**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 server is used to search for potential customers and manages large amounts of data. The server used to store customer data can later be used to track performance. It is critical to secure the system because of it’s regular use for marketing operations.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| *Hacker* | *Obtain sensitive information via exfiltration* | *3* | *3* | *9* |
| *Employee* | *Disrupt mission-critical operations* | *2* | *3* | *6* |
| *Customer* | *Alter/Delete critical information* | *1* | *3* | *3* |

# 

# Approach

These three threats represent significant business risks as critical information can be lost and sensitive information about customers can be accessed. The severity of the potential incidents were weighed against the impact on day to day operations.

# Remediation Strategy

To alleviate these issues we will restrict access to the database to only employees that are required to use the database for their daily tasks. Implementation of MFA (Multi-Factor Authentication) and using strong passwords to limit user privileges. Also adding in auditing mechanisms to ensure that only authorized users are accessing the database server.