Database Security Policy

Destiny Hale

Old Dominion University

CYSE 300

Professor Gladden

1/28/2024

Database Security Policy

Statement and Purpose

The company has a responsibility to protect the information under its custody and control. The purpose of this information system policy is to address database security practices to ensure the protection of sensitive information and data. Also to inform about database security protocols and cyberattack awareness. The following practices that will be discussed are access control, data classification, encryption, server care, and threat awareness.

Access Control

Within a database facility, the server room is highly surveillance and alarmed for monitoring and trespassing purposes. It is mandated for authorized individuals to use identification and a source of verification, such as biometrics or code, before entering the server room. The key cards track and log both entries and exits for auditing and futher security purposes. If the key card is stolen or lost, please report and notify the card department for them to issue a new one. Old key cards will be deactivated and discarded for further protection. While exiting, the individual must check their surroundings for any personal or important items before leaving the server room. Also, the individual should make sure the server room is locked and secured. This will prevent any theft, damage, and unauthorized access within the server room.

Data Classification and Encryption

Data classification is the process of organizing items, objects, subjects, categories, or collections with similar attributes. To keep data secure, all data must be organized into categories to prevent full accessibility to sensitive data. According to CISSP, there are four types of classification which are confidential, private, sensitive, and public. Confidential is the highest level of classification used for highly sensitive data and for internal use only. Private is the

second highest level of classification which is also used for internal use only. Sensitive is used for data classified than public data. Public is the lowest level of classification which this type of data doesn't fit with the other 3 classifications. However, there must be ownership to apply these classifications of data. Encryption will secure the transfer of data and keep it confidential within the network. One method the NIST suggests is AES which stands for Advanced Encryption Standard. This algorithm can be used to encrypt and decrypt information and it's also symmetric which the key is the same for encryption and decryption. This would make it difficult for unauthorized individuals to gain access to the information from the servers.

Server Care and Threat Awareness

If the servers are left unattended, this would lead to multiple vulnerabilities and threats within the server and network. A few examples of threats and vulnerabilities are worms, trojan horses, viruses, and many others. The NIST framework provides definitions for each. A worm is a self-replicating program that is self-contained and does not contain a host. A trojan horse is a program that performs a desired task but includes unexpected functionality. Last but not least, a virus is a code segment that replicates itself by attaching copies of itself to existing executable. However, these can be prevented by proper server care. To keep the servers up and running, proper server care must be maintained. For systems to properly run, servers must be updated and tested every month to keep the transfer of information flowing smoothly. Also, the servers must be up-to-date in the prevention of downtime and being vulnerable to malicious actors. Downtime is when a machine is out of action or unavailable for use. It is important to keep the servers available for both clients and user ends. As for the environment, proper ventilation, lighting, and temperature is needed in prevention of overheating. By all of these practices, this will protect and secure the servers.

Summary

It is the responsibility of the company to protect and secure their data under their custody and control. This policy is intended to address and inform security practices for database security and cyberattack awareness. The following practices that were discussed in this policy were access control, data classification, encryption, server care, and threat awareness. For access control, it is important to use identification and verification before entering. As for exiting, it is recommended to check the surroundings and make sure the server room is secured. For data classification, it is important to organize sensitive data into the four classifications which are confidential, private, sensitive, and public to prevent full access. To further protect the data, encryption will protect the transfer. A suggested method is using the advanced encryption standard which can be used to encrypt and decrypt data. To prevent vulnerabilities and threats such as worms, trojan horses, downtime, and viruses, proper server care must be maintained.

References

Chukwube, M. (2023, May 4). *5 best practices for Physical Security*. Dzone. https://dzone.com/articles/protecting-your-server-room-5-best-practices-for-p

Stewart, J.M., Chapple, M., & Gibson, D. (2015). *CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide, Seventh Edition* (textbook)

Nieles, M., Dempsey, K., & Pillitteri , V. Y. (2017, June). *An Introduction of Information Security*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf