**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

This server hosting the database manages and stores data important for the everyday business operations of the company such as customers’ financial and personal information. A security incident that would detrimentally alter, delete, or cause the data to be stolen would have a negative impact on the operations of the company. The company would face significant financial loss due to a disruption in operations as well as in payments of fines caused by non-compliance with regulations to protect user data. Additionally, the company’s reputation and ability to do future business would suffer due to the perception of lack of security for the confidentiality, integrity and availability of user data.

# Risk Assessment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| *Internal users* | *Alter/Delete critical information* | *3* | *3* | *9* |
| *Interruptions due to service outages / natural disasters* | *Disrupt mission-critical operations.* | *1* | *3* | *3* |
| *Disgruntled employees* | *Obfuscate future attacks.* | *2* | *3* | *6* |

# Approach

The server hosting the database requires proper administration to minimize risk of a security incident. The most likely incident is the deletion or altering of data accidentally by internal employees who have access to the database. This could be customer data and the loss would violate the principles of data integrity and accessibility. Disgruntled employees may also install malware or other means to obfuscate future attacks, possibly hiding vulnerabilities such as misconfiguration of the database. Finally, and not as likely, the server can go down due to physical interruptions such as loss of power or natural disaster.

# 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.