Dez Johnson

11/5/2022

SCADA Systems

Supervisory Control and Data Acquisition, Also known as SCADA, is a software application that is used to control infrastructure processing systems. Critical infrastructures are very vulnerable to cyber attacks due to the fact they are dependent on computer systems to function. SCADA systems understand this and have Attack Prevention Strategies

Critical Infrastructure Vulnerabilities

Critical Infrastructure is very vulnerable to cyber attacks due to facility dependencies on computer systems. Three vulnerabilities associated with critical infrastructures are Network segmentation, DDoS attacks, and Malware Attacks. Network segmentation is the division of a network into many segments that then allow the network admin to control the traffic flow. When there is not any network segmentation, people pretending gain access inside an organization's network to valuable assets (Laremenko). DDoS attacks, attack an organization's Public Cloud Infrastructure and affect the availability of things in the cloud. This can happen before anyone can even detect it and the attacks can blend in with legitimate users (Laremenko). Malware attacks are when malicious software is used to harm or exploit a device or network. Malware attacks can result in "data loss, cripple devices, and shut administrators out of systems in return for an oftentimes large ransom sum" (Laremenko).

SCADA Attack Prevention Strategies

SCADA understands that the threats of cyber-attacks are greater than ever. With that, two of the SCADA attacks prevention strategies are, Secure LAN and Physical Site Security. Secure LAN or local area network involves securing communications transport. With securing LAN, you would "deploy RTUs capable of working with both LAN and fault-tolerant dedicated serial lines. You can utilize the same RTU devices to provide SCADA security at all of your sites" (Siggins). Protecting the SCADA network also involves Physical site Security. This means Making sure that physical resources are protected, as well as, "ensuring that your hardware-based security devices are always up and running" (Siggins). This doesn't mean old lock and key systems for security, rather a single proxy card or key code can be used to let users access sites when they need. Other things that can be used for physical security are Entry Control Units (ECU) at every door, Cameras and Notifications, and Security-Enhanced Devices.

Conclusion

In conclusion, as critical infrastructures develop more, so do the threats that come along with them. Which makes it very vulnerable to attacks, this is why it is very important that an organization is aware of these threats and takes the steps necessary to protect itself from an attack.

References

Iaremenko, Andrey. "5 Threats to Critical Infrastructure Security." HUB Security, 31 Oct. 2022, hubsecurity.com/blog/critical-infrastructure-security/5-threats-to-critical-infrastructure-security/.

Siggins, Morgana. "SCADA Attack Prevention Strategies." DPS Telecom, 14 Jan. 2022, www.dpstele.com/blog/scada-attack-prevention.php#:~:text=SCADA%20systems%20monitor%20and%20control,of%20bogus%20or%20harmful%20traffic.