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 centralized computer system that manages and stores large amounts of data. The server is used to store customer, campaign, and analytic data that is later able be analyzed to track varying performance and personalize marketing efforts. It is important to secure the system due to its regular use in the organization for marketing operations.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Conduct Denial of Service (DoS) attacks.*	*3*	*3*	*9*
Hacker	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Employee	*Disrupt mission-critical operations*	*2*	*3*	*6*

Approach

The threat sources and risks that were considered can impact the data storage and management methods of the organization. The likelihood of a threat occurrence and the impact that these potential events can have were weighed against the risks to day-to-day operational needs.

Remediation Strategy

The recommended strategy for securing the organization's data assets are as follows. Immediate implementation of authentication, authorization, and auditing mechanisms to ensure that only authorized users are able to gain access to the database server. This should include the use of strong passwords, role-based access controls, and multi-factor authentication to limit user privileges. Encryption of data in motion using TLS instead of SSL. and finally IP allow-listing to corporate offices to prevent random users from the internet from connecting to the database and being able to access the organizations data assets.