Vulnerability Assessment Report

21st September 2023

System Description

The server hardware features a robust CPU processor and 128GB of memory, ensuring optimal performance. Running on the latest Linux version, it hosts a MySQL database management system. The network connection is stable, utilizing IPv4 addresses for seamless interaction with other servers. Security is prioritized with SSL/TLS encrypted connections, ensuring data protection during transmission.

Scope

The vulnerability assessment has a specific scope, which pertains to evaluating the existing access controls of the system. The assessment will encompass a three-month timeframe, commencing from June 20XX and concluding in August 20XX. The risk analysis process is guided by NIST SP 800-30 Rev. 1, ensuring that the assessment aligns with established industry standards and practices.

Purpose

The database server functions as a centralized computing system designed for the storage and management of substantial volumes of data. Its primary purpose is to house customer, campaign, and analytic data, facilitating subsequent analysis for tracking performance and tailoring marketing initiatives. Due to its frequent utilization in marketing operations, ensuring the security of this system is imperative to safeguard sensitive and critical data.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker	*Obtaining sensitive information*	*3*	*3*	*9*
Employee	*Disrupt important operations*	*2*	*3*	*6*
Customer	*Edit or delete critical information*	*1*	*3*	*3*

Approach

Risks were assessed by focusing on the data storage and management procedures within the business. Identification of potential threat sources and events involved evaluating the likelihood of security incidents, taking into account the open access permissions of the information system. The severity of potential incidents was then weighed against their impact on day-to-day operational needs.

Remediation Strategy

- **Authentication, Authorization, and Auditing Mechanisms:**

Implementation of robust authentication mechanisms to ensure that only authorized users can access the database server.

Utilization of role-based access controls to restrict user privileges based on their roles and responsibilities.

Implementation of auditing mechanisms to monitor and log access activities for security analysis.

- **Password Security Measures:**

Adoption of strong password policies to enhance the security of user accounts.

Regularly enforce password updates and complexity requirements.

- **Multi-Factor Authentication (MFA):**

Implementation of multi-factor authentication to add an additional layer of security, requiring users to provide multiple forms of identification.

- **Encryption of Data in Motion:**

Deployment of TLS (Transport Layer Security) for encrypting data in motion, ensuring secure communication between clients and the database server.

Phasing out the use of SSL (Secure Sockets Layer) due to known vulnerabilities.