Cybersecurity in Power Generation

David A. Bush

University of Wisconsin-Stout

Table of Contents

INTRODUCTION

Cybercrime is nothing new. It has been around even before computers became mainstream and took control of our economies and lives. However, hackers have traditionally focused their attention on cooperate business networks preferring to capture things like industry secrets, employee and customer data or simply tamper with a company's network.

While corporate networks are still very much a prominent target, industrial control systems (ICS) have become a viable target in recent years also. Marina Krotofil, a researcher at Hamburg University of Technology, told visitors at a 2015 Blackhat USA security conference that hackers have been penetrating industrial control systems of utility companies on a large scale for extortion since at least 2006 (Warwick, 2015).

More recently it hasn't just been rogue hackers or hacking groups looking to make some quick money. Nation state sponsored hacking has become more prevalent and it isn't extortion that motivates a nation state hack. Political motives of nation states have begun to move closer to the forefront of cyberattacks. In the last decade it seems that Iran has been at the heart of many disruptive industry attacks across the Middle East and even some in the United States (Greenberg, 2019).

This is not surprising when you consider in 2010 the discovery of Stuxnet; a piece of code jointly launched by Israel and the U.S. that destroyed Iranian nuclear enrichment centrifuges (Greenberg, 2019).

In fact, according to Fox News as recent as the April 2020 Iranian hackers hit Israeli Water Authority structures by cyberattack. These attacks had been launched on ICS of wastewater treatment plants, pumping stations and sewers (Weiss, 2020).

Of course, as we know, it isn’t just the US, Israel and Iran involved in the state sponsored hacking game. In 2017 a Saudi Arabian oil refinery was hit by hackers of unknown nationality by malware known as Triton or Trisis which disabled safety systems. But perhaps even more alarming is that it isn’t just private industry that is being targeted. In December 2016 malware called Industroyer was used by Russia to briefly cause a blackout in the Ukrainian capital city of Kyiv (Greenberg, 2019).

WHY ATTACK THE POWER INDUSTRY?

The motives behind hacking any industry are varied but are basically the same as for most other hacking targets. It could be money gained through ransomware or selling data through underground markets or to affect a competitor’s stock price. In many cases it is politically motivated either from hacktivist or nation states. And of course, there could always be the person with a personal grudge against the company. However, when an industrial control system is compromised, safety of employees and the surrounding community can be affected, as was the case with the Saudi oil refinery in 2017. There can also be costly damage to equipment and possibly even environmental disasters.

Many of these reasons apply to the power grid and all and more apply to power generation (power plants). For example, an attack to the power system could be part of a military action or a punitive measure in response to U.S. actions in some other area or simply a distraction to create a delayed response to some other initiative (Knake, 2017).

When you add the fact that many businesses and industries don't have the capability to supply their own power and few have the capability to supply themselves power long-term, it isn't hard to see how areas of the country could go from first-world to third-world status very quickly.

WHAT WOULD AN ATTACK ON THE POWER INDUSTRY LOOK LIKE?

If you think that in general, ICS is better protected than typical corporate IT networks, you may be surprised to learn that a 2019 report by the security company CyberX, shows that internationally, ICS networks continue to be soft targets for hackers. This is based on twelve months with data on over 850 production ICS networks in varying industries. While this report reaches across six continents, it shows some serious ICS security gaps such as plain-text passwords (69%), direct connections to the internet (40%) and weak anti-virus protection at 57% (CyberX, 2019). These vulnerabilities show how hackers may gain access, but what do they target?

As mentioned earlier, the Stuxnet worm was used to take control of Iranian centrifuges by targeting Siemens' supervisory control and data acquisition (SCADA) systems. Part of Stuxnet was to use the targeted PLCs as a hacker tool by means of a PLC rootkit and by manipulating the communication between the control computer and the PLC. By targeting both the control computer and the PLC, Stuxnet succeeded in achieving its goal and at the same time deceived the operators, buying enough time to destroy the centrifuges (Houmb, 2018).

