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 stores and manages customer, campaign, and analytic data critical for tracking performance and personalizing marketing efforts. It operates on powerful hardware with a high-performance CPU and 128GB of memory, running the latest Linux version and MySQL database management system. The server connects with other systems via IPv4, and data is protected with SSL/TLS encryption. This vulnerability assessment aims to identify security risks and safeguard the sensitive data stored. Ensuring its security is essential to maintaining the integrity and availability of marketing operations.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Customer	*Alter or delete self-identifying information or information about other customers within the public database that all employees use.*	*2*	*3*	*6*
Current Employee	*Accidental information information leaks, disruption of critical operations, or falling victim to social engineering tactics.*	*2*	*3*	*6*

Disgruntled Employee	*Access the database that is available for public viewing and give customer information to a competitor or new/future competing employer. Leaking customer-sensitive data, damaging the reputation of the company.*	*3*	*3*	*9*
Competitor	*Competitor finds out about the database and use it to get customer-sensitive information and poches the customers to their businesses.*	*3*	*3*	*9*
Hacker	*Infiltrates the system and gets access to even more sensitive information about customers and employees.*	*3*	*3*	*9*

Approach

The risks assessed took into account the business's data storage and management practices. The likelihood of potential security incidents was evaluated based on the open access permissions of the information system. Threat sources and possible events were identified, and their potential severity was measured against the impact on daily operations. By balancing these factors, the analysis aimed to understand the risks posed to business continuity and operational needs.

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.