The Social Meaning and Impact of Cybersecurity-Related Technical Systems

Introduction

As the threat landscape of cyber-attacks continues to evolve, organizations are investing heavily in cybersecurity to protect their valuable information assets. There are many rules and options to follow or listen to when you are following this career. However, there is always a tradeoff between investing in cybersecurity training and additional technology when working within a limited budget.

On the other hand, investing in technology can help organizations stay ahead of the constantly changing threat landscape. Technology can provide a more comprehensive and automated approach to cybersecurity. With advanced tools like firewalls, intrusion detection systems, and encryption, organizations can detect and respond to cyber-attacks in real-time. All these factors play a significant role in this career, but the biggest one of all is just understanding the social meaning behind attacks and why these attackers are committing crimes or attempting to steal your data.

The CIA Triad Model

To understand attackers and how to better protect yourself against them we need to understand the CIA Triad. It's the foundation of information security. It provides us with the 3 building blocks of what good security means. Without the CIA Triad model, security today would not be where it's at right now. However, the CIA Triad does need to be updated because, with technology and attacks changing daily, the CIA Triad will soon be vulnerable and will not be relied upon anymore.

The CIA Triad, not to be confused with the Central Intelligence Agency, is a security model that consists of three components: confidentiality, integrity, and availability. Confidentiality means the protection of information from unauthorized disclosure. Integrity means the protection of information from unauthorized modification. Availability means the ability of authorized users to access information when needed. The three components of the CIA triad form the foundation of information security.

According to (Authentication - glossary: CSRC 2023), authentication means "Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system." In simpler terms, it means that you need to have the right credentials to have permission to use an application or device. As an example, you go to unlock your iPhone, but it needs to scan your face or fingerprint. That is authentication and without it, all our data would be at a loss.

According to (Security authorization - glossary: CSRC 2023), authorization means "The right or permission that is granted to a system entity to

access a system resource." This is the next step after authentication to access your information. If your authentication fails, then authorization will not happen.

The key difference between authentication and authorization is that one is a verifier, and the other either denies or grants access. Authentication happens before authorization. During authentication, the device or application will need to verify the person logging in is who they are. Next, authorization occurs and most of the time access will always be granted if authentication passes. However, if authentication fails then authorization will not happen.

In conclusion, the CIA Triad is a very important building block to the foundation of IT and Cyber Security. Without it, organizations would be losing thousands of pieces of data every day because there would be no confidentiality, integrity, or availability when it comes to the protection of data. However, it does need to be updated so it can continue to be relied upon as the key factor to security in IT. Along with the CIA Triad being important for Cyber Security, authentication and authorization cannot be forgotten as well. Without these two necessities, data leaks would be another problem for organizations and personal devices. But the CIA Triad Model isn't the only important system to follow and understand when it comes to protecting data. Another option could be SCADA Systems.

SCADA Systems

SCADA (Supervisory Control and Data Acquisition) systems are software applications that play a crucial role in mitigating the risks associated with critical infrastructure systems. These systems help to monitor and control industrial processes in real time, enabling operators to respond quickly to any incidents or anomalies. SCADA systems gather data from sensors and other sources, then analyze and present it in a way that can be easily understood by human operators. This helps to prevent downtime, reduce costs, and improve overall efficiency.

A con to the SCADA systems is that they're vulnerable to cyber-attacks. These systems are often connected to the internet, making them accessible to potential hackers. Once a hacker gains access to a SCADA system, they can cause serious damage by manipulating the data or controlling the industrial processes. For example, a hacker could cause a power grid to fail or disrupt water treatment systems, leading to significant health and safety risks. Some other vulnerabilities could be weak authentication, lack of data encryption, and human error (Ten et al. *Vulnerability Assessment of Cybersecurity for SCADA systems | IEEE ...*)

To mitigate these risks, SCADA applications use various security measures, including firewalls, intrusion detection systems, and encryption. These security measures are designed to prevent unauthorized access and detect any suspicious activity within the system. Additionally, SCADA systems are often designed with redundancy in

mind, so that if one component fails, another can take its place.

In conclusion, SCADA applications play a critical role in mitigating the risks associated with critical infrastructure systems. By monitoring and controlling industrial processes in real-time, these systems help to prevent downtime, reduce costs, and improve overall efficiency. However, it is crucial to recognize the vulnerabilities associated with these systems and take steps to ensure their security. Another thing is that anyone can use the CIA Triad Model or the SCADA Systems but none of it will matter unless you have the accurate funds and knowledge to use them.

The Human Factor in Cybersecurity

As cyber threats continue to evolve, organizations are investing heavily in cybersecurity to protect their valuable information assets. However, with a limited budget, it can be challenging to balance the tradeoff between investing in cybersecurity training and additional technology. In this section, we will discuss a Chief Information Security Officer's (CISO) approach to allocating funds effectively between cybersecurity training and technology to achieve the maximum protection of their organization's information assets.

