Proper Security precautions for a secure Information System

Gerkeil Owens

Old Dominion University

CYSE 300

1/21/2023

Database security is a challenging task involving all facets of information security policies and procedures to protect against cyberattacks and vulnerabilities of obtaining confidential information from a corporation or organization. According to (Kostadinov, 2020) Five or more key concerns need to be taken into consideration when creating a strategic security approach for a corporate information system that includes local web, application, and database servers. These include how to fix a breach, notifying consumers, and other necessary actions, as well as the cost of compromising intellectual property, harm to a company's system, potential effects on business continuity, and potential fines or penalties for this happening. As well as, reviewing the laws of the tech work that needs to be done to secure your company, so you won't break those laws because in the UK they have a list of legislation laws (Kostadinov, 2020).

With that you must account for the threats to database security and where they can come from. Security threats can come from a variety of places, such as dishonest or careless individuals, software bugs or configuration errors, computer viruses, human mistakes by not properly giving enough time to monitor or update their systems or putting the money into that software to get the best security possible, and human error from not properly taking the right precautions. Any security vulnerability to the network infrastructure must be addressed because databases frequently need a network for access and use.

The security policy must consider physical security, administrative and network access controls, end-user account/device security, encryption, software security, and application/web

server security. If the database is on-premises, it is crucial that the environment is secure and controlled. According to (*Database Security: An Essential Guide*, n.d.) another crucial step is looking into backup databases or software that must be subject to the same or similar strict security standards as the primary database, backup security is also essential.
Having administrative controls should be in place to regulate database installation, modification, and configuration. Preventative controls should be in place to regulate access, encryption, authentication and authorization, and any other activity occurring in the corporation's database. Detective controls should be integrated using tools for database activity monitoring and data loss prevention.

The security policy should be intact and aligned with the organization's objectives, including safeguarding critical intellectual property, and supporting cybersecurity and cloud security regulations. Security controls, security awareness training and education programs, penetration testing and vulnerability assessment techniques, as well as responsibilities for maintaining and evaluating security controls, should all be implemented. To enable and support a formal security policy, each of these steps should be put in place for a better understanding of the system and how to fix the problem for a better and secure database. As well as, doing a test run to make sure that the database is secure to prevent any errors from occurring.

In conclusion, five or more important steps should be taken into consideration when creating a security policy for a corporate information system. These include the costs of correcting a breach and notifying consumers, compromised intellectual property, harm to brand reputation, potential effects on company continuity, and potential fines or penalties for non-compliance. As well as the laws put in place when handling databases to prevent any illegal activity from occurring (Kostadinov, 2020). In addition to factors within the database itself, the security strategy must consider physical security, administrative and network access controls, end-user account/device security, encryption, software security, application/web server security, and backup security. constant updates to the system, constantly monitoring the system, and support of an official security policy.

References

Database Security: An Essential Guide. (n.d.). IBM. Retrieved January 21, 2023, from https://www.ibm.com/topics/database-security

Kostadinov, D. (2020, July 20). *Key elements of an information security policy | Infosec Resources*. Infosec Resources. Retrieved January 21, 2023, from https://resources.infosecinstitute.com/topic/key-elements-information-security-policy/