The Global Cyber Advisor

by the Cyber Security Services Group

Schneider Electric

July 2015
Volume 46

Korea Hydro & Nuclear Power Corporation Attacked Online (APAC)

From www.businesskorea.co.kr, 7/13/2015

Korea Hydro & Nuclear Power Corporation's internal data was circulated online again on July 8, with a self-proclaimed hacker threatening to expose the corruption of the corporation. The Public Prosecutors' Office has launched an investigation. The problem is that the Public Prosecutors' Office failed to meet expectations in a similar incident that occurred Dec. last year. At that time, the Public Prosecutors' Office pegged North Korea as the mastermind, because the IP addresses and the "Kimsuky" malware used in the hacking were similar to those used by North Korean hackers, and most of the access points corresponded to IP addresses in Shenyang, China, home to a lot of North Korean hacker activities. However, the Public Prosecutors' Office only found that circumstantial evidence. It also had to stop its investigation due to the lack of diplomatic cooperation with China.

this issue

Building Management Systems and Cyber Security

Over the past couple of years, the market has witnessed Building Management Systems (BMS) and Energy Management Systems (EMS) develop their inherent weaknesses. Many of these weaknesses are not just unique to BMS and EMS but also extend to most digital control systems. Most Building Automation Systems (BAS) communication protocols have their origins with serial communications and have little, if any, cyber security. However, as we move into the Internet of Things (IoT), the BMS and EMS are now being interconnected to the Ethernet networks, linking these systems to the corporate networks and many other dissimilar networks.

This near seamless integration with the larger networks and IoT presents a high level of inherent cyber risk to the BAS. Virtually everyone has connectivity or access to networks that they should not have access to. This paves the way for internal breaches, whether accidental or malicious.

Virtually every building, regardless of industry, region, or market has a BMS system or HVAC system. The high-profile cyber attack on national retailer Target all started with a malware-laced phishing email sent to employees at the HVAC vendor, not Target. The vendor had access to Target's network login credentials in order to remotely monitor energy consumption and temperatures at various stores where their HVAC systems were deployed. The phishing attack turned up those credentials, and the hackers used them to access the store's corporate network and, specifically, the company's payment systems. What makes this attack even worse is the low-tech simplicity of the attack.

Due to the evolving, diverse and complex nature of these control systems, many BMS and EMS owners simply do not know where to start when it comes to devising a cyber security strategy. A lack of awareness about their current vulnerability state means that the effective application of security technology or process is not possible. Many customers experience difficulty in determining vulnerability levels, exposure, and possible impact as well as the inability to monitor who has access to networks and critical assets. They also face difficulty in effectively distributing and enforcing appropriate policies and procedures.

As businesses and organizations become more reliant on technology to remain operational, a comprehensive cyber security plan is no longer just an option. A Cyber Security Assessment can help identify critical assets and define any potential risks, and from there, you can develop a plan to strengthen your organization's network to prevent or thwart potential cyber attacks and any lasting damage. While no organization can be 100 percent cyber secure, you can reduce your overall attack profile, making cyber criminals want to look someplace else.

Cyber Security Services by Schneider Electric

July 2015 / Volume 46

Cyber Central

Cornerstones of Cyber Security

Earlier this year in our January newsletter, we introduced ourselves and explained what we do at Schneider Electric. Then in February, we began our four-part "How We Do It" series, outlining our lifecycle methodology: Assess, Develop, Implement, and Manage. Last month we talked about how we benefit our customers using our seven cornerstones of cyber security, which are implemented through our Cyber Cornerstones Assessment.

Our Cyber Cornerstones Assessment includes an on-site and hands-on review of the customer's facility. By working closely with Control Staff, Operation Technology, IT, and Security Teams, we review and study:

- Current risk posture
- Applicable standards or regulatory needs
- Network security perimeter
- Patch management process
- Backup and recovery procedures
- Anti-virus status
- Operational critical assets

Benefits

A Cyber Cornerstones Assessment can help businesses and organizations become more cyber-secure, with benefits such as:

- Smoother adoption of a cyber defense program due to a team approach of solutions and strategies
- A site report detailing the seven cornerstones of cyber defense and how they can be integrated into processes and procedures
- Identification of potential interconnectivity issues that could lead to a compromise in cyber defense
- Site-specific technology planning and cyber defense strategies for Process Control and Automation
- Identification of cyber defense resourcing requirements needed for implementing and maintaining cyber defense strategies and technologies
- The ability to collaborate with Schneider Electric's Cyber Security Services team, which has extensive an background and experience in identifying and designing cyber defense solutions for Process Control and Automation

Our team can help equip organizations with up-to-date, comprehensive cyber security solutions to meet any requirement or regulation, whether it is company-mandated, industry-specific, government-issued, or merely a matter of best practices. Our experience in process automation environments allows our team of experts to deliver platform-agnostic solutions that help the client bridge the IT gap.
All of our solutions are hardware, software, and product independent.

