Reed Wilhelm

CYSE 200T

Professer Kirkpatrick

11/6/2022

The Security Risks within Critical Infrastructure

As more critical infrastructures are integrated with networks and the internet, many systems can be exposed to cyberthreats, the consequences of which could be catastrophic. Supervisory control and data acquisition systems, or SCADA, can help mitigate these cyberthreats.

Threats to Critical Infrastructure

Whether its water treatment, power grids, or gas pipelines, critical infrastructure has always been a target for attacks. However now with more and more critical systems being integrated online, this opens the door for hackers and cybercriminals tamper with systems which could have catastrophic consequences. To truly understand how bad a cyber attack on critical infrastructure can be it's important to look at some of the attacks that have already happened and the consequences of those attacks.

Cyber Attacks on Critical Infrastructure

One of the most recent cyber attacks that comes to mind is the attack on the Colonial Pipeline in 2021. The attackers stole over one hundred gigabytes of data over a two hour window, after the theft the hackers infected the Colonial Pipeline network with ransomware which affected many of their online systems including billing and accounting. The Colonial Pipeline ended up shutting down to prevent the ransomeware spreading, until they paid the attacking group to get the

decryption key to regain control of their systems (Kerner). Another example of an attack on critical infrastructure came in 2021 when a hacker attempted to poison water at a treatment plant in part of the San Fransisco Bay Area, the hacker used a former employees login credentials to access their TeamViewer account, a program that lets users remotely control their computers. After logging in the hacker deleted some of the plants programs that were essential to treat drinking water, the attack wasn't discover until the next day but luckily, "No failures were reported as a result of this incident, and no individuals in the city reported illness from water-related failures," (Collier). There was another almost identical attack on a water treatment plant in Florida, where the attacker used the same method of gaining access to a TeamViewer account and this time raise the level of lye in the drinking water to poisonous amounts, however this time employees at the treatment facility caught it right away so no harm was done (Bing).

Mitigation

Cybersecurity at many critical infrastructure sites can often be quite lacking, with one cybersecurity consultant saying, "If you could imagine a community center being run by two old guys who are plumbers, that's your average water plant," (Collier). However these recent attacks have helped to bring light to the situation, with steps now being taken to improve cybersecurity, or at lest improve detection for cyberattacks. With more companies offering SCADA systems to assist in monitoring and correcting issues on the fly.

The Basics of SCADA

SCADA essentially is a type of centralized control system which is often used both for controlling and monitoring things like critical infrastructure and other large industrial facilities. The majority of control actions that are a part of SCADA are preformed automatically by remote

terminal units (RTUs) or by programable logic controllers (PLCs). These remote terminal units can PLCs can be used to send signals to a user interface which shows the status of the given facilities functions. SCADA systems also traditionally run on their own dedicated networks which can help prevent the information it feeds from being tampered with. SCADA systems tend to be built with a lot of redundancies, so that in the event that some of the monitoring systems fail, there will be a back up that can be used until the issue is fixed. Overall, one of the main functions of SCADA is to essentially set off an alarm, most of its RTUs and PLCs main goals is to simply detect if its under any type of threat or if anything is out of the ordinary, and set off an alarm when its encounters irregularities.

Conclusion

Overall cybersecurity on critical infrastructure is improving, however it still has a long way to go as there's no defined limit to what a group of hackers are capable to doing. On the positive side through, systems like SCADA, while not cybersecurity its self, can be used effectively in tandem with standard cybersecurity measures to help monitor and guard critical infrastructure from threats. As one of its main purposes is to detect anomalies within the system, and while it may not directly prevent it, it can expose when something is under a cyber attack meaning that the issue can be dealt with much sooner.

Sources

Bing, Cristopher “Hackers try to contaminate Florida town’s water supple through computer breach” *Reuters.* Feb 8, 2021. https://www.reuters.com/article/us-usa-cyber-florida-idUSKBN2A82FV

Collier, Kevin “50,000 security disaster waiting to happen: The problem of America’s water supplies” *NBC News.* June 17, 2021. https://www.nbcnews.com/tech/security/hacker-tried-poison-calif-water-supply-was-easy-entering-password-rcna1206

Kerner, Sean Michael “Colonial Pipeline hack explained: Everything you need to know” *TechTarget.* Apr 26 2022. https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know

“SCADA Systems” http://www.scadasystems.net (this is the original article from canvas, wasn’t really sure how to cite it as it lists no authors, date, or additional information.)