As with Stuxnet, SCADA systems seem to be a primary attack vector to gain access into control systems. SCADA is a system of software and hardware elements that allow industrial organizations to control and monitor industrial processes locally or at remote locations. It can also allow personnel to directly interact with equipment through human-machine interface (HMI) software (Inductive Automation, 2018). If an attacker can gain access to a SCADA system, they may be able to gain complete control of the device.

Even though many SCADA systems are used with PLCs inside a plant and have no connection to the outside, there is a possibility of an attack from within the plant such as someone attaching a rouge laptop or plugging in a USB with malware on it into a control system, as was the case with Stuxnet. However, not all SCADA systems are on a closed network. SCADA is often used for control and monitoring over a large geographical area (Goodcore, 2020). This means that those SCADA systems are connected to the internet and can become cyber-attack targets.

Unfortunately, SCADA presents some unique challenges when it comes to security when compared to typical IT infrastructure. Some challenges with SCADA are that it typically has limited security software options due to usually being highly customized for a process and are also designed to have a very long-life span when compared to typical IT systems so are not upgraded often (Vô Ưu, 2016).

In fact, in a paper by General Electric titled *Top 10 Cyber Vulnerabilities for Control Systems*, communication of internet-based SCADA makes the list. GE’s solution uses a stateful firewall to protect against unsolicited in-bound traffic as well as providing firmware hashes to verify the integrity of GE firmware files to their customers (GE Oil & Gas, 2016).

One particularly interesting solution that is being developed to address hacking threats to internet facing SCADA systems is to use blockchain to constantly monitor the integrity of components of the system using SCADA to know if the system has been hacked (HDIAC, 2016).

Security vulnerabilities directly associated with SCADA are not the only ways to gain access to industrial control systems. Hackers are targeting energy companies, including those working in nuclear power and other critical infrastructures providers, with a technique that puts a new spin on a tried-and-tested form of cyberattack.

Cybercriminals are using phishing techniques and crafting a legitimate-looking email and sending it to the intended victim along with a malicious attachment. Once executed, it runs code for dropping malware, which can be used for ransomware, stealing data, or another form of attack. While this technique is not new, now attackers can run phishing campaigns without the need of an attachment or link with malicious code, instead, downloading a template file injection over an SMB connection to silently harvest credentials, according to researchers at Talos Intelligence (Palmer, 2017).

While the attack method is currently only used to steal data (such as credentials), researchers warn it could be employed to drop other malware. Since May 2017 hackers have been using this new technique to target energy companies around the world, predominately in Europe and the US (Palmer, 2017).

WHAT SAFEGUARDS ARE IN PLACE?

To address the growing risk posed by cybersecurity to the North American grid electrical system or Bulk Electrical System (BES) as it is referred to and ensure that it stays intact, the US has empowered FERC (The Federal Energy Regulatory Commission) to impose mandatory reliability standards on electric systems owners and operators. FERC chose NERC (North American Reliability Corporation) to be the Electric Reliability Organization (ERO) to develop reliability standards and enforcing compliance of FERC orders. In 2008 FERC issued order 706 which established the Critical Infrastructure Protection Cybersecurity Standard referred to as CIP standards. CIP standards focus on identifying and protecting the cyber BES assets critical to the electrical infrastructure. NERC in turn maintains and assesses the effectiveness of the CIP standards. Because CIP has the highest penalties of any regulatory framework in North America, electric companies are forced to take cyber threats seriously. While not the norm, CIP can issue penalties as high as 1 million dollars a day per violation! Even if a power generating or distribution company doesn’t want to think a cyber-attack could happen to them, they cannot afford the stiff penalties that may be enforced by CIP if they are found to be out of compliance (SANS Security Awarness, 2015).

