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 the only way for remote working employees to find potential customers by querying and requesting data. It is important for the business to secure the data because it helps maintain company integrity as well as can be used for personalized marketing algorithms. If the server were to be disabled, the company wouldn't be able to operate with employees that work remotely as well as not be able to have access to the customer's data.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Alter/Delete critical information*	*2*	*3*	*6*
Hacker	*Install persistent and targeted network sniffers on organizational information systems*	*3*	*3*	*9*
Customer	*Alter/Delete critical information*	*1*	*3*	*3*

Approach

The risks that were chosen are possibly the common types of threats that appear on a day to day basis, relating to the data storage. These chosen threats are not only common, but high in severity. If any of these threat events were to play out, the company may lose credibility.

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. IP allow-listing to corporate offices to prevent random users from the internet from connecting to the database. Regular audits to ensure only properly authorized users are able to access the database.