Name: Shannon Harris

Date: March 24, 2024

The SCADA Systems

SCADA Systems are an essential necessity in the industrial and manufacturing world. These beautiful systems provide great outcomes but can also be complex and pose disadvantages.

Vulnerabilities

The SCADA systems used today are packed with technology. These systems are just like any other computer network. They are very important to controlling lots of the nation's needs like electricity, gas, water etc. These networks face everyday vulnerabilities and are at risk of cyberattacks. As SCADA systems become more advanced, they are often prone to more risk and vulnerabilities. One of the main vulnerabilities of these systems is the lack of monitoring. Many of the systems often lack an active network within the system. This makes it difficult to detect when there is the possibility of suspicious activity. If there is some activity happening and no detection systems are more open to an cyberattack.

Another vulnerability that is seen is not properly updating the systems. Most of these systems are designed to control and keep things at certain levels. In turn constant updates to both hardware

and software are needed. This is often becoming an issue and is overlooked and can cause unwanted hiccups. This will also leave an opportunity for hackers to get into the system.

Studies show that a lot of employee personnel are not completely familiar enough with SCADA systems. A lot of the managers don't fully understand how the traffic, data analysis and other technical things work over the network. The more advanced that systems become the more knowledge is needed. Companies will need the proper knowledge or team in place for these systems to stay running properly. This can cause a delay in information and create a possible gateway for cyber threats to happen if not knowledgeable on network part of systems.

There is also a common issue found in authentication processes. This is designed to help keep SCADA systems safe. Passwords are often weak or poorly chosen. Some authentication methods are not strong enough to keep out threats. Companies are at times unaware of the risk that comes along with password safety and frequently share usernames and passwords. Overtime it can put the systems at risk or threat to become compromised.

Mitigating Risk

These systems in today's time should be designed with the capabilities to prevent risk and threats to the critical infrastructure. One way to mitigate these risks is network segmentation which isolates the system from the rest of the internet. Network segmentation creates barriers that prevent unauthorized access or communication between zones. Firewalls, VPNs, and other security measures can be used to protect the network and minimize unwanted access. Systems

that require multi-factor authentication can also help protect against unauthorized entrance. Another addition to help mitigates risk is management of patches. Keeping the SCADA system updated with the latest patches. This will help to stay secure against vulnerabilities and exploits.

Monitoring and detection are a system that is very important to protection of critical infrastructure. This needs to involve collecting, analyzing, and reporting data from system logs. Also, any data from sensors, alarms, and any other indicators of concerning activities. Companies can use intrusion prevention systems (IPS) or intrusion detection systems (IDS). These systems work on a constant schedule to help detect any suspicious activity. Incident response is vital to the overall protection of the SCADA systems. Having an incident response plan in place will help in the event of an attack. The plan will layout the process of how reduce damages and what to do to stay operational.

Although advanced technology has come to make life easier for people and companies to stay in business and keep up with the demand of needs. The SCADA systems are a major asset to making that possible around the clock. The integration of all the advanced technology also comes with errors and technical issues at times. Companies must ensure they implement and develop the best systems to protect against intrusion. Cyberattacks happen a lot more now than ever before with the increase in technological development in the workforce. Systems can easily become vulnerable with the use of the network and internet. With the correct applications in the SCADA systems and understanding of knowledge these systems can continue to work miracles and save time and cost.

References

Works Cited

assisgment, A. f. (2024, March 24). *SCADA Systems.* Retrieved from http://www.scadasystems.net

community, A. a. (2023, April 16). *How do you secure your SCADA system from cyberattacks.* Retrieved from https://www.linkedin.com

SCADA systems and their vulnerabilities . (2024, 03 24). Retrieved from https://www.secpoint.com