Cybersecurity in Oil Storage and Transportation

ABSTRACT

Cyber threats to the oil and gas industry have been existent in one form or another for as long as computing and networking systems have utilized to increase the efficiency of production and transportation operations. The number of systems that are utilizing internet-connected technology to aid the industry has risen dramatically over the past 20 years, seeing use on exploration, management of production systems, Supervisory Control and Data Acquisition (SCADA), and supply chain management. As the number of available exploits and attacks against these systems increases over time, it is more necessary than ever to ensure that cybersecurity is in facility and vessel plans. Incorporating cybersecurity measures into the existing security framework will be critical to ensuring that malicious actors do not impact communities and the environment through destructive attacks upon production and transportation. This paper will provide a look at the impact cyberattacks may have on the safe production, storage, and transportation of oil, as well as provide insight as to what industry standards and legal proposals exist to ensure that industry partners are operating securely throughout the US.

Introduction

As we step into the next decade of oil and natural gas production, there are new challenges to safeguarding the systems that support the production and storage of these products. It is my opinion that the most dangerous of these challenges is the emergence of easy to use and

sophisticated attacks against Industrial Control Systems (ICS), which are the underpinning for most modern industrial production environments. With the advent of nation-states using cyberattacks as a weapon against critical infrastructure, there is now an increased focus on the vulnerabilities found within industrial systems.

These attacks that have originated from nation-states have primarily targeted electrical distribution systems and nuclear material refinement. The possibility of an attack against oil production, refining, or distribution can result in real-world consequences that include harm to the public at large, environmental disasters, and economic impact. It is for these reasons that the oil industry should ensure that cybersecurity best practices are implemented across the entire scope of the product life cycle.

Threat Types

The first part to consider when evaluating the threat of a cyber attack is what physical effects result from a compromised or failed process controlled by an ICS. While the loss of production may result in an economic impact, the permanent damage caused to operational systems, or the manipulation of these processes by attackers to cause future unintended effects to create possibilities above and beyond downtime. The compromise of an ICS network can result in two attack paths. The first is the manipulation of the process control logic, which results in a change to the process and the control of actuators such as pumps or motors. The second is altering the sensor and input data sent across the network, such as rerouting sensor data.

Uniquely to ICS is that once compromised, there is very little forensic analysis that can be conducted on most of the critical components. Much of the network information, as well as memory states of devices such as Programmable Logic Controllers (PLC), were designed from the standpoint of maintaining a high degree of availability but not necessarily retaining data

integrity. There does not currently exist a practical way to monitor network traffic across the lower levels of an ICS network. These deficiencies, present in many ICS networks, mean that not only is an attack going to alter the process, but evidence of the attack also may not be present. Without this evidence, forensic analysis of the devices may not contain needed information for law enforcement and security staff.

The physical changes which can be performed on a system were demonstrated in the Aurora Generator Test of 2007. Conducted at Idaho National Laboratory in 2007, this demonstration showed that an attacker could remotely affect a generator in a way that physically destroys it. The attack consisted of taking the generator out of phase through the repeated manipulation of breakers, causing catastrophic failure. This attack was done in a manner that caused existing protection systems to critically fail (Lemos, 2007).

While this test was to serve as a warning to the power transmission industry, it is not hard to piece together how an attacker could cause damage to systems in the oil industry. With control of an ICS network, an attacker can manipulate remotely operated pumps and valves in a way that could cause the destruction of equipment or even alter the flow of liquids in a manner that would cause damage to valves and piping systems. In the transfer of products from vessels to facilities, monitoring systems protect overflow with Human Machine Interfaces (HMI). If an attacker gains control of these systems they can be manipulated in displaying a false state of the transfer process. From there, varying degrees of damage can be caused depending on the process and the knowledge of the attacker.

Another attack path is that of ICS networks operating onboard the maritime vessels, which provide a crucial role of transportation for both oil and chemical products. The potential of compromising a ship and their associated automated systems presents several attack paths that

range from controlling the ballasting process of a vessel to disabling generators in an attack similar to the one demonstrated in the Aurora project.

Recent Incidents

To see how a cyber attack could undermine and damage an industrial process, TRISIS, the 2017 cyber attack on Aramco in the Middle East, provides a strong example (Drago, 2019b). The attack targeted a particular component of the Aramco ICS network; the Schneider Electronics Triconex safety instrumented system (SIS). This attack is worth noting in that it focused on this process control component. Yet, it did not have to rely upon any vulnerabilities that were present in the Triconex SIS itself. This attack ultimately failed in its goal to do one of two things, shut down the process entirely, or create an unsafe environment by rewriting the logic of the SIS. This type of attack, with detailed knowledge of the targeted industrial system, can culminate in physical damage to the plant, which could cause additional impacts to surrounding areas.

An example of how a coordinated attack can lead to incredible effect is the 2018 Russian attack of the Ukrainian power transmission system. These attacks featured a fully formed and sophisticated campaign against Ukrainian power companies in 2015. These attacks originated with a coordinated spear-phishing campaign, which sent emails containing malware embedded in documents to IT personnel located at separate locations. This malware allowed further reconnaissance of the energy companies' enterprise network, eventually leading to a complete takeover of the compromised system. After gaining a foothold in the enterprise networks, the attackers pivoted into the ICS network. At this point, through coordinated attacks on all 3 of the targeted power companies, the attackers were able to shut down the power to approximately 230,000 customers for a short time. While the victimized companies were able to restore power

in a relatively short time, this was only completed by disabling the ICS system and reverting to manual control of the process (Lee, 2016). The ICS components which were compromised are still unable to return to fully automated control, which speaks to the lasting impact that a compromise of an ICS network can have.