Schneider Electric

The Global Cyber Advisor
Cyber Security Services
July 2015 / Volume 46

Industry News

German missiles 'hacked by foreign source' (EU)

From europe.newsweek.com, 7/8/2015

A German missile system stationed on the Turkish-Syrian border was reportedly hacked by a "foreign source" and carried out "unexplained commands." The Patriot missiles, stationed on the Turkish side of the border under the Nato pact, were briefly taken over by an unidentified hacker, according to German civil service magazine Behörden Spiegel. The magazine does not give details about what these orders were or when they were carried out, but suggests hackers may have gained access to the missile system through a computer chip which guides the missiles, or through a real-time information exchange which allows the missiles to communicate with their control system.

Cyber attack on US power plants could cause $1T in economic damage (NA)

From www.greentechmedia.com, 7/10/2015

Let's imagine an "improbable, but not impossible" cyber assault on the U.S. power grid, causing up to 50 power-plant turbines to overload and burn out, blacking out the power grid between Chicago, New York City and Washington, D.C., and leaving 93 million people across 15 states without electricity. While some power is restored within 24 hours, it takes weeks for the rest—and the cost to the U.S. economy adds up to $243 billion, or in a worst-case scenario, nearly $1 trillion. That's the scenario that "Business Blackout," a joint report by Lloyd's and the University of Cambridge's Centre for Risk Studies, lays out for a utility industry that's seeing cyber intrusions rise at an unprecedented pace. It also takes on the challenging questions of how to invest in protecting utilities against cyber threats that are evolving as quickly as the defenses against them, if not more quickly.

Italian cyber security firm suspects foreign government was behind mass attack (EU)

From www.reuters.com, 7/12/2015

Italian cyber-security firm Hacking Team said a government might have been behind a massive hack of its systems and warned that the subsequent leaking of its computer codes could prove a field day for criminals. Unknown hackers downloaded 400GB of data from the firm, which makes surveillance software that allows law enforcement and intelligence agencies to tap into the phones and computers of suspects. Much of the data, including thousands of private corporate emails, has since been dumped onto the Wikileaks website. The source code of a number of its top secret programs has also been published online. "Given its complexity, I think that the attack must have been carried out at a government level, or by someone who has huge funds at their disposal," David Vincenzetti, the CEO of Hacking Team, told Sunday's La Stampa newspaper.

Cyber crime 'costing Middle East $1 billion' (MENA)

From www.tradearabia.com, 7/1/2015

The Middle East IT sector is on track to register a year-on-year growth of 8 per cent against a backdrop of cyber crime which is costing the region up to $1 billion, said organizers of an upcoming cyber security event in Abu Dhabi, UAE. The first Middle East Cyber Security Life event, organized by Comexposium and DG Consultants and to take place on February 16-18 201, will address the issues associated with the latest trends in technological development and IT security, attended by industry experts from around the world.

Europe lags behind US, China and Russia in cybersecurity race (EU)

From www.ibtimes.co.uk, 7/13/2015

The US is at the forefront of cybersecurity – conceptually, politically and in terms of business. Having spent at least a decade integrating cyber into its security and societal thinking, it has also taken the lead in using cyberattacks as a tool of foreign and security policy, placing it far ahead of countries in Europe. Most European countries have cyber strategies on paper but public discussion at policy and doctrinal levels and practical measures are not as mature as they are in the US. The difference between the America and Europe is notable, and without serious efforts in Europe, the gap is only likely to widen. This would increase the potential for Europe to become the focal point for more serious cybercrime, espionage and even debilitating attacks. It would be foolish not to learn from the US but it is time for Europe to take more proactive role in cyber security—for its own sake.

The Global Cyber Advisor
Cyber Security Services
July 2015 / Volume 46

Cyber News

21.5 million exposed in second hack of federal office

From www.politico.com, 7/9/2015

Hackers stole sensitive information on 21.5 million people in the recently disclosed breach of the federal government's background-check database, the Obama administration said—a shocking number that revived lawmakers' calls for high-level resignations in the Office of Personnel Management. OPM Director Katherine Archuleta told reporters she will not resign and won't fire her chief information officer despite mounting calls for her to leave. House leadership added their names to the mostly Republican pile Thursday, with House Speaker John Boehner calling on President Barack Obama to "install new leadership at OPM." Sen. John McCain (R-Ariz.) also called for Archuleta's head, saying the new numbers were "nothing short of staggering," and adding that "it is time for new leadership at OPM to address the serious failures that led to this disastrous breach."

