nuclear power plant operator released more files, but a company official said the data was not believed to have been newly stolen but from previous hacking. Korea Hydro & Nuclear Power, part of state-run utility Korea Electric Power Corp, said in December its computer systems had been hacked but only non-critical data had been stolen and operations were not at risk. The hacker had at that time demanded the shutdown of three reactors threatening, in Twitter messages, "destruction" if not.

US industrial control systems attacked 245 times in 12 months (NA)

From www.pandct.com, 3/19/2015

US industrial control systems were hit by cyber attacks at least 245 times over a 12-month period, the US Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) has revealed. The figure was included in a report by the ICS-CERT, which operates within the National Cyber Security and Integration Center, itself a part of the Department of Homeland Security. The report is classed as covering the 2014 fiscal year which, under US government dates, was between 1 October 2013 and 30 September 2014. “ICS-CERT received and responded to 245 incidents reported by asset owners and industry partners,” the report said.

U.S. power grid attacked every 4 days: 362 times in last 3 years (NA)

From www.examiner.com, 3/26/2015

A report released on March 25 by USA Today pointed to a grim vulnerability in the nation’s power and electrical systems. According to an analysis of federal energy records, a section of our power grid is hit by “a cyber or physical attack” once every four days. Between 2011 and 2014, there were 362 reported physical and cyber attacks of electric utilities that resulted in partial power outages or disturbances. Few of these attacks have resulted in major cascading outage events. However, they have heightened efforts by federal and energy agencies to explore ways they can use to thwart security attacks. Why? Electrical outages affect water distribution systems, air traffic control, military defense systems, and almost all modern conveniences we use daily without thought.

Iran poses global cyber threat (MENA)

From sputniknews.com, 3/11/2015

Iran poses a global threat to cyber security in addition to its nuclear endeavors, US Joint Chiefs of Staff Chairman Martin Dempsey said. "And then the two global threats [from Iran], of course, are their nuclear aspirations… and then cyber is the other global threat they pose," Dempsey stated at a US Senate Foreign Relations Committee hearing on the US President Barack Obama’s request for authorization of use for military force (AUMF) against the Islamic State. Dempsey also said Tehran's regional surrogates and proxies, weapons trafficking, ballistic missile technologies and new mines constitute security threats.

Cyber threat to U.K. power is real, evolving (EU)

From www.bloomberg.com, 3/11/2015

The U.K.’s power system faces an evolving threat from hackers as it becomes more dependent on computerized systems and data tools, according to a panel of lawmakers. The government must work ever more closely with utilities and security agencies, and provide sufficient funding to stave off cyber attacks, the House of Lords Science and Technology Select Committee said in a report published Thursday. “The risk of breaches to cyber security are real and will continue to evolve,” the panel said. “We are concerned about the threat in the medium term as the electricity system becomes increasingly reliant on fast communication, on data and dependent on automation.” The government said in December it is increasing spending on its cyber-security program by almost a third to 860 million pounds ($1.3 billion). About 10 percent of U.K. cyber attacks were in the energy sector in the last quarter of 2014, according to statistics from the nation’s Computer Emergency Response Team.

EU must adapt to new security challenges (EU)

From www.europarl.europa.eu, 3/10/2015

The EU and its member states must shoulder more responsibility for their security and defense at once, given the unprecedented levels of instability at EU borders, say Foreign Affairs Committee MEPs in a resolution voted. Member states must, as a matter of urgency, make more effective use of Common Security and Defense Policy tools, coordinate their internal and external security actions and pool resources more closely, says the text. In their annual resolution on the EU’s Common Security and Defense Policy (CSDP), MEPs press it to adopt a common strategy to tackle new challenges to its security. Strategic reflection already under way within the European External Action Service and the Council on a new European Security Strategy to deal with new geostrategic scenarios, threats and global challenges must be given a clear and concrete boost at the June 2015 European Council, they say.

