Vulnerability Assessment Report

1st January 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 purpose of this cybersecurity vulnerability assessment is to evaluate the potential risk with current access and control systems. Our customer database is a valuable asset that is accessible to generate leads for our employees. Having a secure access control system will allow for an increased security posture by securing customer data and ensuring integrity across our business operations. The customer database is our main source for leads, any attack could handicap employees in doing their jobs successfully and/or shut down critical business functions..

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Employee	Disrupt mission-critical operations.	*3*	*2*	*6*
Customer	Alter/Delete critical information	*1*	*2*	*3*

Approach

Risks were measured and considered with the current access control management of the business. Potential threats were considered and events were determined likely to happen given the current public availability of the database. The severity of each incident was weighed against the impact of mission-critical operations of the company.

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.