Levi Reeves

11-09-20

Vulnerabilities in Critical Infrastructure and Mitigations

In this write up we will discuss some potential risks, threats, and vulnerabilities in reference to critical infrastructure. Critical infrastructures include sewage and waste systems, steam and nuclear plants, wind farms, refineries, etc. This make up of infrastructure is referred to as SCADA, or Supervisory and data acquisition. We will also discuss how SCADA applications can be used to mitigate these vulnerabilities.

Vulnerabilities

The two major security issues concerning SCADA are unauthorized access to ICS software systems and ability of threat actors to access packets to network segments. Other problems include poor credentials management, subpar firewalls, flawed network design, poor event monitoring, and even poor physical security. This is critical because many of these systems have multiple failsafes in place that kick in case something malfunctions. This was the case with a Saudi Arabian chemical plant in 2017. The system was compromised and infected with a malicious code known as Triton. The hackers responsible for the attack were able to gain access to a physical work station and infect the plant's safety instrumented systems. The same systems used to shut the plant down automatically if unsafe conditions were to occur. It is evident why keeping these systems secure is so important.

Mitigations

As we all know the responsibility of security falls upon the organization as a whole. Some ideas to help prevent these issues from occurring are education of employees, constantly testing for security vulnerabilities, routine security patches, conduct third party audits, implement strong encryption methods, restrict user privilege by assigning role-based access control, and of course to change all default passwords. All of these preventatives will be a result of creating a culture centered on security. For example, Microsoft has done this by requiring all new code to pass a series of test before being allowed for commercial use. Inasmuch, the users working on the code were tested to ensure that they had to skills to write secure code. Another key factor to remember is that ICS is ever changing much like cyber security and there is no one fix all patch. Therefore, we must remain vigilant and frequently adapt to changing needs for security.

Conclusion

Upon investigation into ICS and SCADA we can see that many of the same principles that apply to regular cyber security apply to these systems as well. Ultimately, it is us to the user and the company to implement strong security protocols in order to protect assets and lives.

WORKS CITED

Nelson, T. (2011, May). Common Cybersecurity Vulnerabilities in Industrial Control Systems [PDF]. Department of Homeland Security.

SCADA Systems. (n.d.). Retrieved November 09, 2020, from http://www.scadasystems.net/