The effects of a cyber attack upon an ICS attack in 2014 upon a steel mill in Germany is yet another demonstration of the impact these attacks can have. The exact details of the attack and the investigation results are not public knowledge, information that has been gathered points to the breach occurring through a spearphishing campaign. Spearphishing allowed attackers to gain a foothold in the mill's ICS network subsequently. There was an amount of physical damage done to the mill itself as a result of the attack upon the ICS processes in place. The extent of the damage is not known, but the proof of a cyber-physical attack demonstrates the importance of safeguarding ICS in any application (Lee, 2014).

The rise of ransomware and the risk that it can pose for an operation notable in the damage or disruption caused to victims. The 2017 cyber attack on Maersk disrupted operations across the company through the infection by NotPetya ransomware. The estimate of the financial impact of this attack is approximately $300 million (Greenberg, 2018). Even a nontargeted attack can be devastating to businesses. It is not an unrealistic scenario to have a worm pivot from an initial compromise on an enterprise network into an ICS network and cause an effect upon operations by rendering hosts inoperable.

Risk

The production and distribution of oil represent a critical infrastructure sector within the US. As such, the industry is a significant target, with many groups pursuing ways to exploit ICS networks and components that are in industrial applications. Dragos (2019b) indicates that at this

time, five groups are targeting North American oil and gas companies currently. Also, there has been a noted increase in activities from these organizations over the course of 2019. The ability to disrupt this sector does a great deal to cause a significant economic impact on a region, a tempting proposition for many groups.

An attack against an oil refinery could, if well-coordinated, could result in the release of petroleum products and other hazardous materials, potentially causing harm to human life and damaging the environment. It is important to note that a successful attack of this nature will additionally strain local response resources, both private and public. This ripple effect of events that would be triggered by a coordinated cyber-physical attack upon a port illustrates what makes these targets so desirable for attackers. The conclusion of the Dragos (2019a) report gives a grim warning. "Dragos assesses with moderate confidence that the first major cyber-related ICS event causing major process and equipment destruction or loss of life will occur in the oil and gas sector."

Prevention

Preventing these types of catastrophic events should be a priority for all oil and gas companies, and many methods already exist for mitigating risks that are known to provide some amount of protection from compromise. However, due to the nature of ICS networks, there are many features and security appliances usually available for enterprise networks that currently have no equivalent product for ICS. This should not be a limiting factor in hardening networks and deterring attacks upon your ICS network.

There exist several tools and guidelines to assist facilities and vessels in shoring up their security across bothe enterprise and ICS networks. The Cybersecurity and Infrastructure Security Agency (CISA) was formed in 2018 under the Department of Homeland Security (DHS) and

provides several products to businesses considered to be a part of the United States' critical infrastructure. The full list of these assessments can be found online at their website (https://www.cisa.gov/cybersecurity-assessments). The services range from vulnerability scanning of internet-facing hosts on a regular basis to on-site vulnerability assessments and penetration testing.

In addition to this, there are steps you can take to evaluate and harden your ICS networks without outside assistance. The Cyber Security Evaluation Tool (CSET) provided by CISA is a free product that can guide an organization by determining its overall security stance. CSET pulls components of industry guidelines such as NIST 800-82 (Guide to ICS Security) and provides the reviewer with results that can be analyzed over time to ensure compliance and security measures are being adequately maintained. These and many other security measures should be considered to prevent attacks, but there is no single method which will prevent all attacks. A good program must be constantly evaluated for its effectiveness, and facility and vessel operators must remain vigilant to ensure that a devastating cyber-attack is avoided.

References

Dragos. 2019a. Global Oil and Gas Cyber Threat Perspective. https://dragos.com/wp-content/uploads/Dragos-Oil-and-Gas-Threat-Perspective-2019.pdf

Lee, R.M., Assante, M.J., Conway, T. 2014. ICS CP/PE (Cyber-to-Physical or Process Effects) case study paper – German Steel Mill Cyber Attack. SANS ICS, 2014.

Filkins, B., Wylie, D. 2019. SANS 2019 State of OT/IC Cybersecurity Survey. SANS Institute.

Slowik, J., 2019. Evolution of ICS Attacks and the Prospects for Future Disruptive Events. https://dragos.com/wp-content/uploads/Evolution-of-ICS-Attacks-and-the-Prospects-for-Future-Disruptive-Events-Joseph-Slowik-1.pdf

Drago. 2019b. TRISIS Malware: Analysis of Safety System Targeted Malware. https://dragos.com/wp-content/uploads/TRISIS-01.pdf

Lemos, R.. 2007. DHS video shows the potential impact of a cyberattack. https://www.securityfocus.com/brief/597

Lee, R.M., Assante, M.J., Conway, T. 2016. Analysis of the Cyber Attack on the Ukrainian Power Grid. SANS ICS. E-ISAC. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

Greenberg, Andy. 2018. The Untold Story of NotPetya, The Most Devastating Cyberattack in History. Wired. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Resources

Cybersecurity Evaluation Tool (CSET)

https://www.us-cert.gov/ics/Assessments

NIST 800-82 Guide to Industrial Control Systems Security

https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

CISA Assessments

https://www.cisa.gov/cybersecurity-assessments