**Vulnerability Assessment Report**

# 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 company stores information on a server, since many of the employees work remotely. Employees of the company regularly query, or request, data from the server to find potential customers. The server is crucial to the company’s operations, it contains PII and sensitive company data if misused it could cost the company business, public trust, and or money in the form of regulatory and or legal fines. The database has been open to the public since the company's launch three years ago.

# Risk Assessment

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

# Approach

The risks were considered based on their overall impact on the business. The threat sources were determined based on opportunity, potential motive, and potential gain for the source. The events were then selected by weighing the likelihood of the threat, the potential risk to the company, and how they might affect the company’s operations.

# Remediation Strategy

To remediate the potential security risks, we evaluated the risk and implemented solutions to ensure only authorized personal access the server. We can first secure the data in transit via TLS encryption instead of the current SSL encryption and use public key infrastructure (PKI) to address exfiltration of information. Next, we should establish who inside the company is authorized to access the server, how much access that individual needs, and a record of what takes place on said server with logs. Following this, institute a way to audit and authenticate these users to give them proper access whilst limiting the chances the authentication can be compromised. This can include things like passwords, role-based access, allow listing only necessary IP’s, scheduled password changes, and multi-factor authentication.