Amyah Robinson

CYSE 200T

November 12, 2025

Professor Duvall

Human and Third-Party Threats to SCADA Systems

BLUF: Reducing human error and managing third party risks decreases the threats to SCADA systems.

Human Threats

Humans are a big threat when it comes to maintaining security in an organization. Many cybersecurity incidents are caused by human error, negligence, and insider threats. In Scada systems human error can cause major cyber security attacks if protocols aren't being followed. To prevent these attacks there needs to be regular cybersecurity training, access controlling, and monitoring activity in and out of the system. SCADA vendors use specialized VPN and firewall solutions to protect the network. To keep SCADA systems secure human awareness and accountability needs to be prioritized.

Supply Chain and Third-Party Risk

When it comes to water treatment, wastewater, wind farms, etc. , they all rely on systems that may be serviced by a third party. Examples of third-party services would be hardware such as sensors and software such as system applications. Third party risk and prevention strategies are different for every country all over the world.[1] These third-party services can introduce vulnerabilities when it comes to protecting cybersecurity of the organization. If a supplier/ third-party's product contains vulnerabilities in security this will weaken the whole organizations security. Ways to decrease the chances of vulnerabilities is to test systems before implementing them into the organization. SCADA Hardware will be important in controlling security risk. Using firewalls will prevent unauthorized access and monitor traffic for unusual activity. The supervisory station will provide continuous monitoring and control over all systems. Overseeing third party components and enforcing security policy will keep SCADA systems safe.

Conclusion: Protecting SCADA systems requires both human responsibly/supervision and technological monitoring. With human error being a big threat to security it is important to follow cybersecurity guidelines. Testing third party hardware before implementation lowers chances of an attack. By prioritizing security, business will be able to maintain the integrity and safety of the systems.

Source

Levy, M. (2024, August 25). Understand Third-Party OT Risks and Learn The Best OT Security. Scadafence.com; SCADAfence. https://blog.scadafence.com/understand-third-party-ot-risks-how-tackle