Name: Timothy Taylor

Date: November 5th, 2023

SCADA: Roles & Vulnerabilities

Supervisory Control And Data Acquisition (SCADA) systems are centralized systems that oversee and coordinate industrial, infrastructure, or facility-based process or processes. These systems have become increasingly vulnerable to cyber warfare attacks due to internet connectivity and Internet Protocols. Physical security is no longer enough to maintain the data integrity stored in SCADA systems.

Vulnerabilities of SCADA Systems

SCADA systems use a Human Machine Interface that gives processed data to the human operator. This interface is linked to the system databases, meaning these human operators can access the same information as the SCADA systems. Human error, such as improper training and awareness of SCADA security, may pose a severe risk to the integrity of the data stored in this system.

With the implementation of integrated SCADA systems, open communication between third-party SCADA packages has appeared within the market. The security practices of these third parties can impact the overall security of the SCADA systems and significantly increase the vulnerability of SCADA systems. If a security breach were to occur through a third-party package, this new gateway could infiltrate any SCADA system it is associated with.

SCADA systems tend to have poor network segmentation. Instead of separate networks and firewall protection, they often run on weakly secured Virtual Private Networks (VPNs) or Land area networks (LANs). The inadequate network segmentation of SCADA systems allows for easy lateral movement and increases the potential impact of a breach.

How do SCADA Systems Mitigate the Risk of Vulnerability?

Network analysts and penetration testers perform routine security audits and vulnerability tests to ensure that the system's security is addressed and up-to-date. This procedure minimizes the likelihood of a system breach and prioritizes any weaknesses identified in SCADA systems.

Physical security is equally as important as network security in breach prevention. SCADA systems store a multitude of company data, meaning that tampering and property theft are just as much of a security risk as network infiltration. Proper authentication and access control, such as multi-factor authentication and monitored work environments, are essential to protecting physical company assets.

Companies that use SCADA systems have begun developing firewalls and whitelisting solutions to harden the defensive barriers connecting sensitive company data to wireless access control systems. These solutions allow for easier traffic filtering, quicker intrusion detection, and log generation. The company will have a better handle on who has entry to the system and instant threat handling.

Conclusion

SCADA systems are ever-evolving as a database control system. As we expand on its capabilities, there are many unknown or overlooked risks associated with them. As an essential asset for company infrastructure, its routine maintenance and management is critical for the company to operate. Despite the best effort of cyber experts, there are still many vulnerabilities that need to be investigated and mitigated by cybersecurity professionals.

References

SCADA Systems. (2023). *SCADA systems*. SCADA Systems. https://www.scadasystems.net/

G. Yadav and K. Paul. (2019). *Assessment of SCADA System Vulnerabilities.* https://ieeexplore.ieee.org/abstract/document/8869541