**Vulnerability Assessment Report**

**21st July 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 April 2024 to June 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.

# Purpose

* ***How is the database server valuable to the business?***

*The database server is an integral part of the business as many of its employees are working remotely and they regularly access the database stored in the server.*

* ***Why is it important for the business to secure the data on the server?***

*It is crucial for the business to secure and protect the data on the server as in contains confidential information and customer details, the access to the database is made public so anyone can access the database and view the data, this does not meet the regulatory compliance requirements and also lets the competitors to view and access the customer details.*

* ***How might the server impact the business if it were disabled?***

*If the server were to be disabled intentionally or due to a threat, it would severely impact the business and their workflow. It would impact the efficiency of the employees and cause serious monetary loss as most of the employees access the data on the server to find potential customers.*

# 

# 

# 

# Risk Assessment

| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| --- | --- | --- | --- | --- |
| *Competitor* | *Obtain sensitive information via exfiltration* | *1* | *3* | *3* |
| *Hacker* | *Alter/Delete critical information* | *3* | *3* | *9* |
| *Power outages* | *Disrupt mission-critical operations.* | *1* | *3* | *3* |
| *Malicious software* | *Perform reconnaissance and surveillance of*  *Organization such as spyware* | *3* | *3* | *9* |

# Approach

Risks that were measured considered the data storage and management methods of the business. Potential threat sources and events were determined using the likelihood of a security incident given the open access permissions of the information system. The likelihood of a threat occurrence, the impact and the severity 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.