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

Consider the following questions to help you write:

- *How is the database server valuable to the business?*
  The database server (in this case the computer running the hardware mentioned in the description) stores and manages a significant amount of data.
- *Why is it important for the business to secure the data on the server?*
  Because the system is used for marketing operations.
- *How might the server impact the business if it were disabled?*
  If disabled, the marketing operations would be forced to stop, and worst case scenario, sensitive data could be stolen.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Alter information necessary for conducting operations properly.*	*1*	*2*	*2*
Employee	*Stop operations by overloading the system.*	*2*	*3*	*6*
Hacker	*Penetrate the system and steal sensitive data*	*3*	*3*	*9*

Approach

Risks considered the data storage and management methods of the business. The likelihood of a threat occurrence and the impact of these potential events were weighed against the risks to day-to-day operational needs. The severity of potential incidents was weighted considering the effects they would have on regular 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.