Vulnerability Assessment Report

12th February 2024

System Description

The server hardware consists of a powerful CPU processor and 128GB of memory. It runs on the latest version of Linux operating system and hosts a MySQL database management system. It is configured with a stable network connection using IPv4 addresses and interacts with other servers on the network. Security measures include SSL/TLS encrypted connections.

Scope

The scope of this vulnerability assessment relates to the current access controls of the system. The assessment will cover a period of three months, from June 20XX to August 20XX. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The database server is a centralized computer system that stores and manages large amounts of data. The server is used to store customer, campaign, and analytic data that can later be analyzed to track performance and personalize marketing efforts. It is critical to secure the system because of its regular use for marketing operations.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Employee	*Disrupt mission-critical operations*	*2*	*3*	*6*
Customer	*Alter/Delete critical information*	*1*	*3*	*3*

Approach

The measured risks took into account how the business stores and manages data. We identified potential sources of threats and events by considering how likely a security incident would be, given the system's open access permissions. We also compared the seriousness of potential incidents with their impact on daily operations.

Remediation Strategy

We implemented authentication, authorization, and auditing mechanisms to ensure that only authorized users access the database server. This includes using strong passwords, role-based access controls, and multi-factor authentication to limit user privileges effectively. Additionally, we prioritize data security by encrypting data in motion using TLS instead of SSL, safeguarding it from interception during transmission. Furthermore, we enforce IP allow-listing to corporate offices, preventing random users from the internet from connecting to the database and enhancing overall network security.

Conclusion:

In conclusion, the vulnerability assessment of the database server system helped identify potential risks and implement strong security measures to mitigate them effectively. By following NIST SP 800-30 Rev. 1 guidelines, we prioritized actions based on the likelihood and severity of threats from hackers, employees, and customers. Our remediation strategy focused on authentication, authorization, and auditing mechanisms to ensure only authorized users access the server. Incorporating strong passwords, role-based access controls, and encryption of data in motion enhances user security and network defenses. Continuous monitoring and updates are vital to adapt to evolving threats and maintain a resilient defense posture, safeguarding our marketing operations and data assets. Conducting this assignment helped strengthen NIST framework understanding and how vulnerability assessment and risk management is critical in organizational information security.