Schneider Electric

The Global Cyber Advisor
Cyber Security Services
March 2015 / Volume 42

Cyber News

Shift in focus on infrastructure cyber security

From www.reuters.com, 3/2/2015

Lockheed Martin Corp , the Pentagon's No. 1 supplier, said it has seen a "sea change" in demand for cyber security services in critical infrastructure areas such as energy, oil and gas, and financial institutions over the past 18 months. Increased media coverage, more sharing of data about cyber attacks, tighter government regulations, and growing concerns about the fiduciary duties of corporate boards and chief executives have stoked that demand over the past 18 months, said Chandra McMahon, vice president of commercial markets for Lockheed's Information Systems security services.

Medical data has become the next cyber security target

From www.nextgov.com, 3/20/2015

Hackers often carry out massive cyberattacks to gain access to financial data through banks and retail companies, but this month's cybercrime hit a seemingly new target: medical data, taken from the health insurance company Premera Blue Cross. The attack affected 11 million patients, making it the largest cyberattack involving medical information to date. The healthcare industry has been catching hackers' attention lately. In February, the health insurance company Anthem reported a breach in which hackers accessed to about 80 million records, and in 2014, the Tennessee-based hospital operator Community Health Systems saw 4.5 million records accessed, though both companies said no medical data was exposed.

Air traffic control system vulnerable to cyber attack

From www.cnn.com, 3/2/2015

Problems with the Federal Aviation Administration's cyber security is "threatening the agency's ability to ensure the safe and uninterrupted operation of the national airspace system," a new Government Accountability Office report found. The 42-page document "Information Security: FAA Needs to Address Weaknesses in Air Traffic Control Systems" concludes the agency has taken steps to decrease vulnerabilities, but did not fully address problems including those which could make critical computer systems vulnerable to hackers. "These include weaknesses in controls intended to prevent, limit, and detect unauthorized access to computer resources, such as controls for protecting system boundaries, identifying and authenticating users, authorizing users to access systems, encrypting sensitive data, and auditing and monitoring activity on FAA's systems," the GAO authors wrote.

Cyber attacks on federal government hit record high

From thehill.com, 3/4/2015

Federal network cyber security incidents were up 15 percent in fiscal 2014 from the previous year, according to a recent government report. An annual Office of Management and Budget (OMB) report details information security practices across the government. A "cyber security incident" doesn't necessarily mean a network was breached, but it does mean hackers were trying. Those efforts hit record highs in FY 2014, up to 70,000. Nearly half of these incidents "were related to or could have been prevented by strong authentication," the report said.

Cyber attacks target small to midsize firms, security experts say

From www.jsonline.com, 3/10/2015

Small and midsize companies are among the most vulnerable organizations to cyber attacks, and many of them don't know it. That was one of the messages at a cyber training session sponsored by the Wisconsin Homeland Security Council. Obscurity is not security. Just because your business is small and isn't a household name, like Target or Apple, doesn't mean it's safe from cyber criminals. Small and midsize companies are probably more at risk because they don't always have adequate staffing to manage their websites and online business, said William J. Adams, a vice president with the Merit Network, a Michigan nonprofit that assists government and businesses with cyber security issues.

Premera security breach exposes 11 million customers

From www.king5.com, 3/17/2015

Millions of Premera customers are finding out their insurer was hit by a huge cyberattack. But the company says it has no evidence any data was removed from its system. Premera, based in Mountlake Terrace, announced Tuesday the security breach impacts its 11 million customers, including customers dating back to 2002. The insurer said an investigation revealed the initial malware attack happened on May 5, 2014, and went undetected until January 29, 2015.

Schneider Electric

The Global Cyber Advisor
Cyber Security Services
March 2015 / Volume 42

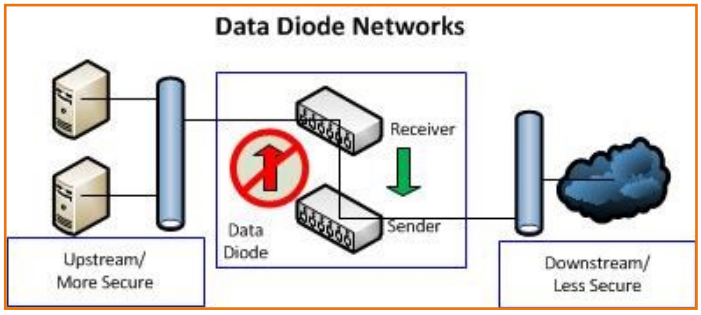
Is a Data Diode the Silver Bullet?

