Jose Gonzalez

11/1/2024

CYSE200T

Professor Hagh

SCADA and their role in CIS vulnerability mitigation

What is SCADA

As said by Peter Loshin “SCADA (supervisory control and data acquisition) is a category of software applications for controlling industrial processes, which is the gathering of data in Real Time from remote locations in order to control equipment and conditions” (Loshin, 2021). These SCADA systems are used in many industrial settings like oil and gas pipelines, production lines, food processing plants and many other settings. As said by the website “scadasystems.net “SCADA refers to ICS (industrial control systems) used to control infrastructure processes, facility-based processes, or industrial processes” (SCADA systems, 2018). SCADA systems are made up of many different systems like PLC, RTU and Human Machine Interface. While SCADA systems may seem like they are reliable and will work for many years without any issues, that is completely wrong.

Vulnerabilities

Many SCADA-based systems are being investigated as many question if they pose a considerable risk of being targeted by cyberterrorism/cyberwarfare attacks (SCADA systems, 2018). Many of these risks are presented due to a lack of cybersecurity and updated software. As

said by Stephan Venter on the blog “5 Cybersecurity Weaknesses Critical Infrastructure Owners Should Guard Against” “...older operational technology (OT) systems with insufficient user and system authentication, data authenticity verification, or data integrity checking features that can allow attackers uncontrolled access” (Venter, 2023). By not updating and using older operational technology, it allows bad actors and hackers to gain access to these important systems and allows them to damage equipment or completely stop industries like oil and water purification. Stephan Venter also says, “Just like cybersecurity in any other organization, human weaknesses are exploited by threat actors targeting critical infrastructure” (Venter, 2023). By not having employees and workers understand the role they play in their own cybersecurity as well as the company’s cybersecurity, they lead the way for the exploitation of their information and data. With these vulnerabilities becoming more prevalent as time goes on, there are many mitigation strategies taking place to reduce them.

Mitigating Vulnerabilities

Some examples of mitigating vulnerability said by Morgan Siggins are “Implement the security features provided by your devices, Manage authorizations and user accounts, and Have system backups and disaster recovery plans” (Siggins, 2020). By adding these mitigations, it allows for safer SCADA systems. Implementation of policies that employees must follow such as using complex passwords on SCADA systems may also for better cybersecurity for any other technology used in the company. Another way is presented by the website “scadasystems.net” “SCADA vendors are addressing these risks by developing specialized industrial VPN and firewall solutions for SCADA networks that are based on TCP/IP” (SCADA, systems 2018).

Conclusion

While SCADA systems are something useful that helps many industries like oil and gas pipelines and food processing, they also provide and enable lots of vulnerabilities that can be taken advantage of by threat actors and cybercriminals. By understanding the vulnerabilities that SCADA systems bring, many mitigation strategies are presented. Strategies like the use of complex passwords, managing who has access to SCADA systems, and other policies can allow for safer uses of these systems. By protecting these systems, it allows citizens and employees to rest easy knowing that their needs that SCADA systems provide will be safe and sound.

Sources

Loshin, P. (2021, December 16). *What is SCADA (supervisory control and data acquisition)?*. WhatIs. https://www.techtarget.com/whatis/definition/SCADA-supervisory-control-and-data-acquisition

SCADA systems. SCADA Systems. (2018, July 25). https://www.scadasystems.net/

Siggins, M. (2020, May 28). *Where can vulnerabilities be found in SCADA systems?*. DPS Telecom. https://www.dpstele.com/blog/where-can-vulnerabilities-be-found-in-scada-systems.php

Venter, S. (2023, May 16). *5 cybersecurity weaknesses critical infrastructure owners should guard against*. TuxCare. https://tuxcare.com/blog/5-cybersecurity-weaknesses-critical-infrastructure-owners-should-guard-against/#poor