Shawn Ziegler

CYSE 200T

Write-Up

4/4/25

SCADA Systems

Introduction

The SCADA system stands for supervisory control and data acquisition. This system is used to control infrastructures, facility-based processes, and industrial processes. This system is critical for organizations to maintain efficiency, communicate issues in a system, as well as process data. The SCADA system is used to manage many industrial processes. This system also has the ability to keep records, report the processing status, and report issues.

Vulnerabilities of SCADA Systems

A SCADA system is designed for environments that are isolated, which presents a lack of authentication. This vulnerability allows for unauthorized users to access the system and enable manipulation control. This system lacks a continuous monitoring system. This type of vulnerability makes it difficult to defend against breaches as well as prolongs the recovery time of data that was stolen because there is an absence of real-time monitoring. Another vulnerability that the SCADA system may face is employee training insufficiency. Employees who are undertrained put the system at risk and are exposed to cyberattacks due to user errors (Amos, 2025).

Mitigating Risks of SCADA Systems

In this article, the risks of cyber-attacks on infrastructure are discussed and implementing the SCADA system is necessary to reduce these risks. This article lists a variety of ways to mitigate the risks. The first strategy is replacing and updating hardware and software. Another way is to update procedures and policies, Lastly, incorporate secure encryption protocols. This article also suggests developing a firewall and virtual private network will help reduce the risk of vulnerability (Edwards, 2021).

Conclusion

After researching the SCADA system it is apparent that the implementation of this system is required to manage infrastructures. It is important that keeping policies and procedures updated ensures security within the system. Real-time monitoring reduces the risk of cyber-attacks. Implementing this type of monitoring system allows for an easier process of gaining back control of the system if it faces a breach attack.

Sources

Amos, Z. (n.d.-a). *9 SCADA system vulnerabilities and how to secure them*. 9 SCADA System Vulnerabilities and How to Secure Them. https://gca.isa.org/blog/9-scada-system-vulnerabilities-and-how-to-secure-them

Edwards, J. (2021, February 9). *Someone is trying to take entire countries offline and cybersecurity experts say "it's a matter of time because it's really easy."* Business Insider. https://www.businessinsider.com/can-hackers-take-entire-countries-offline-2018-12

SCADA systems - SCADA systems. (2018, July 25).

https://www.scadasystems.net/