**Vulnerability Assessment Report**

**2nd February 2024**

**Purpose**

The purpose of this vulnerability assessment is to identify the potential risks of a remote database server that is used to store customer, campaign, and analytic data that can later be analyzed to track performance and create personalized marketing efforts. It is critical to secure the system because it is critical to business operation of this company. If the server is affected, the business operation of the company will be seriously affected as remote company workers access this server to be able to perform their job responsibility of marketing operations.

# 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 December 2023 to February 2024. [NIST SP 800-30 Rev. 1](https://docs.google.com/document/d/1pRpdpQMEWskxSkwqEMv8W7A7x8GXQlcn0hEcDzWet3Y/template/preview?usp=sharing&resourcekey=0-3GRRWAd8HryVgof-Jc33yA) is used to guide the risk analysis of the information system.

# Risk Assessment

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

# 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.