Name: Tay Lamell

Date: March 17, 2024

SCADA Systems

BLUF

SCADA systems are the vital piece to many infrastructures that allow societies to function and thrive. As such, it is of the utmost importance that any vulnerability they may face be corrected and defended against.

Introduction

Supervisory control and data acquisition systems, or SCADA, play a critical role in the functioning of multiple infrastructure systems. Such infrastructure includes mass transit systems, food and beverage production, and in the production, transmission, and distribution of electric power (*Where is SCADA Used? Examples of SCADA System Applications*, 2022), and many more. The incorporation of SCADA systems within these infrastructure systems has allowed for such advantages as the implementation of automated controls, the constant collection and reporting of data, and the ability to avoid downtime through a proactive maintenance system (Siggins, 2020). Because these systems are so crucial to day-to-day life, SCADA has ensured a way to keep things running as smoothly and efficiently as possible; however, that does not mean that it is without its flaws.

The Problem

Just like with all things technological, SCADA systems can, and often do, fall victim to cyberattacks. Dating as far back as 1982 when an attack caused a gas pipeline explosion in Siberia (Alanazi et al., 2023), time has shown that vulnerabilities to SCADA systems have shown that they can end in catastrophic results if left unchecked. SCADA systems used within energy management companies, for instance, help make the generation and distribution of whichever power source is being refined possible (*Where is SCADA Used? Examples of SCADA System Applications*, 2022). They also ensure that the power grids stay functioning. Should the systems utilized by such companies fall victim to an attack, large sections of the populace could go without power, like what occurred during the BlackEnergy attack in Ukraine in 2015 (*Cyber-Attack Against Ukrainian Critical Infrastructure*, 2021). Large scale power outages, especially in today's electricity-dependent world, can have a domino effect that not only impacts other industries (and possibly the economy as a result), but can also be a matter of life and death should medical institutions be impacted as well.

According to reports sent in to Trend Micro's Zero Day Initiative, an organization that collects information on the cyber vulnerabilities discovered by various researchers (*About ZDI*, n.d.), it is very likely that SCADA systems will continue to be victim to their vulnerabilities for some time to come (*One Flaw too Many: Vulnerabilities in SCADA Systems*, 2019). They hold the belief that the existence of vulnerabilities to SCADA systems allows for similar and/or more severe cyberattacks to occur again in the future, and after doing some research of my own, I agree. The very nature of SCADA systems makes them the heart of not only the companies in which they are in use, but of society as a whole. This is not to paint the picture that the weaknesses faced by SCADA systems have never been corrected, nor to say that there aren't steps in place to help mitigate the risks involved. In fact, the National Institute of Standards and

Technology (NIST) has tips for organizations to combat them. These include the maintenance of strict policies for the devices that use SCADA systems, regularly managing user access to these systems, the application of network segmentation to help prevent sensitive information from escaping the organization (*One Flaw too Many: Vulnerabilities in SCADA Systems*, 2019).

Conclusion

SCADA is the heart of many infrastructures which allow other organizations to thrive. When SCADA systems fall victim to cyber attack, the infrastructure in which they're in place fails as well. Beyond the organization in which they're used, SCADA vulnerabilities can have a ripple effect into the surrounding community depending on scale. The fallouts of the exposure of these risks can range from crippling financial institutions to wreaking havoc on the environment (Alanazi et al., 2023). Because of this, despite the benefits that SCADA systems offer organizations, it is important to remain vigilant to the risks posed by their use, and that they are updated to properly combat them.

References

About ZDI. (n.d.). Zero Day Initiative. Retrieved March 15, 2024, from https://www.zerodayinitiative.com/about/

Alanazi, M., Mahmood, A., & Chowdhury, M. J. M. (2023). SCADA Vulnerabilities and Attacks: A Review of the State‐of‐the‐Art and Open Issues. *Computers & Security*, *125*(103028), 103028. https://doi.org/10.1016/j.cose.2022.103028

Cyber-Attack Against Ukrainian Critical Infrastructure. (2021, July 20). Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01

One Flaw too Many: Vulnerabilities in SCADA Systems. (2019, December 16). Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/one-flaw-too-many-vulnerabilities-in-scada-systems

SCADA Systems. (2024). SCADA Systems. https://www.scadasystems.net/

Siggins, M. (2020, May 27). *Top 7 Benefits That a SCADA System Brings to Your Organization*. DPS Telecom. https://www.dpstele.com/blog/top-7-benefits-that-a-scada-system-brings-to-your-organization.php

What is SCADA and Where is it Used? (2022). Antaira. https://www.antaira.com/What-Is-SCADA-and-Where-Is-It-Used

Where is SCADA Used? Examples of SCADA System Applications. (2022). DPS Telecom. https://www.dpstele.com/scada/where-is-used.php