Name: Eric Corpus

Date: March 26, 2023

Critical Infrastructure Systems and SCADA Applications

As seen across all information technology systems an area of concern is the increase risks and vulnerabilities of critical infrastructure systems. These systems carry the same types of concerns but what needs to be considered is that the impacts of a cybersecurity incident would be at a much larger scale and most likely would be gravely devastating and lasting effects.

An Overview of Critical Infrastructure Systems and SCADA Applications

There are essential systems that are required to ensure the smooth functioning of everyday life. These systems are reffered to as critical infrastructure. These systems encompass an extensive range of highways, bridges, and tunnels that connect regions, railways, utilities, and buildings. These necessary systems are indispensable for transportation, commerce, and the supply of water and electricity (Critical Infrastructure | Homeland Security). Supervisory Control and Data Acquisition (SCADA) refers to a group of software applications that are utlized for contolling or monitoring industrical processes. This involves collecting information from entire sites, or complex systems deployed over vast areas for further processing by a centralized computer. SCADA is an essential capability to allow those that are responsible for these systems to determine and implement data-driven solutions and/or decisions for infrastructure processes, facility-based processes, or industrial processes (“SCADA Systems”).

Vulnerabilities associated with critical infrastructure systems

Vulnerabilities associated with critical infrastructure systems fall into either a logical (cyber) attack or physical attacks. The Department of Homeland Security states, “Cybersecurity threats to critical infrastructure are one of the most significant strategic risks for the United States, threatening our national security, economic prosperity, and public health and safety” (Secure Cyberspace and Critical Infrastructure | Homeland Security). To further examine vulnerabilities of critical infrastructure systems, first and foremost, these systems are a target for various bad actors. They can be at the state-sponsored level, hacktivists, or cyber terrorist. The motivations of these indivduals varies and spans a wide-range of goals. These individuals are seeking to attack and effect all and every type of critical infrastructure systems deployed everywhere. The Cybersecurity & Infrastructure Security Agency (CISA) list 16 critical infrastructure sectors which include communications, commercial facililties, critical manufacturing, energy, financial, healthcare, and transporation systems to name a few. These threat actors are using any and every combination of cyber malware, phishing, Denial of Service attacks as well as physical attacking of these systems which include physical theft, manipulation, and tamparing of components. These systems are vulnerable to attacks 24/7. They can be targets of opportunity or long-term focused. The reality with all critical infrastructure systems is that they are literally everywhere. Critical infrastucture is an increasing target set for attacks because the potential for malicious results are across a very large scale. If there are damaging effects to energy sectors, then the lack of power is immediately recognized. There would be crippeling effects if water, air or other criticial infrastructures were attacked.

The role of SCADA Applications

As previously mentioned, SCADA systems are comprised of hardware, firmware, software, and the people involved in operating these systems. SCADA applications play a crucial role in mitigating cybersecurity risks and vulnerabilities in industrial control systems (ICS). As these systems have evolved to IP based or other modern means to communicate and function, they are exposed to possibility of cyber attacks. There is a strong likelihood that system operations could be disrupted, or damage to equipment, or compromise of sensitive data. There are a few ways that SCADA applications can mitigate risks and vulnerabilities. By implementing strong authentication and access controls, encryption, IDS/IPS, patch management, and incident response planning all are potential ways that SCADA applications can reduce risks. After all, the most critical requirement for these systems is that they are operating safely and reliably.

Conclusion

Critical infrastructure systems should be given the same if not more of a cybersecurity consideration against today cyber threat actors, cyber terrorist, or any against any individual that seeks to do harm. There are many studies that prove that the increase in attacks against these critical infrastructures is increasing every single day. As those that are tasked with protecting these infrastructures as well as the associated SCADA/ICS systems, it is imperative that they do their best to protect against unimaginable catastrophies. For any individual responsible for cybersecurity, an important factor that must be considered is to train, consistently evaluate against threats, and train some more. This will ensure that in the event of an attack, those in charge of operating these systems do their job to the best of their abilities.

References

"Critical Infrastructure | Homeland Security." *Department of Homeland Security*, www.dhs.gov/science-and-technology/critical-infrastructure#:~:text=Critical%20infrastructure%20includes%20the%2 0vast,rely%20on%20these%20vital%20systems. Accessed 21 Mar. 2023.

Loshin, Peter. "SCADA (Supervisory Control and Data Acquisition)." *WhatIs.com*, 16 Dec. 2021, www.techtarget.com/whatis/definition/SCADA-supervisory-control-and-data-acquisition.

"SCADA Systems." *SCADA Systems*, 25 July 2018, www.scadasystems.net.

"Secure Cyberspace and Critical Infrastructure | Homeland Security." *Department of Homeland Security*, www.dhs.gov/secure-cyberspace-and-critical-infrastructure. Accessed 21 Mar. 2023.