

Short Research Paper #2

Vincent Saunders

Department of Cybersecurity

CYSE 300

9-17-2023

To ensure the confidentiality, integrity, and accessibility of sensitive data, a comprehensive security plan for a business information system is required, particularly one that encompasses on-premises web, application, and database servers. This short paper will examine five critical issues that must be addressed in such a security approach. These elements are critical to defending the organization's assets and maintaining stakeholder trust.

One of the most vital dangers relates to figuring out who has the ability to access private data. The security policy ought to include potent control over access procedures like role-based access control, also known as RBAC, or restricted access in order to restrict access solely to approved individuals. Strong means of authentication, such as multi-factor authorization (MFA), should be utilized to make certain individuals are the individuals they represent as. This aids in the prevention of unwanted access and logs user activity for auditing reasons.

Database servers must encrypt sensitive data in transit as well as at rest. It's assured that the data will remain unintelligible even in the case of unauthorized access by employing industry-standard encryption technologies such as TLS for data in transit and disk encryption for data at rest. The treatment of encryption keys should be laid out in the security policy, and regular adjustments to the algorithm ought to be introduced to take into account increasing problems with security.

It is necessary to periodically update and patch systems of operation, internet servers, application servers, and database management software for the purpose of protecting oneself against known security flaws. The security policy should contain a patch management mechanism that ensures timely patch identification, testing, and deployment. Additionally, doing frequent penetration testing and vulnerability assessments can assist in identifying and closing any gaps before attackers exploit them.

Since no security system is impregnable, the security strategy must include a well-defined incident response plan. This strategy should explain the steps to be taken in the case of a security breach, including communication processes, evidence preservation, and legal compliance. Early detection of suspicious behavior necessitates continual monitoring of system logs and network traffic. SIEM (Security Information and Event Management) solutions may be utilized to automate and streamline this procedure.

Human mistakes and carelessness are frequently the weakest links in business security. Employee training and awareness activities must be included in the security policy. These programs should educate employees on security best practices, social engineering dangers (such as phishing), and the value of data security. To promote the security culture throughout the firm, regular training and assessment of workers' understanding should be mandatory.

To summarize, developing a security plan for a company information system that involves sensitive data stored on on-premises servers is a difficult task. To protect their assets, organizations may build a solid security architecture that addresses access control, encryption, patch management, incident response, and employee training. To stay ahead of evolving threats and technologies in the ever-changing realm of cybersecurity, it's necessary to alter and update the security policy on a regular basis.

Reference Page

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '06), 581-590.

Schneier, B. (1996). Applied Cryptography: Protocols, Algorithms, and Source Code in C (2nd ed.). John Wiley & Sons.

Northcutt, S., Novak, J., & Winters, R. (2008). Network Intrusion Detection: An Analyst's Handbook. New Riders.

Hadnagy, C. (2011). Social Engineering: The Art of Human Hacking. John Wiley & Sons.