**Vulnerability Assessment Report**

**1st January 20XX**

# 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](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 a centralized computer system that stores a large amount of sensitive data, including customer information, data analytics, and marketing campaigns. Its significance lies in the critical nature of the information it holds, and it is regularly accessed and utilized by the marketing team.

# Any compromise to the security of this database would result in significant damage to the company's reputation. Furthermore, potential leakage of customer information may lead to regulatory fines. Additionally, the disruption of normal operations could result in considerable financial losses for the company. Therefore, ensuring the robust protection and integrity of the database is of utmost importance to safeguard the company's interests and maintain trust with its customers and stakeholders.

# Risk Assessment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| *Competitor* | *Obtain sensitive information via exfiltration* | *1* | *3* | *3* |
| *Competitor* | *Disrupt mission-critical operations.* | *1* | *3* | *3* |
| *Hacker* | *Obtain sensitive information via exfiltration.* | *3* | *3* | *9* |
| *Hacker* | *Conduct Denial of Service (DoS) attacks.* | *3* | *2* | *6* |
| *Employee* | *Alter/Delete critical information.* | *2* | *3* | *5* |
| *Employee* | *Disrupt mission-critical operations.* | *2* | *3* | *6* |

# 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.

# 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.