Name: Richard Young

Date: 3/16/2024

Critical Infrastructure and SCADA

BLUF

SCADA (supervisory control and data acquisition) systems are powerful tools used to monitor and control infrastructure, facility-based, and industrial processes. Even though modern-day SCADA systems are well protected physically and digitally, they remain high-value targets to threat actors. Organizations must act diligently when it comes to the cybersecurity of critical infrastructure.

Brief History of SCADA

Even though the birth of controlling processors became a reality in the 1950s, the 1970s saw the evolution of digital computing, which futurised SCADA systems. With the invention of programmable logic controllers (PLCs) and digital communication protocols, such as Modbus and WinCC, SCADA systems became more advanced and capable of handling complex industrial processes. This era marked the transition from analog to digital control and monitoring.

As information technology (IT) continued to advance, SCADA systems increasingly integrated with IT technologies with the evolution of the internet. The convergence of SCADA with IT led to the adoption of web-based interfaces, real-time data analytics, and cloud computing capabilities. These advancements enabled remote access, enhanced decision-making, and improved operational efficiency. In recent years, cybersecurity has emerged as a critical concern for SCADA systems. High-profile cyber attacks targeting critical infrastructure have tested the vulnerabilities present in SCADA networks. Consequently, there has been a concerted effort to enhance the security posture of SCADA systems through measures such as encryption, authentication, and intrusion detection.

Critical Infrastructure Sectors

According to *CISA.org, "There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof".* The sectors consist of chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government,

healthcare and public health, information technology, nuclear reactor/waste/materials, transportation systems, and water/wastewater systems sectors.

These sectors are the most important parts of a civilization. If a threat actor gained access to or disrupted standard operational flow of any of these services, security and health would be at risk. An example of a threat successfully attacking a sector of our infrastructure could be the $22 million dollar *Change Healthcare* ransomware attack of 2024 carried out by “AlphV” or “BlackCat”. This ransomware attack forced people to go “10 days and counting” without their prescribed drugs. Though the healthcare system may not use SCADA systems to automate, monitor or control processes, they do use similar software like EHR (electronic health records) to secure personally identifiable information. This adds to the subject that no matter how secure physical or digital information may seem, the whole system is only as strong as its weakest link.

Similar to how *Change Healthcare* was compromised, hackers who are affiliated with China’s People’s Liberation Army took a stab at Texas’s electrical grid in 2023. The difference between the two attacks is the conclusion. With one attack, $22 million dollars was extorted and millions of patients' data was stolen and with the other, nothing came of it. Like I mentioned earlier, an organization can have the best physical and digital security but it’s only as strong as the weakest link. The policy that is enforced along with the security creates an in depth strategy. “ERCOT prepares year-round for any type of threat to the electric system. Whether the threat is cyber or physical, ERCOT continually invests in trained staff and resources to help keep the electric grid safe. From system redundancies to controlled access, ERCOT has multiple layers of protective measures to safeguard its critical infrastructure. This layered cyber and physical security approach is known as a defense -in-depth strategy.” -Electrical Reliability Council of Texas.

Conclusion

Throughout its evolution, SCADA technology has played a pivotal role in optimizing industrial operations, enhancing efficiency, and ensuring the reliability of critical infrastructure systems. As industries continue to embrace digital transformation, SCADA systems are poised to evolve further, leveraging emerging technologies to meet the demands of an increasingly interconnected and secure world. It’s important for organizations to inherit positive cybersecurity procedures like risk assessment and management, network segmentation, access control, encryption, active/proactive monitoring, incident response management, security awareness training, and regulatory compliance to actively and proactively secure the machines that we rely on.

References

Critical Infrastructure Sectors: CISA. Cybersecurity and Infrastructure Security Agency CISA. CISA. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

Greenberg, A. (2024, March 4). *Hackers behind the Change Healthcare Ransomware attack just received a $22 million payment*. Wired. https://www.wired.com/story/alphv-change-healthcare-ransomware-payment/

Huber, C. (2023, December 11). Chinese hackers targeted Texas Power Grid, other infrastructure. Chinese hackers targeted Texas power grid. Spectrum News. *https://spectrumlocalnews.com/tx/south-texas-el-paso/news/2023/12/11/report--chinese-hackers-targeted-texas-power-grid--hawaii-water-utility--other-critical-infrastructure-*

SCADA systems. SCADA Systems. (n.d.). https://www.scadasystems.net/