Olivia Woodward

CYSE 200T

11/5/23

SCADA Systems and Their Vulnerabilities

This write-up defines SCADA systems and their common exploits. Along with that, explains the mitigations to prevent these exploits.

SCADA Systems

According to scadasystems.net (2023), SCADA (Supervisory Control and Data Acquisition) is a system used in industry facilities to control their processes. The system is made up of 3 main components: a Human Machine Interface (HMI), a Remote Terminal Unit (RTU), a Programmable Logic Controller (PLC), and a Supervisory Station. All together, these components can monitor processes of facilities and industries easily.

Common Vulnerabilities

Considering that this system holds big responsibility over significant systems such as airports, water treatment, and manufacturing, scadasystems.net (2023) claims, the security and reliability is assumed exceptional. However, the Ponemon Institute (2011) claims that 67% of energy organizations do not use “state

of the art" tech to minimize SCADA risks; 41% believe their security is not sufficient in risk management.

One of the most common risks is data breaches. In the same Ponemon (2011) study, 48% of the respondents' organizations claim to have had only one data breach,13% say they have had 2 to 5 breaches, and 9% with over 5 breaches. How are these data breaches achieved? Ponemon claims that respondents responded that the top three threats that affect the organization are: Negligent insiders, insecure web applications, and system glitches.

Mitigations

Overall, it seems that the real problem isn't the problem with SCADA itself, but the organizations that use it are not taking employee training, security, and system maintenance into account.

Employee Training

There should be a focus on employee training because negligent insiders are the top threat. Employee training in onboarding, bi-monthly retraining, and annual tests make sure that the employees' duties are solid. There is no need to worry about negligence if it is something that employees start to do intrinsically. However, if push comes to shove, it is reasonable to establish discipline measures or have those refreshed during training to deter negligence.

Security

Insecure web applications are the second biggest problem, so there are plenty of factors to consider. For example, if the application is one the organization made on its own, maybe it would be better to start outsourcing that application to make management better; it also can put more focus into cybersecurity of the website without having to worry about developing it themselves. If the application is already being outsourced, it is time for the organization to start consulting with the outsource its cybersecurity options. An alternative would be to start researching other outsourcing companies that have solid security options.

System Maintenance

System glitches being the third biggest threat goes hand in hand with negligent insiders. If employees are ignorant to their tasks, that leads to analysts and administrators leaving bugs that need to be tackled untouched. Along with employee training, the organization could invest into an application that tracks these sorts of issues if they haven't already. Instead of having employees pick their way through, which could likely be skipped over by the human eye, the application will monitor it for them telling them the location and possibly priority.

Conclusion

The SCADA systems play a significant role in modern times. From traffic lights to manufacturing, they are an essential part for the human experience to run smoothly in this world of tech. If these systems are not taken care of the results could be detrimental; that is why it is worrying to see so many organizations being neglectful of their systems. Luckily, the solutions are easily implementable for the exploits commonly found. With the right tools, there would be no need to stress over these systems.

References

Ponemon Institute. (2011). *State of IT Security: Study of Utilities & Energy Companies.* https://www.ponemon.org/local/upload/file/Q1_Labs%20_WP_FINAL_3.pdf.

SCADA Systems. (2023). SCADA Systems. https://www.scadasystems.net/.