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?*
- *Why is it important for the business to secure the data on the server?*
- *How might the server impact the business if it were disabled?*

The database server is valuable to the business as it stores information that employees need to access in order to query data to find potential customers. It is important to secure the data on the server since public access allows anyone to alter, delete, and steal critical information in a way that negatively impacts the business. If the server were disabled, there would be a great loss of business in obtaining customers.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Customer	*Alter/Delete critical information*	*1*	*3*	*3*
Hacker	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*

Employee	*Disrupt mission-critical operations*	*2*	*3*	*6*

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.

A customer could accidentally alter or delete critical information since the database is publicly accessible, which would negatively impact the business. A hacker could install malicious software on the organizational systems to acquire sensitive information from the database. Even an employee could accidentally compromise the integrity of information stored on the database that would prevent critical business 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.

Implementing the principle of least privilege would help make sure only those who need the information have access to it. This would reduce the access from being public to only the employees that need the query data from the database to find potential customers.