Vulnerability Assessment Report

23rd May 2025

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 service operates with a powerful CPU professor, 128GB of memory, and hosts a MySQL database management system which allows it to hold large amounts of data on customers along with fast processing time allowing for employees' regular and fast query on the database to find potential customers. If the server were disabled or compromised, the business would experience a serious data breach with countless customer personal information being used for illegal purposes, potentially leading to damaging company reputation or leading to loss of revenue since employees are unable to access the database for their day-to-day operations. It's important to secure it in order to protect customer and business information.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Employee	Disrupt mission-critical operations.	2	3	5
Customer	Alter/Delete critical information	1	3	4
Competitor	Perform reconnaissance and	2	2	4

	surveillance of organization			

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.

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.