Short Research Paper #2

Lilibeth Rodriguez Sanchez

Old Dominion University

CYSE 300

Malik A. Gladden, MS.CYB

1/25/2024

Technology has advanced tremendously over the years and in a rapid pace. With all these continuous enhancements comes more security policies in place becoming one of the most prominent aspects in organizations to ensure that their information is secure. While researching I was able to conclude that the five major matters that should be addressed when designing a security policy for a database would be access control, data encryption, security patching and updates, auditing and monitoring, and backup and disaster recovery. Such areas must have more focus to be able to support the database through standards and policies. It is essential to maintain focus on these specific areas to prevent any possible risks. A security policy is a document that in formatted for an organization or company to provide a framework on how to ensure that security measures are put in place to prevent from any dangers, threats, or attacks.

Access control is one of the key concepts that should be implemented when creating a security policy. Implementing access control mechanisms can help protect sensitive data. When creating a security policy, it should follow strict rules and regulation regarding user authentication, authorization, and privileges that each one of them are meant to have. It is crucial to be able to provide a framework that involves the procedures for creating and managing user accounts. Such policy should address the importance of strong passwords and multi-factor authentication for administrative access. When creating a security policy, it is advised to provide certain access based on the roles and responsibilities of the individual. Also, when avoiding such threats and attacks it is important to ensure that responsibilities are spread within employees to ensure that not only one person has complete control over critical systems and data.

Data encryption is important when creating a security policy. It provides security to sensitive information that is stored in the database servers. It would be crucial to ensure that the security policy outlines encryption requirements for the data while in transit and at rest. In the

security policy it should be specific when describing the use of strong encryption algorithms and appropriate key management policies. Ensuring that there are proper data encryption mechanisms involved the security policy would help ensure that data is being kept confidential.

When developing an effective policy security policy patching and updates is important to be implemented and discussed. “Security policy patching and updates is used in order to protect against any known vulnerabilities and exploitations” (CISA). It is necessary to implement a clear policy for monitoring and applying patches and updates for the database server. Ensuring that patches are being reviewed in a timely manner would help mitigate the risk of potential security breaches.

Auditing and monitoring would be necessary for an effective security policy. The policy should emphasize the importance of auditing and monitoring activities being made in the database system. “The security policy would need to outline implementation of robust logging practices being used to capture and retain relevant security events” (Dash). For an effective security policy, it is crucial to ensure that logs are being generated involving information based on which logs should be generated, where they should be kept, and lastly for how long they should be stored. It is significant that there are regular investigations being done to be able to detect any suspicious activity.

Lastly, backup and disaster recovery are important to involve in an effective security policy because it helps protect sensitive data. The security policy should provide an outline of a proper backup procedure which would involve frequency of backups, retention periods, and storage locations. A security policy should also involve a disaster recovery plan in order to ensure that employees know the procedures necessary to be able to restore in an event of a major incident or a system failure.

Developing a strong and effective security policy is critical to ensure that all information form the organization is kept confidential and secure. Implementing the five mechanisms above access control, data encryption, security patching and updates, auditing and monitoring, and lastly backup and disaster recovery will ensure that information is kept secure.

References

Best practices for developing effective security policies. Dash Solutions. (2023b, November 14).https://www.dashsdk.com/resource/best-practices-for-developing-effective-security-policies/

Cybersecurity Best Practices. Cybersecurity Best Practices | Cybersecurity and Infrastructure Security Agency CISA. (n.d.). https://www.cisa.gov/topics/cybersecurity-best-practices

For additional information on APA Style formatting, please consult the APA Style Manual, 7th Edition.