Vulnerability Assessment Report

1st March 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 January 2024 to March 2024. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The database server serves as a centralized system responsible for storing and managing extensive volumes of data. This includes customer information, campaign data, and analytics, all of which are utilized for tracking performance and customizing marketing endeavors. Given its integral role in marketing operations, it is imperative to implement robust security measures to safeguard the system and the data it contains.

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 risk assessment focused on evaluating the data storage and management protocols within the business. Potential threats and events were identified by assessing the likelihood of security incidents based on the open access permissions of the information system. Furthermore, the severity of potential incidents was analyzed in relation to their impact on day-to-day operational requirements.

Remediation Strategy

To enhance security measures for the database server, the following actions should be implemented:

1. Authentication, Authorization, and Auditing Mechanisms: Deploy robust authentication methods, such as strong passwords and multi-factor authentication, to verify user identities before granting access to the database server. Utilize role-based access controls to assign appropriate permissions to users based on their roles and responsibilities. Implement auditing mechanisms to monitor user activities and ensure compliance with security policies.

2. Encryption of Data in Motion: Encrypt data while it is being transmitted over the network using Transport Layer Security (TLS) protocols. Avoid using Secure Sockets Layer (SSL) due to known vulnerabilities. Encryption ensures that data remains protected from unauthorized access during transmission.

3. IP Allow-listing: Restrict access to the database server by allowing only authorized IP addresses, such as those associated with corporate offices, to connect. This prevents random users from the internet from accessing the database server and reduces the risk of unauthorized access attempts.

By implementing these security measures, the database server can be better protected against unauthorized access and data breaches, thereby enhancing overall system security.