Stephen Giorgi

CYSE 200T

Professor Kirkpatrick

11/2/2022

Introduction

Supervisory Control and Data Acquisition (SCADA) systems are the systems in place used for monitoring and controlling critical infrastructure systems. Critical infrastructure refers to the assets of a business, group, or government that is necessary for society to function. SCADA systems can cater to anything from manufacturing processing for a business to gas pipelines. Through this write-up I will outline the importance of SCADA systems, the possible vulnerabilities, and ways to mitigate the risks associated with them.

Importance of SCADA systems

According to an article on EWeek.com by Fahmida Y. Rashid, in 2011 the FBI confirmed that SCADA systems for two cities (Springfield, Illinois and South Huston, Texas) were compromised. This led to multiple issues, while the attacks were brief, they caused the water systems to be tampered with and the unauthorized shutting down of a power plant. This also led to reasonable fear of other systems becoming compromised, such as the Illinois Fusion Center. Truly, the importance of the SCADA systems and the systems they are integral to can not be overstated. When these systems are compromised, it can mean serious consequences including lives lost.

Vulnerabilities

Before we ask how we can prevent future SCADA systems from being compromised, we must ask how these systems may be compromised. Most believe these systems are safe based on the fact that they are not connected to the internet and are physically built to last. The problem is that most can still be hacked by tapering with systems they connect to and can still be physically compromised through human access. Malware can be injected into a SCADA system either physically, directly into the system or through a network device on the same LAN as the SCADA system such as a switch.

Mitigating risks

What can be done to mitigate these risks are fairly simple. First and foremost, employees need to be trained in operational security and not allow for unauthorized personnel to have

access to the system or have the system compromised from misuse. Second, security measures regarding the network side of the system, such as packet asses, must be emplaced. For example, Forcepoint has their own application designed for operational security and management called Next Generation Firewall (NGFW).

Conclusion

Forcepoint is just one option for security application. It would be wise for someone in charge of a SCADA system to consider multiple options to fine the best solution for their situation. Time and money can only be so much of a consideration in protecting a system that is this important. Once again, these systems being compromised can mean that lives could be lost, and environments could become unlivable. Both human and network vulnerabilities should be prioritized and managed through training and application.

Works Cited

-, F. Y. R. (2021, February 2). *FBI admits attackers compromised SCADA systems in three U.S. cities*. eWEEK. Retrieved November 2, 2022, from https://www.eweek.com/security/fbi-admits-attackers-compromised-scada-systems-in-three-u.s.-cities/

SCADA systems. SCADA Systems. (n.d.). Retrieved November 2, 2022, from http://www.scadasystems.net/

What is Scada Security. Forcepoint. (2021, May 6). Retrieved from https://www.forcepoint.com/cyber-edu/scada-security