Ryan Jackson
4/20/23
CYSE200T
Analytical Paper

Cybersecurity and Balancing Human Factors in the Field

Introduction

Cybersecurity is an ever-growing field. This is especially the case with recent advancements in technology. Cybersecurity is the practice of protecting systems, networks, and sensitive information from attacks, whether physical or digital. In this day in age, it is important to combat threats against networks, software, hardware, whether those threats are internal or external. In this paper, I will be explaining the foundation of cybersecurity and the balancing act that must occur between technology and human intervention.

The Foundation of Cybersecurity

Cybersecurity has a foundational principle called the CIA triad. The CIA triad is a widely accepted model and principle in information security. Together, confidentiality, integrity and availability are considered the three most important concepts within the field of cybersecurity. Confidentiality is essentially privacy, meaning only authorized users are able to access the data. It is a set of rules that puts limits on access to information. Integrity means the data consists of trustworthy information that hasn't been tampered with. Availability means information should be readily accessible for

those particular authorized parties. Authentication is the process of verifying an individual. Authorization is the process of verifying what the individual has access to. For instance, if you were to fly on a plane, you show your identification to authenticate your identity. Then the flight attendant will authorize you to board the plane and allow access for you to take the flight.

SCADA; An example of Human Intervention

SCADA means Supervisory Control and Data Acquisition. SCADA is a system with the goal of monitoring and controlling infrastructure processes (SCADA Systems, 2023). According to the National Institute of Standards and Technology (NIST), SCADA is a system that is capable of gathering and processing data and then applying operational controls over long distances (NIST, *Supervisory Control and Data Acquisition*). Typical uses include power transmission and distribution and pipeline systems. SCADA was designed for the unique communication challenges (e.g., delays, data integrity) posed by the various media that must be used, such as phone lines, microwave, and satellite. Usually shared rather than dedicated. Industries where SCADA is used consist of water management systems, electric power, airports, traffic signals, transit/transportation systems, and more. Threats can be completely naturally occurring or accidental, however, they could also rise through ill intent. Any one of these sets of infrastructures could fail or falter in any way at any time, though, intentional attacks occur as well. SCADA systems are imperative as it collects and processes real-time data. Critical infrastructure going digital could increase vulnerabilities. Energy,

healthcare, water, communication, financials, and transportation could all be affected. If an attacker were to gain control over these systems and networks, it could lead to major consequences. SCADA can be easily configured for a vast number of applications with varying needs in an effort to mitigate these vulnerabilities and risks. In conclusion, being able to see real-time data allows fixes to take place, both manually and automated. SCADA systems are crucial for industrial organizations since they help to maintain efficiency, process data for smarter decisions, and communicate system issues to help mitigate downtime. SCADA architecture relies on programmable logic controllers (PLCs) or remote terminal units (RTUs). These help with communication between machines, sensors, and computers with SCADA software. The software processes, distributes, and displays data. Operators must analyze the data to make whatever decision must be made. The operator in this process is simply one instance of balancing act the must take place between humans and technology. The world is advancing rapidly in technology, however, we as a society cannot rely entirely on these advancements without intervention.

Human Intervention and the Balancing Act

The balance between training and cybersecurity technology is very important. I personally would prioritize training. Cybersecurity technology itself is beneficial, however, training within the field should take priority. Lack of training and skillset in

cybersecurity could result in roundabout ways to do work rather than following protocol. More specifically, a lack of training could result in weak passwords, the utilization of unauthorized file-sharing applications, and more. Ensure security awareness training as well. This should include awareness of phishing, spoofing, DoS, malware, and other cyber-attacks. Employers hold a lot of responsibilities in regard to the field of Cybersecurity. The CISO or chief information security officer is an executive responsible for developing procedures, policies, and systems and keeping them well protected from both internal and external threats. To ensure protection many things could be done. Backing up the company's data is one thing. You want to be able to recover information if you experience some sort of cyber incident. This should also be done regularly. Data redundancy is important as it refers to keeping data in multiple places within a database. You could also keep backups over multiple networks. If there are data corruptions or any kind of data loss, you will be prepared. These backups should also be kept up to date. Train employees in keeping both software and hardware security. The baseline teaching of this would be requiring strong passwords. Limit access to data and information among employees. Do not provide one singular employee with access to too vast or all data systems. Access should be given for data based on the job and its requirements. Limit the authority to install or update software. Ensuring and maintaining the availability of systems still would most likely come down to utilizing redundant networks and servers. They can be made available when primary systems break down. The importance of employee training and deviance cannot be overstated. Cyber technology has been great, but has also contributed to workplace deviance, especially in recent times when businesses have gone remote. Certain

employees when left unmonitored may spend company time in wasteful ways. However, regarding remote working, cyber technology is not the only culprit. When working at home, some may simply have other responsibilities, such as children to tend to. Deviance directly related to cyber technology can cause significant damage when dealing with rouge employees. Unethical actions may be more likely to take place when done through cyberspace. Issues like this are made more important when remote working is in play. Systems, networks, and physical hardware may contribute to vulnerabilities when remote that would not have occurred in the workplace. For example, websites that are blocked on-site may not have any hold on an employee when remote. Deviance can easily happen in the workplace.

Conclusion

In conclusion, it is important to combat threats against networks, software, hardware, etc. As stated prior, these threats could be both internal or external, technological or human inflicted. There is and will always be a balancing act between technology and human intervention. As technology advances, society must realize that any form of technological deviance is just as likely to happen. It could even occur more often as it may add a layer of anonymity. Fund allocation should primarily go towards programs and classes for teaching and training employees. Educating employees is and will always be a crucial step in a good business. Teaching about ideal practices can prevent threats. If you were to prioritize the technology, you would still have to ensure

that everybody knows how to utilize the hardware/software to increase productivity. This would be a the most effective way to maintain balance.

Citations

Amos, Z. (2022, April 22). How to balance cybersecurity and Productivity. Cybersecurity Magazine. Retrieved April 2, 2023, from https://cybersecurity-magazine.com/how-to-balance-cybersecurity-and-productivity/?utm_source=rss&utm_medium=rss&utm_campaign=how-to-balance-cybersecurity-and-productivity

NIST. (n.d.). *Supervisory Control and Data Acquisition (SCADA) - glossary: CSRC*. CSRC Content Editor. Retrieved April 21, 2023, from https://csrc.nist.gov/glossary/term/supervisory_control_and_data_acquisition

SCADA - Tech-FAQ. Tech. (2019, April 6). Retrieved March 19, 2023, from https://www.tech-faq.com/scada.html

SCADA systems. SCADA Systems. (n.d.). Retrieved March 19, 2023, from http://www.scadasystems.net/