# Vulnerability Assessment Report

**4th, March 2024**

## 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 to August. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

## Purpose

The server is used for marketing purposes to store customer information and campaign data. Currently the server is publicly accessible due to the remote nature of the company. It is important to secure this data because of the sensitive personal information it stores and its use for the marketing efforts of the company.

## Risk Assessment

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

## Approach

I assessed risks by evaluating its data storage and management protocols. I identified potential threats and events based on the likelihood of security breaches due to the open access permissions of the information system. The severity of potential incidents was compared against the impact on daily operational requirements.

## Remediation Strategy

The implementation involves deploying authentication, authorization, and auditing measures to safeguard the database server, ensuring that only authorized users gain access. This entails employing robust passwords, role-based access controls, and multi-factor authentication to restrict user privileges effectively. Additionally, data encryption during transmission will utilize TLS instead of SSL for enhanced security. Furthermore, IP allow-listing will restrict access solely to corporate offices, mitigating the risk of unauthorized internet users connecting to the database.