UCLA health and CVS Photo latest victims of cyber attack

From www.newsweek.com, 7/17/2015

University of California (UCLA) Health, which runs four hospitals in the university's campuses, and drug retailer CVS Health Corp's CVSphoto.com became the latest victims of cyber attacks. UCLA Health said on Friday that data on as many as 4.5 million individuals was potentially at risk, although it added it had not yet found evidence that individuals' personal or medical information was actually accessed or acquired during the breach.

Defense chiefs warn of Russian cyber attacks

From www.telegraph.co.uk, 7/15/2015

Top defense chiefs fear banks and finance firms across the UK and US could become targets of Russian hackers if relations between Moscow and the West worsen. Former GCHQ director Sir David Omand told an audience at the London Stock Exchange that state-led attacks on banks are an increasing threat. He spoke alongside US Admiral Michael Rogers, who said too many banks are ill-prepared for the consequences of a successful attack. "We have to take note of the potential for offensive state cyber attacks against our financial sector, not for criminal gain but for political purposes, for retaliation," Sir David told the event organized by the Royal United Services Institute.

Chinese hackers use US servers in cyber attacks

From freebeacon.com, 7/17/2015

Chinese-government linked hackers are using American computer services companies in conducting cyber attacks against private company networks, according to cyber security analysts. A detailed computer forensic investigation by a major U.S. security firm revealed that three recent cyber attacks were carried out by two Chinese hacker groups known as Deep Panda and Wekby. Both groups appear linked to each other and are part of a Chinese-government run cyber espionage campaign. The Department of Homeland Security stated in an internal report that cyber espionage targeting the bulk collection of personal data from government and private networks included nine attacks over the past year.

NSA Chief expects more cyber attacks like OPM hack

From www.wsj.com, 7/15/20215

The U.S. should brace itself for more attacks like one on the U.S. Office of Personnel Management—in which millions of sensitive government records were stolen, the director of the National Security Agency warned. The U.S. government last week said that two cyberattacks on the agency compromised more than 21 million Social Security numbers, 1.1 million fingerprint records, and 19.7 million forms with data that could include a person's mental-health history. "I don't expect this to be a one-off," said Navy Adm. Mike Rogers, who heads the NSA and the U.S. military's Cyber Command. The incident is causing the government to review cybersecurity policies, he added. "As we are working through the aftermath of OPM," Adm. Rogers said one of the questions is "what is the right vision for the way forward in how we are going to deal with things like this."

Schneider Electric

The Global Cyber Advisor
Cyber Security Services
July 2015 / Volume 46

Do you know where you are in regards to Cyber Security?

Do you know where your systems stand in regards to cyber security? With any endeavor in life, whether it is performing maintenance on your car or planning for retirement, an assessment of where you currently stand is the first step. Identifying where you currently are as well as anticipating what obstacles may come will have a direct impact on whether you will reach your destination or goals. Cyber security is no different. Rather than hoping for the best that your car will get you from New York City to Los Angeles, wouldn't you check the condition of your tires, ensure that you put new oil in your car, and ensure that your spare tire has adequate air pressure and that the jack is located in your trunk with all other necessary tools to change a tire in the event you get a flat? Cyber security is no different – performing an assessment will identify where you are and what steps you may need to take to reach your goal of protecting your systems from both internal and external threats.

The first step is to determine where you are – in my earlier example, you would identify things like what size tire your car uses, the approved air pressure, the conditions will you be driving through – will you be driving in January across country through snow and ice conditions, or will you be driving during the middle of summer where road conditions are dry? What is the current air pressure and tread depth of your tires, and how recently have you performed an oil change? For process control systems, you would need to identify what digital assets are part of the system, what operating system / applications are used on those assets, what approved security patches have been installed, and whether this system is a standalone system or if it connects to a network that may be accessible from networks external of the process control network. After you identify where you are, you can then make sound decisions on what actions should be taken – prioritizing what steps should be taken and scheduling when they should be performed.

Just like your car, assessments do not stop after you perform the initial evaluation. On a routine basis, you should reassess your systems. Have conditions changed that leave your system vulnerable to a different threat? New threats may require updates to your operating system or the addition of new virus signatures to your anti-virus solution, and in some cases, termination of employees require modification of user accounts and passwords.

As part of our comprehensive services, we can provide an assessment and gap analysis of where your systems currently stand and what steps should be taken for you to reach your goals of being compliant with your applicable regulatory body, whether it is NEI, NRC, CFATs, or other.

This month's contributor to Consultant's Corner is Michael Gasparovic
Consultant, Cyber Security Services
michael.gasparovic@schneider-electric.com

Schneider Electric

The Global Cyber Advisor
Cyber Security Services
July 2015 / Volume 46

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 WordPress!

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