**Vulnerability Assessment Report**

**26th January 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 20XX to August 20XX. [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

Consider the following questions to help you write:

* *How is the database server valuable to the business?*
  + *The database server is valuable to the business because it allows the business to work more efficiently and faster.*
* *Why is it important for the business to secure the data on the server?*
  + *It is important to secure the data on the server because there is a lot of information between the business and customer information that needs to be protected. Losing this information can cause the company to lose customers, data, and money. Also, customer will be upset and leave if their information is taken by somebody else.*
* *How might the server impact the business if it were disabled?*
  + *If the server was disabled, the business would corrupt because it may take MONTHS in order for the server to be up and running again. Also, important information could be lost. Also, end user won’t be satisfied about how thing are operating within the business.*

# Risk Assessment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| *Workers* | *A current worker has a risk of messing up the system, making other systems not operating and loss of information* | *3* | *3* | *3* |
| *Hacker* | *Somebody could hack the system and take valuable information* | *2* | *2* | *3* |
| *System Failure* | *System getting old or slow* | *3* | *1* | *1* |

# 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.