Anthony Gonzalez

Professor Kirkpatrick

CYSE 200T

06 November

SCADA Systems

Supervisory control and data acquisition or also known as SCADA(SCADA Systems). SCADA systems are a blend between hardware and software. These systems are meant to monitor and analyze over large areas, especially in production facilities and industrial plants. SCADA is meant to gather information in real time and analyze it quickly. It is really helpful for prioritizing critical or time sensitive events(Salgado). An example of SCADA is real life: if there is a pipeline leak, the SCADA systems in place will help detect the leak and send information on the leak and how quickly or how to fix the leak.

Vulnerabilities with SCADA and critical infrastructure

SCADA can be extremely helpful in a job site, but as all things in cybersecurity it has some extreme vulnerabilities that is money costing. SCADA controls some of the main physical processes such as: traffic lights, water distribution, gas transportation etc. If someone were to get some unauthorized control of these SCADA systems it can really hurt what is going on within. Access control is very important to prevent this from happening. DDoS and malware attacks are a huge blow on any critical infrastructure. They both have the potential to ruin an organization's availability(Security insights). Another thing could be lack of software or hardware maintenance.

If these aren't kept up to date it is much easier for DDoS and malware attacks to happen on your systems.

SCADA Mitigating risks

Add on detecting and monitoring systems into the SCADA systems, because if these aren't implemented it could go wrong, very quickly. Have network security protocols such as: access control, recovery systems, back-ups etc(Kurii). Access control is extremely important because it gives access to these SCADA systems. Only limited people should have access to these systems. Recovery plan/systems is another important aspect. If there is a problem within your SCADA systems there should be a plan implemented to minimize damage done while these systems were done. Finally, back-ups are important because if you don't back-up your data, you could lose all your data you had piled up for months or years.

CONCLUSION

SCADA is very vulnerable to DDoS and malware attacks, and these are very avoidable. Critical infrastructure is very important to keep up to date with your hardware/software, because if you are unable to do this, you are vulnerable to these attacks. To sum up everything that has been stated, SCADA systems are very helpful in a job field, but if you cannot protect these systems from attackers it can be very hard to keep these systems up.

Works Cited

Salgado, Uziel. “What Is SCADA System & How Does Scada Work? - INDUSTLABS.” *Industrial Automation & Control Systems*, Industrial Automation & Control Systems, 3 May 2020, https://www.industlabs.com/news/what-is-scada.

Top 7 Cyber Threats on Critical Infrastructure - Security Insights. SecurityInsights, https://www.securityinsights.net/top-7-cyber-threats-on-critical-infrastructure/.

Kurii, Yevhenii. “Scada Cyber Security Threats and Countermeasures: Ultimate Checklist.” *ELEKS*, 2 Mar. 2022, https://eleks.com/blog/scada-cyber-security-threats-countermeasures/#:~:text=SCADA%20networks%20without%20monitoring%20and%20detection%20systems%20in,amount%20of%20damage%20done.%20Have%20network%20security%20protocols.