**Vulnerability Assessment Report**

**15th April 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 2024 to August 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

*The database is critical to the daily operations of the business as it’s regularly queried or read from by employees to help them find potential customers. Hence, any breach to the system will cause a temporary disruption of the company’s operations. And since the database interacts with other servers on the company’s internal network, this might lead to very serious breach of restricted data such as PII and SPII. There security controls must be implemented to restrict public access to the server and the data on it be secured to protect the company from potential threat actors.*

# Risk Assessment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| *Competitor* | *Obtain sensitive information via exfiltration. They can install persistent and targeted network packet sniffers on organisational information systems.* | *1* | *3* | *3* |
| *Hacker* | *Cripple the company through a ransomware attack which will cost the company a lot of money and their customers’ trust. They can also damage the company’s critical infrastructure by installing harmful malware.* | *3* | *3* | *9* |
| *Employee* | *A disgruntled employee seeking payback might delete or alter information that is critical to the day-to-day business operations.* | *3* | *3* | *9* |
| *Privileged User* | *Privilege Escalation* | *2* | *3* | *6* |

# Approach

Risks considered the ease of access and security of the data stored on the company’s server. The likelihood of a threat occurrence and the impact of these potential events were weighed against the risks to day-to-day operational needs.

Although competitors are an unlikely source of threat, they still pose a medium risk to the business as competitors with the capacity can install a malware that can track and recover top company secrets. This may eventually lead to a data leak that will quickly be acted upon by hackers if not remediated quickly. Disgruntled employees might alter or altogether delete sensitive data that will affect the day-to-day running of the business.

Since the database is open to the public, it makes it an easy target for threat actors who might cash in on the vulnerability by installing ransomware on the company’s systems. This will have disastrous consequences as the company’s daily operations will come to a halt until they can afford the ransom.

# 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 transit using TLS instead of SSL. IP allow-listing to corporate offices to prevent random users from the internet from connecting to the database. Implementing VPN’s will allow company employees to connect securely from their remote locations to internal systems.