Designing a Security Policy

Miles Anderson

Old Dominion University

CYSE 300: Introduction to Cybersecurity

Dr. Joseph Kovacic

January 28, 2024

In regards to designing a security policy, there are many steps that need to be taken to ensure the policy is strong, has little vulnerabilities, and methods to counteract a cyber attack. Security policies made to protect data servers containing sensitive information need to uphold the elements of the CIA Triad: confidentiality, integrity, and availability (Chai, 2022). This way, data can be protected from unauthorized users, stay updated and accurate, and remain accessible at all times. In order to achieve this, data should be protected with a security policy that features multi-factor authentication, data monitoring systems, and data backup. Additionally, this policy needs to prioritize employee training and practice the use of anti-virus software.

The use of multi-factor authentication, data monitoring systems, and data back-up are all techniques to ensure confidentiality, integrity, and availability respectively. First, multi-factor authentication is a verification method that requires several steps to access an account besides a username and password ("What is Multi-Factor Authentication", n.d.). Multi-factor authentication steps can include phone pings, fingerprints, or 4-8 digit codes sent to the account holder's email or text ("What is Multi-Factor Authentication", n.d.) With multi-factor authentication in place, if an unauthorized individual gained access to the login credentials of someone with access to sensitive information, they wouldn't be able to log into their account. Next, ensuring integrity through data monitoring systems can be utilized to detect electromagnetic pulses, server crashes, and read digital signatures to view user logins and their activity (Chai, 2022). Finally, protecting against data loss and upholding availability can be achieved through backing up data. In case of unpredictable events such as natural disasters, data can be stored in an isolated, fireproof, waterproof safe (Chai, 2022).Obtaining a balance in confidentiality, integrity, and availability with these three techniques is essential to protecting information.

In addition to implementing the elements of the CIA Triad, a strong security plan should have extra defenses to mitigate cyber attacks. Employee training needs to be prioritized to prevent accidental security breaches. Human error makes up nearly 80% of cyber security incidents (Chamorro-Premuzic, 2023). If employees are all well trained and well versed in company procedures, it is likely that accidental breaches will significantly decline. Moreover, the use of anti-virus software can mitigate the intrusion of malware. Anti-virus software scans files and alerts the user of the presence of malicious software in files and malware activities("Understanding Anti-Virus Software", 2019). This allows the user to then delete any malicious files located on their devices, eliminating the malware before it can do any harm. Implementing these two techniques in the security policy adds an extra layer of protection and mitigation against a cyber attack.

A strong security policy is absolutely necessary to protect sensitive database servers. Cyber attacks against sensitive data can result in dire consequences, including devastating financial losses. As technology advances, the scale of cyber attacks are likely to increase. However, creating a security policy that incorporates elements of the CIA Triad is a sure-fire way to mitigate against avoidable losses. This, in combination with rigorous employee training and the use of anti-virus software, adds multiple layers of security and defense to keep sensitive data out of the hands of cyber criminals.

References

Chai, W. (2022, June 6). CIA triad (confidentiality, integrity and availability). *TechTarget.* https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA.

Chamorro-Premuzic, T. (2023, May 3). Human Error Drives Most Cyber Incidents. Could AI Help? *Harvard Business Review.* https://hbr.org/2023/05/human-error-drives-most-cyber-incidents-could-ai-help.

Understanding Anti-Virus Software. (2019, September 27). Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov/news-events/news/understanding-anti-virus-software.

What is Multi-Factor Authentication (MFA) and How Does it Work? (n.d.). *Onelogin*. https://www.onelogin.com/learn/what-is-mfa.