Write-Up – SCADA Systems

Tyre F Thompson

11/02/22

Bottom line is SCADA systems has many vulnerabilities; with these vulnerabilities it can makes a terrible time for the places that use the system. Of course, this a bad thing but also has some good that can come out of it. I say this because if there is realm of possibility people will always look for the solution to the problem and make the system much better than before.

SCADA Systems

First the term SCADA stands for "Supervisory Control and Data Acquisition". SCADA's are implemented to operate a lot of gears and servers in SCADA environments and industries. Just one of these SCADA systems may be over communication protocols. SCADA are basically systems that regulate and monitor the entire site that it is in, they are very complex systems spread out over very many areas. Some of the things that these systems can do is monitor production, development, and manufacturing. Furthermore, SCADA systems are really used in infrastructural processes like water control, gas, and power distribution. SCADA systems are a worldwide thing with a lot of industries using them now. These systems can control oil pipelines, an even nuclear facility. SCADA systems take in data to analyze so it can find potential threats. One thing to note is The Human Machine Interface, which is a device that humans use to interact with the SCADA systems database. With that being said outlying data that is visible can be

modified in the system to display alarms and produce visual ques to help detect their vulnerabilities. You can also use terminals to get rid of some of the vulnerabilities that the SCADA system has.

Vulnerabilities

Some of the most common threats to critical infrastructure systems are DDoS attacks, malware attack, critical network segmentation, parameter manipulation, and web application attacks. These vulnerabilities can be characterized as systems, assets, installation, applications, or anything that can fail on itself and result in an attack or some sort of threat. These same vulnerabilities have been noted for a very long time. Threats can be technical, caused by humans, accidental or natural. Therefor, we must implement things to reduce the amount of risk that we will take on. Critical infrastructure vulnerabilities are the geographical location because they are so close to one another. Which means if something were to happen in the same area as them, they can be vulnerable to the attack as well. Also, some SCADA systems control water and electrical systems, that are usually connected to a network, which makes them vulnerable to cyber-attacks. SCADA systems are over sensor and application software, which means the system has an extensive attack surface. When SCADA system gets attack the results can vary from the system being down for a time to the system being destroyed. An example of a critical infrastructure vulnerability was a vulnerabilities found in 2015 in the “Schneider Electric ProClima software”, “this software was designed to help the thermal management of an environment. These vulnerabilities were found by tricking someone to open a malicious URL or a suspicious file. This threat can execute arbitrary code on the targeted system.” Once this happened the “Schneider Electric Proclima suffered production delay, damage to equipment, safety hazards, and downtime.” This is all because of the vulnerabilities that have been exploited

in the infrastructure of Schneider Electric Proclima. In order to enhance the security of SCADA to lower some of the cyber risk and the vulnerabilities, we would have to compose a plan and implement suggestions of risk evaluation.

SCADA Application

In conclusion, Risk mitigation involves human factor, like stated once before human factor can obtain data from SCADA systems and even change some things. Human factor data can place automations and facilitate fixes just in case some were to happen to the infrastructure. SCADA systems before installation are required to have a recovery mechanism, so overtime there will be a decrease in some of the cybercrime that happens. As result of more threats emerging modifications to the system will continue to happen in order to mitigate these threats.

References

"One Flaw Too Many: Vulnerabilities in SCADA Systems." *One Flaw Too Many: Vulnerabilities in SCADA Systems - Security News - Trend Micro MY*, https://www.trendmicro.com/vinfo/my/security/news/vulnerabilities-and-exploits/one-flaw-too-many-vulnerabilities-in-scada-systems.

"What Is a Supervisory Control and Data Acquisition System?" *What Is SCADA?*, https://www.dpstele.com/scada/what-is.php.

Staff, Editorial, et al. "What Is SCADA System ? - Basics of SCADA - InstrumentationTools." *Inst Tools*, 17 Sept. 2022, https://instrumentationtools.com/scada-system/.