SCADA

Jonathan Roeseler

Undergraduate Cybersecurity Student, Old Dominion University

CYSE200T: Cybersecurity, Technology & Society

Professor Kirkpatrick

9 November 2023

BLUF:

This writeup on supervisory control and data acquisitions systems[SCADA] will explain the vulnerabilities associated with critical infrastructure systems, and the role SCADA applications play in mitigating these risks.

Vulnerabilities associated with critical infrastructure systems

According to an article on scadasystems.net, SCADA refers to industrial controls systems used to control infrastructure and industrial processes. Due to the ever-growing use of SCADA systems, security concerns have risen as well. An attack on such important systems would be a result of cyberwarfare or cyberterrorism, as such an act would invoke a serious and strong response from the victim nation. Therefore, the compromise of SCADA systems could lead to many deaths, economic loss, and so on. For example, if an attacker was able to shut off an entire electrical grid during the winter; many people could freeze to death, in addition to the fact many would no longer be able to work.

SCADA applications role in mitigating risks of critical infrastructure systems

One of the main protections against outside attacks in SCADA systems is that such systems are disconnected from the Internet. This is a good prevention to a good number of attacks; however, there are still many threats that need addressing. One issue that needs addressing is unauthorized access to the software which controls the host machine. Some mitigations for this vulnerability include: disallowing use of USB devices, patch management, and sandboxing and testing any new software before its deployed to make sure its virus-free and works as intended ("Security News"). Another vulnerability that needs to be addressed would be packet access to the SCADA system. Even though these devices are offline, threats, such as an insider, are still in position to compromise these systems. Therefore implementing policies that only allow certain devices to connect to the SCADA network is crucial, on top of that, adequate access control to further these policies would help prevent unauthorized access to the network.

Conclusion

SCADA systems are most vital to society, and because of this, their security should be treated like it. The impact of a compromised system will always lead to a devastating outcome because of the criticality. Therefore, some of the most common protections(and needed protections) are network segmentation, access control, and the principle of least privilege.

References

"One Flaw Too Many: Vulnerabilities in SCADA Systems." *Security News*, www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/one-flaw-too-many-vulnerabilities-in-scada-systems. Accessed 8 Nov. 2023.

"SCADA Systems." *SCADA Systems*, www.scadasystems.net/. Accessed 8 Nov. 2023.