**Vulnerability Assessment Report**

**1st September 2023**

# 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 2023 to August 2023. [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 server is valuable to the business because like many assets it aids in the business functioning and within the database it contains a lot of Personally Identifiable Information (PII). It is important to secure the data on the database server since there are many threats that face an enterprise that contains assets such as PII and if the CIA triad is compromised with this asset this could damage the company’s business interests. The server is used to store customers, campaign, and analytic data that can later be analyzed to track performance and personalize marketing efforts. It is critical to secure the system because of its regular use for marketing operations. If the server is impacted the company will face a whole host of problems from litigations to financial impacts to also loss in reputation.

# Risk Assessment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| *Competitor* | Perform reconnaissance and surveillance of organization | *1* | *2* | *2* |
| *Employee* | Alter/Delete critical information | *2* | *3* | *6* |
| *Hacker/ Threat Actor* | Obtain sensitive information via exfiltration | *3* | *3* | *9* |

# Approach

Risks considered were 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. To have a successful business means to have competitors which would always try to gain an upper hand over your organization, and this could be done through performing reconnaissance and surveillance of your organization. However, since it would be regulated on what the competitors could do it is not likely that they would do anything malicious but if they are able to exploit a non-malicious vulnerability, it could reduce company function hence why the risk score is a 2. Because an employee would have access to sensitive data, though unlikely if POLP is adhered to, they could willingly or unwillingly alter or delete critical information. Which will severely impact business operation hence why it receives a risk score of 6. And of course a hacker/ threat actor that obtains sensitive information via exfiltration of data could cause major damage to the business and poses the highest risk (risk score 9).

# 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.