SCADA Systems and Vulnerabilities of Critical Infrastructure

BLUF: SCADA systems are designed to collect information about systems and communicate that to central systems for review and analysis.

What is a SCADA System?

Systems across the world need to communicate between systems in order to function efficiently. This is what supervisory control and data acquisition (SCADA) systems are designed to do. They collect data that can be used to detect if a system is performing well or it is failing in some way or another. This is done using programmable logic controllers, remote terminal units, and human machine interface. Programmable logic computers (PLC) are basically simple computers that are programmed to do a specific task and monitor a system at the same time. "Often, the RTU converts all electrical signals coming from the equipment into digital values like the status- open/closed – from a valve or switch, or the measurements like flow, pressure, current or voltage"(2). Remote terminal units (RTU) are basically devices that are the connection between physical equipment and central control systems.

Vulnerabilities in Critical Infrastructure

One of the first problems with critical infrastructure is that in large scale projects there is an even larger number of devices all connected to that system. With there being so many devices if malware gets into one system it can spread throughout all the other systems. So all the systems that are connected to the central systems need to be protected just as much as the central system. Another vulnerability just as important in critical infrastructure is human error. "Think about social engineering attacks, insider threats, lack of security awareness training, and inadequate

response planning”(2).Software and hardware can also be a major vulnerability in critical infrastructure in many companies. Older operating systems that are not updated can be vulnerable to all kinds of attacks. Then the reason for these systems not being updated can be because of these systems not being compatible with newer technologies.

Mitigating Risk

In order to minimize risk in the large number of systems that control a network of machines many options of protection are taken into account. Patches to operating systems are sent out monthly and usually have patches for new vulnerabilities that have just been introduced. Therefore, it is important to update your operating system as soon as possible. System monitoring and system logs can help identify any suspicious activity going on in a system. They can also be configured to message your phone if there is any suspicious activity that needs to be taken care of. Segmenting or restricting access can be used to make sure that SCADA systems are not accessible by other networks. The principle of least privilege can also be used to make sure that a system can only see what it needs to do its job.

Conclusion

SCADA systems are used all around the world and are one of the best ways to monitor and control a network of systems. Even with the vulnerabilities new ways to mitigate risk are being produced. As a cybersecurity major SCADA systems would be a large point of interest for me and I should be knowledgeable of them.

References

1. TuxCare PR Team. (2023, May 16). 5 Cybersecurity Weaknesses Critical Infrastructure Owners Should Guard Against. TuxCare. https://tuxcare.com/blog/5-cybersecurity-weaknesses-critical-infrastructure-owners-should-guard-against/
2. SCADA Systems. https://www.scadasystems.net/
3. Jordan, Z. (2024,March 9). SCADA System Security: A Control Engineer's Guide To Best Practices 2/3. Linkedin. https://www.linkedin.com/pulse/scada-system-security-control-engineers-guide-best-practices-jahan-tlbif#:~:text=Preventive%20Measures%20to%20Mitigate%20Risks%3A&text=Physically%20secure%20SCADA%20systems%3A%20Implement,to%20prevent%20unauthorized%20physical%20access.