Emmanuel Asare

CYSE 200

Vulnerabilities associated with Critical Infrastructure Systems

Critical infrastructure systems, like power plants, water treatments and transportation. Critical infrastructure systems are needed for cities, the economy and using it in our lives. But these allow us to be vulnerable to threats like cyber attacks, natural disasters etc. Supervisory Control and Data Acquisition systems are needed to protect infrastructure. SCADA is used to check and control power grids, oils, gas and water treatment. SCADA collects real data from sensors and devices and the data is analyzed and used to control these systems.

What is SCADA Systems

SCADA systems are used in alarms and also have digital points. Even though SCADA systems can help mitigate potential risks it can create its own vulnerabilities. With SCADA systems people operating the systems can detect abnormalities and respond to them. SCADA systems can deal with remote management and reduce the need to physically access infrastructure. SCADA systems are industrial control that provides control over machinery. In the article “The massive impact of vulnerabilities in critical infrastructure” Micheal Johnson states that “businesses are ramping up their security initiatives and investments to defend and protect, their efforts have largely been siloed, reactive, and lack business context”.

Infrastructure such as energy, water, transportation and healthcare systems are needed for survival. Being able to disable and remove access to these resources poses a threat to a country's economy. Consequences of critical infrastructure attacks can be pretty devastating. If our healthcare or telecommunications, or financial markets are attacked it can cause our daily activities to be put on pause.

Security threats associated with SCADA

Even though people believe that SCADA networks are safe they are easily vulnerable. One of the threats is when someone gets unauthorized access to software systems, it can be human access or viruses. Potential vulnerabilities are the systems are connected to the internet and other networks. Since SCADA systems are connected to other networks it can be easier for attackers to gain access to multiple systems, some systems might not have great security resources which can cause the systems to not be able to handle attacks.

Works Cited

"One Flaw Too Many: Vulnerabilities in SCADA Systems." *Security News*, https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/one-flaw-too-many-vulnerabilities-in-scada-systems.

Labus, Helga. "The Massive Impact of Vulnerabilities in Critical Infrastructure." *Help Net Security*, 11 Mar. 2022, https://www.helpnetsecurity.com/2022/03/15/critical-infrastructure-security/.