**Vulnerability Assessment Report**

**18th October 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.

Notes

Open to public

Remote access for employees

# **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/1Fc4L2azQlnUM-8r43PU9mYlT30BnxTwdjAMqpT7JeZk/edit?resourcekey=0-Q-XglnC3Li7JPK2hIvMkVg#heading=h.hvbcmqwzo9do) is used to guide the risk analysis of the information system.

# **Purpose**

*This database stores and manages large amount of data important to the companies’ everyday operations. It holds customer PII among other data on customer to help coordinate tailored experiences and provide insightful analytics towards business improvement. This should be protected to remove the risk of disruption to daily operations, keep customer data confidential, ensure that data’s integrity and availability and comply with government regulations.*

**Risk Assessment**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| *Competitor* | *Obtain sensitive information via exfiltration* | *3* | *3* | *9* |
| *Malicious Actor* | *Ransomware attack for financial gain* | *2* | *3* | *6* |
| *Customer* | *Customer may accidently make alternations/deletions* | *1* | *3* | *3* |

# **Approach**

The risk measured in this assessment reviewed the storage and management procedures and practices for this organization. A combination of the likelihood of a security incident and severity resulting from that accident were considered to determine the risk level and potential threat in relation to the impact on daily operations.

**Remediation Strategy**

To reduce the risk of these threats I would recommend the implementation of authentication, authorization and auditing protocols. With special emphasis of strong and secure password policies, reinforced with the use of multifactor authentication. User access controls should be reviewed, and the policy of least privilege implemented. Data encryption should be exclusively carried out with TLS protocols not SSL and lastly IP addresses should add to allow-listing’ to ensure that only authorized business IP’s are accessing the data on the server.