**Vulnerability Assessment Report**

**9th 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 June 2022 to August 2023. [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**

The database is an organised store of information. It is used to store customer, orders and marketing data which can be used for analytic and directing marketing information. It is of importance to secure the database as it is used for all our customer acquisition efforts.

**Risk Assessment**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| *Hacker* | *Obtain sensitive information via exfiltration* | *3* | *3* | *9* |
| *Employee* | *Accidentally delete important information* | *2* | *3* | *6* |
| *Customer* | *Delete important information* | *1* | *3* | *3* |

# **Approach**

Risks that were measured considered the data storage and management procedures 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 severity of potential incidents was weighed against the impact on day-to-day operational needs.

# **Remediation Strategy**

Implementing the AAA framework helps to ensure that authorized users access the database server. This is through using strong passwords, role-based access controls and MFA to limit user privileges. Data in transit can be encrypted using TLS instead of SSL.