Hannah Johnson

CYSE 200T

October 25, 2024

SCADA Applications and Mitigating Risk

BLUF

SCADA is a term that stands for supervisory control and data acquisition , which involves systems used to control and monitor infrastructure processes, facility-based processes, and industrial processes. The SCADA system addresses vulnerabilities in critical infrastructure systems and determines practical and secure methods to resolve issues that may arise (SCADA Systems).

Critical Infrastructures Vulnerabilities

A critical infrastructure basically includes any vital systems in our day-to-day lives (Critical Infrastructure). Such systems include transportation, running water, and electricity (Critical Infrastructure). Considering that critical infrastructures are intrinsic to almost every aspect of our lives, it's no surprise that there are a myriad of weak spots and vulnerabilities in these systems and ways that people can exploit these vulnerabilities. Three prominent areas of possible exploitation include:

- Cyber security threats (in this case, malware and ransomware). Recently, more than 2 in 5 ransomware attacks have been targeted toward critical infrastructure, specifically in healthcare and manufacturing (Kapco, 2024).
- Physical threats such as vandalism or natural disasters.

- Supply chain risks. Critical infrastructure systems frequently contain sensitive information about individuals, including Personally Identifiable Information (PII). By targeting supply chains, attackers can access this data for malicious purposes (Innovative Technologies LLC).

The SCADA System Structure

The SCADA system works by involving three different aspects of the infrastructure; Equipment, RTUs (Remote Terminal Units), and HMIs (Human Machine Interfaces). The basic system operates thusly: The RTU sends commands to the equipment, which then collects and sends data back to the RTU. The HMI (either on-site or remote) sends manual and automatic controls to the RTU, which then sends the collected data from the equipment forward to the HMI. The HMI creates overviews based on that data, as well as reports to help maintain the equipment and system (What is SCADA?).

Reducing Vulnerabilities Through the SCADA System

The SCADA system enables multiple users to oversee and control various functions simultaneously. This not only allows for continuous monitoring, but also adds more pairs of eyes to the information. Such monitoring can ensure that the data is not only accurate, but also that it has not been tampered with by an outside source. The SCADA system also uses secure equipment enclosures to help keep unauthorized individuals out (Cybersecurity of Critical Infrastructure with ICS/SCADA Systems). Network segmentations, such as firewalls or software-defined micro-segmentation,

create a barrier between ICS networks and IT environments, as well as the internet, making it harder for hackers to access the information as well as giving hackers plenty of time to detect the threat (Cybersecurity of Critical Infrastructure with ICS/SCADA Systems). To further protect and keep the confidentiality of data, SCADA systems employ a solid identity and access management system, ensuring that only verified and authorized personnel can make changes (Cybersecurity of Critical Infrastructure with ICS/SCADA Systems). Using all of these protections and more, the SCADA system effectively protects the data and operations of critical infrastructure.

Conclusion

Supervisory Control and Data Acquisition (SCADA) systems play a very important role in safeguarding critical infrastructure by utilizing technological tools and human-machine interfaces. These systems increase operational efficiency while minimizing vulnerabilities associated with cyber threats, physical attacks, and supply chain risks. By providing real-time monitoring, automated responses, and enhanced security measures, SCADA applications help detect and mitigate risks before they escalate and ensure the integrity and reliability of essential services (SCADA Systems).

References

Critical Infrastructure. U.S. Department of Homeland Security. (n.d.). https://www.dhs.gov/archive/science-and-technology/critical-infrastructure

Cybersecurity of Critical Infrastructure with ICS/SCADA Systems. IEEE Public Safety Technology initiative. (n.d.). https://publicsafety.ieee.org/topics/cybersecurity-of-critical-infrastructure-with-ics-scada-systems

Innovative Technologies LLC. (2024, April 11). *Why are supply chain attacks targeting critical infrastructure?*. LinkedIn. https://www.linkedin.com/pulse/why-supply-chain-attacks-targeting-critical-ztaee/

Kapko, M. (2024, March 11). *Ransomware attacks are hitting critical infrastructure more often, FBI says*. Cybersecurity Dive. https://www.cybersecuritydive.com/news/ransomware-hitting-critical-infrastructure-fbi/709814/

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

What is SCADA?. SCADA International. (n.d.). https://scada-international.com/what-is-scada/