Creating An Effective Database Security Policy

Eric Mung'aũ Preston

Old Dominion University

CYSE 300: Introduction to Cybersecurity

Mr. Malik A. Gladden

1/27/24

Creating An Effective Database Security Policy

Abstract

Due to the short but growing awareness of cybersecurity, many laws and policies have been made to protect all forms of infrastructure. Information Technology departments and Chief Information Security Officers are further proof of that. However, there are still many security issues that need to be mitigated to protect crucial data from databases and corporate information systems overall. This paper will address multiple database security policy vulnerabilities and how to properly mitigate them, creating an information security policy for databases across several areas.

Introduction

Database security policies and overall data privacy are an integral part of any information system. These policies benefit companies via the protection of sensitive information and user data which if leaked, creates large costs in damages for the company and worry for customers over their information. Recognizing the importance of database security policy, this paper focuses on the essential components of an effective security policy by targeting five separate database security policy issues, which provide fundamental information for companies with vulnerabilities in their information systems.

ISSUE 1 – SQL Injection

SQL Injection is one of several issues that jeopardizes database security. According to Humayun et al. (2020), it manipulates databases by injecting a string of code to change information. This causes loss of data, as well as locks out authorized users, and concedes to unauthorized groups. This issue is solved with improved programming and applying restricted privileges to prevent access. Furthermore, using prepared statements to prevent SQL queries and

stored procedures are other options that provide security (Hlaing and Khaing, 2020). However, while fortifying the database backend is important, securing information within the database itself in the event of a breach is needed.

ISSUE 2 – Poor Encryption

Another database security issue comes from a lack of encryption. Fundamentally, encryption is "the process of concealing or converting information using cipher code or code to be unreadable to all other people except those that hold the key information" (Tanwar, 2022). Encryption changes data within a database so that if unauthorized people see it, unreadable text shows, maintaining confidentiality. However, unencrypted data allows for tampering or theft, hence why proper encryption and key management are crucial (Hlaing and Khaing, 2020). Encryption is useful in protecting databases, but other difficulties arise in maintaining database security.

ISSUE 3 – Database Misconfiguration

The misconfiguring of a database has long-term effects on other security issues due to being a fundamental issue that permeates its functionality. This occurs due to default accounts and configuration parameters which hackers easily exploit and steal the data. An effective solution is an increase in Information Technology staff to properly program and implement the software for managing the data of many users (Mousa et al., 2020). While proper configuration is beneficial, necessary methods for recovery and warning are also needed in the event of an eventual breach.

ISSUE 4 – Denial of Service (DoS) Attacks

DoS attacks target entire systems or slow down the traffic flow of a network. This leads to unusable systems, defective devices, and high damage fees when restoring databases.

According to Humayun et al. (2020), “One reason for a DoS attack is that various industries use similar technologies and potential attackers take advantage of this.” Fortunately, solutions include an Intrusion Detection System (IDS) network and correcting the registry settings on the TCP/IP stack to increase the TCP connection list (Mousa et al., 2020). Solutions to cyberattacks are advantageous, and constant improvements are needed for database vulnerabilities.

ISSUE 5 – Malware

Malicious software or malware is one of the most common cyberattacks, but an ever-prominent danger that impacts databases. The attack focuses on gaining access to the network via exploits and the incentive is primarily to profit by selling large amounts of data (Humayun et al., 2020). Its flexibility comes in many forms including worms, viruses, trojans, and ransomware (Alenezi et al., 2020). Despite different types of malware, solutions to handle the issue take the form of anti-malware software. According to Iffländer et al. (2019), with ransomware, programs like RWGuard work at the firmware level to prevent intrusion.

Conclusion

Database security policies are essential for several reasons. Layers of security on the database’s backend prevent SQL Injection and maintain integrity, while encryption protects data from unauthorized users in and out of a company. Additionally, proper database configuration is necessary both for traffic flow as well as mitigating vulnerabilities, and networks like IDS against DoS attacks are necessary for protecting database shutdown and minimizing cost repairs. Lastly, the installation of anti-malware software fights database intrusion. Overall, the implementation of these solutions from security policy issues creates an effective policy and a sizeable first step toward improving corporate information systems.

References

Alenezi, M. N., Alabdulrazzaq, H., Alshaher, A. A., & Alkharang, M. M. (2020). Evolution of Malware Threats and Techniques: A Review. *International Journal of Communication Networks and Information Security, 12*(3), 326-337. http://proxy.lib.odu.edu/login?url=https://www.proquest.com/scholarly-journals/evolution-malware-threats-techniques-review/docview/2483989571/se-2

Hlaing, Z. C. S. S., & Khaing, M. (2020). A Detection and Prevention Technique on SQL Injection Attacks. *2020 IEEE Conference on Computer Applications(ICCA)*. https://doi.org/10.1109/icca49400.2020.9022833

Humayun, M., Niazi, M., Jhanjhi, N., Alshayeb, M., & Mahmood, S. (2020). Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. *Arabian Journal for Science and Engineering*, *45*(1). springer. https://doi.org/10.1007/s13369-019-04319-2

Iffländer, L., Dmitrienko, A., Hagen, C., Jobst, M., & Kounev, S. (2019). Hands off my database: Ransomware detection in databases through dynamic analysis of query sequences. *arXiv preprint arXiv:1907.06775*.

Mousa, A., Karabatak, M., & Mustafa, T. (2020). Database Security Threats and Challenges. *2020 8th International Symposium on Digital Forensics and Security (ISDFS)*. https://doi.org/10.1109/isdfs49300.2020.9116436

Tanwar, S. (2022). Database Security and Encryption. *International Journal of Advanced Research in Science, Communication and Technology*, *2*(6), 355–357. https://doi.org/10.48175/ijarsct-5036