From the perspective of a power generating facility, CIP lays out requirements that must be met to maintain the integrity of the control system. This does not however, apply to the business network that is used for things like email, writing work orders, using the intranet or internet. CIP regulations are concerned with the control systems (ICS) that, if compromised, would impact power generation. The amount of generation a plant is responsible for dictates the compliance level they must maintain. For example, if a plant has several generating units, the units must be segregated well enough so that a certain number of megawatts won’t be lost at one time if any piece of equipment is compromised.

Another example would be that any equipment (breaker, air compressor, etc.) that has an ethernet port that is not in use and documented as such must be locked. Additionally, USB drives must be scanned in a kiosk before they can be used in a control console. Additionally, USB ports are typically locked out to prevent someone from mistakenly putting a USB thumb drive into a control computer. Every piece of control equipment that is identified as a cyber asset is cataloged, tracked and audited to know what it does and what it is connected to. Every effort is made to minimize risk of cyber assets even down to the physical access to the equipment.

As mentioned earlier, the cost of non-compliance with NERC CIP is much higher than the cost associated with keeping current. Because of this, cyber assets are also kept up to date with the latest technology available. For example, even though there are firewalls where needed, unidirectional security gateway products sometimes referred to as a data diode or more vendor specific a Waterfall, is used to provide a gateway for one-way flow of data were needed. Much like a check-valve for data packets (The Department of Homeland Security (DHS), 2016).

SUMMARY

In the book titled "*Cybersecurity and Cyberwar What Everyone Needs to Know"* Leslie Harris of the Center of Democracy and Technology referred to Stuxnet as the opening shot in a war we will all lose. The author went on to say that it really depends on which aspect you wanted to focus on; the damage that can be done by cyberwarfare or the damage that isn't done (Singer & Friedman, 2014). Either way Stuxnet was a game changer. Certainty for the power sector. Now, in addition to hacker groups and lone hackers trying to see what they can do, the resources of nations are directed to look for ways to break into control networks that could cripple an economy, temporarily shut down vital services or simply create chaos to distract the masses.

It seems that power generation has been forced by the government to wake up and take measures to ensure cyber assets are protected from those with nefarious intent. As someone who has been involved with NERC-CIP requirements, self-audits as well as government audits, cybersecurity is being taken very serious by energy companies, especially in the power sector. But only time will tell if it is enough.

REFERENCES

CyberX. (2019). 2019 GLOBAL ICS & IIoT RISK REPORT. Retrieved from www.cyberx-labs.com

GE Oil & Gas. (2016). *Top 10 Cyber Vulnerabilites for Control Systems.* General Electric Company.

Goodcore. (2020, January 24). SCADA Systems and Their Role in Industrial Automation. Retrieved from www.goodcore.co.uk

Greenberg, A. (2019, November 20). A Notorious Iranian Hacking Crew Is Targeting Industrial Control Systems. Retrieved from www.wired.com

HDIAC. (2016, December 5). SCADA Vulnerabilities and Critical Infrastructure. Retrieved from www.youtube.com

Houmb, S. H. (2018, October 25). More exploits: the great PLC hack. Retrieved from www.controldesign.com

Inductive Automation. (2018, September 12). Retrieved from www.inductiveautomation.com

Knake, R. K. (2017, April 3). A Cyberattack on the U.S. Power Grid. Retrieved from www.cfr.org

Palmer, D. (2017, July 10). Hackers are using this new attack method to target power companies. Retrieved from www.zdnet.com

SANS Security Awarness. (2015, June 19). NERC CIP Cyber Security Training - Full Video. Retrieved from www.youtube.com

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford: Oxford University Press.

The Department of Homeland Security (DHS). (2016). *Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies*. Retrieved from www.us-cert.cisa.gov

Vô Ưu. (2016, October 26). CISSP - Communications and Network Security SCADA Security Concerns. Retrieved from www.youtube.com

Warwick, A. (2015, Augest 10). *BlackHat 2015: Industrial hacking - the untold story*. Retrieved from Computer Weekly: www.computerweekly.com

Weiss, Y. (2020, July 17). Israeli Water Infrastructure Hit Again by Cyberattacks. Retrieved from Homodia: www.hamodia.com