The first step to allocate funds effectively between cybersecurity training and technology is to conduct a comprehensive risk assessment. A risk assessment helps to determine the organization's risk profile, identify areas that require attention, and prioritize the allocation of funds. Risk assessments are not only essential for allocating funds effectively but also for identifying and managing cybersecurity risks. Therefore, CISOs should make risk assessments a regular practice in their organization's cybersecurity program.

Cybersecurity training is critical to mitigating human errors that can lead to cyberattacks. As most cybersecurity attacks are caused by human errors such as phishing, it is essential to invest in cybersecurity training for employees. CISOs should allocate a significant portion of their budget to provide cybersecurity awareness training, phishing simulations, and cybersecurity incident response training to employees. Investing in cybersecurity training reduces the likelihood of employees falling victim to phishing emails or other social engineering tactics, which can lead to devastating cyberattacks.

After identifying the most significant risks, CISOs should allocate funds to implement technology that can mitigate those risks. The specific technology solutions needed will vary depending on the organization's risk profile. For example, if the organization is at risk of malware attacks, CISOs should invest in anti-malware software and intrusion detection and prevention systems. In addition, organizations should implement multifactor authentication, firewalls, and data encryption to enhance their cybersecurity posture.

Cyberattacks often occur due to unpatched software vulnerabilities. Therefore, it is crucial to allocate funds to ensure that software is regularly updated and patched to reduce the risk of cyberattacks. Regular software updates and patching enhance the security of systems and reduce the likelihood of cyberattacks caused by known vulnerabilities. CISOs should allocate a portion of their budget to regularly update and patch software to ensure the security of their organization's information assets.

Continuous monitoring can help detect and prevent cyberattacks in real-time. CISOs should allocate a portion of their budget to implement continuous monitoring systems such as security information and event management (SIEM) solutions. SIEM solutions collect and analyze security-related information from different sources in real-time, providing valuable insights into potential threats. Investing in continuous monitoring enhances the organization's cybersecurity posture by reducing the time between threat detection and response, thus minimizing the impact of a cyberattack.

In conclusion, a balanced approach is the most effective way to allocate funds between cybersecurity training and technology. The approach involves investing in both cybersecurity training and technology but at different levels based on the organization's risk profile and budget. Conducting a comprehensive risk assessment, investing in cybersecurity training, implementing necessary technology, regularly updating and patching software, and continuous monitoring are all critical steps that CISOs should take to allocate their limited budget effectively. By implementing these steps, CISOs can enhance their organization's cybersecurity posture and protect their valuable information assets.

Conclusion

The CIA Triad Model, the SCADA Systems, and just the social aspect of cybersecurity are all important factors to think about and understand when you are trying to analyze why an attacker may be trying to steal your data or worse and you can use this information to better train yourself on defending either your organization or personal data against these attackers. However, the threat landscape of cyber-attacks continues to evolve and as it evolves eventually, we all need to start evolving with them and start defending our systems and personal data like an attacker is going to try and capture it every day because of how quickly the threats are growing who knows when your data or your organizations data might be next on their list.

References

Chai, W. (2022, June 28). What is the CIA triad? definition, explanation, examples - TechTarget. WhatIs.com. Retrieved January 24, 2023, from https://www.techtarget.com /whatis/definition/Confidentiality-integrity-and-availability-CIA

Editor, C. S. R. C. C. (n.d.). Authentication - glossary: CSRC. CSRC Content Editor. Retrieved January 24, 2023, from https://csrc.nist.gov/glossary/term/authentication #:~:text=Definitions%3A,resources%20in%20an%20information%20system.

Editor, C. S. R. C. C. (n.d.). Security authorization - glossary: CSRC. CSRC Content Editor. Retrieved January 24, 2023, from https://csrc.nist.gov/glossary/term/security_authorization#:~:text= The%20right%20or%20a%20 permission,to%20access%20a%20system%20resource.

“SCADA Systems.” *SCADA Systems*, http://www.scadasystems.net/.

Ten, Chee-Wooi, et al. “Vulnerability Assessment of Cybersecurity for SCADA Systems | IEEE ...” *IEEE XPLORE*, 4 Nov. 2008, https://ieeexplore.ieee.org/abstract/document/4652578.

"Cybersecurity Framework." National Institute of Standards and Technology, U.S. Department of Commerce, Apr. 2018, www.nist.gov/cyberframework.

SANS Institute. "SANS: Information Security Training." SANS Institute, 2023, www.sans.org/.

"Cybersecurity and Infrastructure Security Agency (CISA)." Department of Homeland Security, 2023, www.cisa.gov/.