Introduction

Cybersecurity as a purpose is not overpublicized, and so long as systems are connected to the internet, they are vulnerable to attacks. Any modern digital industrial control system (ICS) in use is presumably connected to the internet in some form, and is therefore vulnerable. Thus, it would make sense to assess the ICS as well as the entire operation for vulnerabilities. Once vulnerabilities are identified, they can oftentimes be fixed; neglecting to prepare for attacks would only open the firm up to further damage. Preparation is mitigation, and the following paper will address how to best assess and improve cybersecurity practices with digital ICS.

How Traditional Control Systems are Deployed (NIST, 2015)

ICS are deployed to help control operations in complex systems. These systems are highly interconnected and mutually dependent. Additionally, these systems are considered critically important since without them people would not have electricity (which, in modern times, is considered essential).

ICS were initially isolated systems that were in physically secured areas. Connecting complex focused systems to the internet did not offer any discernable benefit when these were introduced, however as technology has evolved so have needs. ICS systems thus became feasible to become digitally based.

Presently, these systems are beginning to be linked with remote access, IoT and other IT functions. By introducing closed systems to networks these closed systems become vulnerable to attacks. Connecting these systems to networks has many advantages including reduced labor

costs and a better ability to scale operations (with more generators). Despite these benefits, in general: the more moving parts an interconnected system has, the more point of failure that system has. These points of failure can be exploited by hackers, and then exploited for monetary benefit via ransoms or blackmail.

Current Events and Notable Control System Breaches (Cornelius, 2021; Wintour, 2021)

According to a recent study, one-third of ICS were targeted for malicious activity. Thus, electric utility companies that use these systems have a 33% chance of being targeted for a cyber-attack. There have been significant breaches at many nuclear power plants; given that these power plants have the potential to melt down and cause widespread issues, protecting these assets should be an absolute priority for not only profits but the public good.

Recently, Israel targeted an Iranian nuclear powerplant with a cyber-attack on an ICS. This powerplant is Iran's main Uranium enrichment facility, and the attack set back progress by nine months' worth of progress. 9 months' worth of the wages paid, the loss in public confidence of the powerplant, a decrease in national readiness and the cost of doing business were lost from a security vulnerability in an ICS system. One single cyber-attack decreased the energy output and weapons capability of a developed nation considerably; thus, electric utility providers should be proactive at mitigating threats such as these.

Threat Brief (NIST, 2015)

Based on the current environment, ICS are vulnerable to cyber-attacks. In fact, ICS may be extremely vulnerable given the devastation that going without these systems can cause. Hostile

nations might attack such utility providers as described in the previous section, or even as a prelude to an invasion. Since ICS are prime targets, every avenue should be taken to mitigate the damage that can be done from a security breach.

Best Practices for Securing Control Systems (NIST, 2015)

ICS should be secured by the following procedures:

1. Access control should be restricted as needed to lower the amount of possible threats
    a. Multifactor authentication can stop breaches (via compromised credentials)
    b. Restricting modification of data via permissions can preserve data integrity
2. Security personnel should be posted at points vulnerable to local attacks
    a. ICS attacks used to be entirely local, and attacks could still originate locally
3. Individual components should be regularly patched and inspected for flaws
    a. Out-of-date technology is most vulnerable to attacks
4. System backups and restoration procedures should be readily available to resume ops
    a. Advance planning leads to better, more thorough decision-making

Penetration Test: Goals, Process and Feedback (*Phases of Penetration Testing*, 2021)

The rules of engagement for penetration testing for an electric utility provider must be sensitive to the needs of citizens to electric utilities; thus, such a test should be only conducted on specific parts of the system at times when full-system operation is not needed. For example, an electric utility provider should not have a penetration test right before a hurricane makes landfall near its facility. Additionally, all systems must not be attacked at once to ensure that systems can

continue to supply power to communities without stopping. With these considerations in mind, I outline what a successful penetration test would look like for an electric utility provider's ICS.

Penetration tests have 5 phases. An effective penetration test would include the following:

1. Recon: information about the ICS and the provider would be collected
2. Scanning: provider's computers are scanned for vulnerabilities
3. Gaining Access: testers try to gain access to closed systems and exploit vulnerabilities
4. Maintaining Access: testers create backdoors to facilitate further attacks
5. Covering Tracks: testers erase evidence that there was an attack to not raise security

The success of an electric utility provider in encouraging effective infosec and practicing effective controls would be gauged by each step in this process. If a penetration tester is able to find information about an electric utility that leads to the exact types of hardware and software used, then perhaps employees should be trained more to not share information such as this. Additionally, if a tester is able to execute all 5 steps, then perhaps ICS are extremely vulnerable and need to be taken offline to address issues immediately. A firms' level of success at mitigating such threats in a simulated sense is very effective at mitigating actual threats when they present themselves (which is 33% likely every year).

References

Cornelius, J. (2021, September 22). *Why Are Industrial Control System Attacks Increasing?* Infosecurity Magazine. Retrieved December 12, 2021, from https://www.infosecurity-magazine.com/opinions/why-industrial-attacks-increasing/

NIST. (2015, May). *Guide to Industrial Control System Security*. Retrieved December 12, 2021, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Phases of Penetration Testing. (2021, April 25). All About Testing. Retrieved December 12, 2021, from https://allabouttesting.org/phases-of-penetration-testing/

Wintour, P. (2021, April 13). *Natanz nuclear plant attack 'will set back Iran's programme by nine months.'* The Guardian. Retrieved December 12, 2021, from https://www.theguardian.com/world/2021/apr/12/iran-blames-israel-attack-natanz-nuclear-plant