Recently, there have been many cyber security discussions associated with Unidirectional Data Devices, better known as Data Diodes. Some think the data diode is the silver bullet in cyber security. A data diode can enhance security in the appropriate environment; however, just adding a data diode to your network does not provide 100 percent protection for the network. A data diode cannot protect from an insider threat and unintentional personnel errors.

A data diode is a device that only transfers data in one direction. Think of a boat traveling in a river with a waterfall. The boat can go with the current and over the waterfall, but it cannot go upstream by jumping up the waterfall. This may raise some confusion since all Ethernet TCP/IP communications use a synchronize (SYN), acknowledge (ACK), and a finish confirmation (FIN) embedded in the data headers. Thinking about the boat and waterfall, the acknowledge signal would get trapped downstream of the waterfall and then create confirmation that the boat was still floating.

A data diode consists of two parts: a receiver and a sender. The receiver and sender may be located inside the same box or two separate boxes connected with fiber or wire. The data diode works by the receiver generating an ACK and FIN to make the upstream network connectivity work correctly. The receiver then generates a vendor proprietary data signature and sends data to the sender. The sender uses the data from the receiver, creates the appropriate SYN, checks for the appropriate ACK and sends data until the FIN when data transfer is complete. The sender and receiver ensure the TCP/IP traffic looks as expected; however, the sender never acknowledges to the receiver the data was actually transferred. There is no data flow from sender to receiver or up the waterfall.

If a network does not need communications from outside the network, a data diode provides an excellent security option. The nuclear industry is using data diodes to protect high security networks and data from outside the network is hand carried (better known as “sneaker-net”) to the high security network. Historical information is sent through the data diode; however, the high security network never receives acknowledgment or confirmation the historian received the information. Another application for a data diode is to send information, video, emails, etc. to various places or personnel. The data diode provides the capabilities to securely have real-time displays in maintenance, planning, or management’s offices to monitor plant conditions.



A data diode is limited and not practical if external data must be received by the internal network. A firewall, with good rules, is better suited when bi-directional data is needed. Using a data diode with historians can also be more expensive. Most historians require verification that the historical data is received so two historians are necessary. A historian is needed in the upstream network and a second historian is needed in the downstream network. The upstream network historian sends all historical data through the data diode to the downstream network historian. This is necessary to meet the data receipt validation for the historian and permit personnel to modify data extraction from the historian.

So, is a data diode the silver bullet? No, it is not the silver bullet. A data diode can protect certain types of networks from external threats. A data diode *can* enhance security; however, policies, procedures, and good cyber secure practices are still necessary to protect the network.

This month’s contributor to Consultant’s Corner is Bernie Pella
Consultant, Cyber Security Services, Schneider Electric

Schneider Electric

The Global Cyber Advisor
Cyber Security Services
March 2015 / Volume 42

Cyber Security Services

Schneider Electric's Cyber Security Services organization has the 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 Cyber Security Services include:

Hardware Independence

Cyber Security Services can work with any type of control system or type of technology a customer prefers for the security environment.

Regulation Knowledge

Cyber Security Services 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 Cyber Security Services 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

Cyber Security Services has a number of resources that understand the demands of Controls Networks and the requirements for continued uptime.

Proven Methodology

Cyber Security Services follows a proven life cycle methodology to support the implementation of a comprehensive successful cyber security program. Attributes of the lifecycle approach are Assessments, Development, Implementation, and Management.

Schneider Electric

For additional information please visit us at
http://software.invensys.com/services/security-and-compliance-services/cyber-security-services/

1650 West Crosby Road, Carrollton, TX 75006 ▪ P 972.323.1111 ▪ F 888.758.7675 ▪ www.schneider-electric.com