**Vulnerability Assessment Report**

**1st February 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 December 2023 to February 2024. [NIST SP 800-30 Rev. 1](https://docs.google.com/document/d/1Fc4L2azQlnUM-8r43PU9mYlT30BnxTwdjAMqpT7JeZk/edit?resourcekey=0-Q-XglnC3Li7JPK2hIvMkVg#heading=h.hvbcmqwzo9do) is used to guide the risk analysis of the information system.

# **Purpose**

A database server is a mid-sized, centralized computer system that stores and manages large amounts of important business data. These servers allow the company to store essential customer information, campaign, and analytics data, and customize performance tracking and marketing strategies. Therefore, it is important to protect and secure these systems that are often used to run marketing operations.

# **Risk Assessment**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| *Hacker* | *Obtain sensitive information via exfiltration* | *3* | *3* | *9* |
| *Employee* | *Disrupt mission-critical operations* | *2* | *3* | *7* |
| *Customer* | *After/Delete critical information* | *1* | *3* | *4* |

# **Approach**

Risk considers how the company stores and manages business data. Potential threat sources and events were assessed using the likelihood of a security incident based on the public access rights of the information system, and the severity of the potential incident was assessed based on its impact on daily operational requirements.

**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.