# Vulnerability Assessment Report

15th July 2023 Eliyas Philip

## 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 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?*
- *Why is it important for the business to secure the data on the server?*
- *How might the server impact the business if it were disabled?*

*The purpose of this assessment is to fortify the server that handles critical and sensitive business information. Since the employees in this business can connect from anywhere around the world, it also leaves gaps for any threat actors to take advantage of and possibly disrupt business operations.*

*It is important for the business to secure the data on this server to protect any accidental leaks of sensitive information, safeguard against external threats, and to stop inside actors from disrupting services as well. If the server was impacted, the business would be negatively affected.*

Risk Assessment

| Threat source | Threat event | Likelihood | Severity | Risk |
|---|---|---|---|---|
| *Competitor* | *Obtain sensitive information via exfiltration* | *1* | *3* | *3* |
| *Disgruntled* | *Alter/delete critical information.* | *2* | *3* | *6* |

|  |  |  |  |  |
|---|---|---|---|---|
| *employee* |  |  |  |  |
| *Malicious Software* | *Install persistent keyloggers on employee devices.* | *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.

The threat sources listed are common threat sources among companies that tend to be attacked. While the likelihood of each event happening is low, the chances of any of those events happening is a likely one.

## 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.