Vulnerability Assessment Report

1st January 20XX

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 central system designed to store and manage vast amounts of data. It holds customer, campaign, and analytical information, which can be utilized to assess performance and tailor marketing strategies. Securing this server is essential due to its integral role in marketing operations and frequent usage.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Employee	*Interrupt essential business functions*	*2*	*3*	*6*
Customer	*Alter or Delete important information*	*1*	*3*	*3*

Approach

The assessed risks took into account the business's data storage and management practices. Potential threats and incidents were identified based on the probability of a security breach due to open access permissions. The severity of these incidents was evaluated in relation to their impact on daily operations.

Remediation Strategy

Implementation of 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. Encryption of data in motion using TLS instead of SSL. IP allow-listing to corporate offices to prevent random users from the internet from connecting to the database.