Jordan Sustarsic

IT 200T

Professor Duvall

April 23rd, 2023

Analytical Paper

Introduction

Cybersecurity has emerged as a crucial component of contemporary civilization in the linked world of today. In order to protect people and organizations against online dangers, cybersecurity-related technical systems have become increasingly important as people rely more and more on technology in all facets of their lives. These systems have substantial social significance and consequence. The way these systems are developed and put into use could have a significant impact on civil liberties, national security, and even privacy. In order to build technical systems connected to cybersecurity in a way that combines the need for security with the preservation of individual rights and freedoms, it is crucial to comprehend the social consequences of such systems.

SCADA Systems

Systems that are crucial to a society's ability to function, both physically and virtually, are referred to as critical infrastructure systems. Transportation, electricity, water supply, healthcare, and communication systems are some of these systems. Despite the fact that these systems have typically been run in solitary settings, the growing tendency toward the integration of operational technology (OT) and information technology (IT) has rendered them

more susceptible to cyber-attacks.

One of the primary vulnerabilities associated with critical infrastructure systems is their interconnectedness. A successful attack on one system can have a cascading effect on other systems, leading to a domino effect. For example, a cyber-attack on a power grid could lead to a blackout that disrupts communication systems, transportation systems, and even the healthcare system. In addition, these systems are often managed by aging legacy systems that have not been designed with modern security threats in mind, making them more susceptible to cyber-attacks.

Applications for supervisory control and data acquisition, or SCADA, are essential for reducing the hazards posed by critical infrastructure systems. Critical infrastructure systems are monitored and controlled by SCADA systems, which also provide real-time data on the performance and status of these systems. Sensors, remote terminal units (RTUs), and a central control system are the typical three parts of them.

The capability of SCADA systems to identify anomalies in the behavior of crucial infrastructure systems is one of its important characteristics. These irregularities can be a sign of a cyberattack or another kind of security risk. For instance, a sudden increase in a nuclear power plant's temperature could be a sign of a malfunction or cyberattack. Such anomalies can be found by SCADA systems, which can then inform operators so they can take appropriate action before a more major incident happens.

Security measures like firewalls, intrusion detection systems, and access controls can also be implemented using SCADA systems. SCADA programs can aid in preventing unwanted access and cyber-attacks by limiting access to vital infrastructure systems and keeping an eye on

activities on these systems.

The CIA Triad

The CIA triad, also known as confidentiality, integrity, and availability, is a concept created to direct information security policies inside a company. This is one of the fundamental instruments used in the information security world.

Confidentiality is the first letter in the CIA triad. “It is roughly referred as privacy” (Chai). Measures for maintaining confidentiality are intended to guard against unauthorized access to sensitive data. Data is frequently categorized based on the scope and nature of the harm that could result from it getting into the wrong hands (Chai). These categories can then be used to implement more or less strict measures.

Sometimes safeguarding data confidentiality involves special training for those privy to sensitive documents. Training can help familiarize authorized people with risk factors and how to guard against them (Chai). Further aspects of training may include strong passwords and password-related best practices and information about social engineering methods to prevent users from bending data-handling rules with good intentions and potentially disastrous results (Chai).

Integrity is the upkeep of data throughout its full lifecycle in terms of consistency, accuracy, and dependability (Chai). Data cannot be changed while in transit, and measures must be taken to prevent unauthorized parties from changing the data (Chai). These safeguards include user access restrictions and file permissions (Chai). Version control can be used to stop authorized users from making mistakes or accidentally deleting things (Chai). Organizations

must also provide some method for detecting any data changes that can happen from non-human events like an electromagnetic pulse, natural disaster, or server crash (Chai). Checksums, including cryptographic checksums, may be used in data to verify its integrity; redundancies or backups must also be accessible in order to restore the impacted data to its original state(Chai).

Information should always be regularly and easily available to authorized persons. This entails keeping up with the systems, hardware, and technical infrastructure that store and show the data (Chai). The best ways to do this are to keep all hardware under strict maintenance, fix any hardware issues as soon as they arise, and maintain a stable OS environment free of software conflicts (Chai). “Additionally, it's critical to stay up to date on all required system upgrades” (Chai). Equally crucial strategies include ensuring appropriate communication capacity and avoiding bottlenecks from occurring (Chai). “When hardware problems do arise, redundancy, failover, RAID, and even high-availability clusters can help to prevent major repercussions” (Chai).

The Human Factor of Cybersecurity

“Cybercrime has been constructed as a national threat, and cybersecurity is the tool intended to provide protection from this threat” (Payne). That being said, weak cybersecurity practices can also be seen as a cyber security threat (Payne). As a Chief Information Security Officer, I would prioritize investing in training and education programs for my team, as I believe that human error is a significant contributor to cyber threats. Investing in training programs can help ensure that employees are aware of best practices for cybersecurity, such as how to identify and respond to phishing attacks, how to use secure passwords, and how to keep software and systems up to date.

To keep staff interested and educated on the most recent cybersecurity dangers and best practices, I would also invest in ongoing cybersecurity awareness initiatives. This might include frequent emails, newsletters, and office posters.

Technology for cybersecurity is also essential, but it can be expensive to set up and maintain. As a result, I would give security solutions that have the biggest effects on our firm top priority when investing. For instance, I would think about investing in security information and event management (SIEM) and intrusion detection and prevention (IDS/IPS) systems, which can assist in real-time detection and response to cyber-attacks.

Ultimately, I would want to find a balance between funding my team's training and education programs and funding the appropriate security solutions to safeguard our company. By doing this, even with limited resources, I can make sure that my team gets the information and resources they need to effectively mitigate cyber threats.

Conclusion

In conclusion, critical infrastructure systems are vulnerable to a range of cyber threats, which can have severe consequences for society. SCADA applications play a crucial role in mitigating these risks by providing real-time monitoring and control of critical infrastructure systems, detecting anomalies in system behavior, and implementing security measures to prevent unauthorized access and cyber-attacks. The CIA triad and authentication and authorization are also crucial information security concepts that administers employ to safeguard systems and data. This just goes to show how much cyber-technology has affected the world of today. There are a lot of systems and even people that rely on this technology to

work and serve its intended purpose.

Works Cited

"Authentication vs. Authorization: What's the Difference?" *OneLogin*, https://www.onelogin.com/learn/authentication-vs-authorization#:~:text=Authentication%20verifies%20the%20identity%20of,the%20security%20of%20a%20system. Accessed 12 Feb 2023.

Chai, Wesley. "What is the CIA Triad? Definition, Explanation, Examples." 28 June 2022, https://drive.google.com/file/d/1898r4pGpKHN6bmKcwlxPdVZpCC6Moy8l/view.

Accessed 12 Feb 2023.

Payne, Brian. “White-Collar Cybercrime: White-Collar Crime, Cybercrime, or Both?”. *Criminology, Criminal Justice, Law & Society,* Volume 19, Issue 3, Pages 16-32, drive.google.com/file/d/1id2JHiAfyUjuKj0necP4AKE3gZFrD7__/view. Accessed April 1st, 2023.

“SCADA Systems.” *SCADA Systems*, http://www.scadasystems.net/. Accessed 17 March 2023.