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 hosts a MySQL DBMS storing business data including customer information. The storing of customer information highlights the importance of securing the data present on the server. Customer PII and even SPII may be stored on the server and must be protected. If the server were to become disabled, employees would lose access to valuable information required to perform their tasks. They will be unable to query the system for information leading to disruptions of normal business activity.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Hacker	*Alter/Delete critical information*	*2*	*3*	*3*
Hacker	*Conduct Denial of Service (DoS) Attacks*	*3*	*3*	*9*

Approach

The above 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. Because the server is publicly accessible, it is especially subject to the risks listed. The Risk scores act as indicators of a combination of both the likelihood and potential severity of each risk occurring.

Remediation Strategy

Implementing authentication and authorization mechanisms would ensure that only authorized users are able to access the database server. This would greatly help prevent the intentional or accidental alteration of important data by hackers or other threat actors. Examples of authentication mechanisms could include strong passwords and multi-factor authentication. These measures ensure that only authorized users are able to access the server and its contents. Additionally, implementing role-based access controls would allow the implementation of the principle of least privilege and protect especially sensitive data. In addition to these measures, implementing a measure which only allows connection by IP addresses of corporate offices or employees would prevent random users from connecting to the database. Finally, implementing SSL/TLS encryption to ensure that data is properly encrypted and at a lesser risk of being accessed by threat actors.