**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

Database server is responsible for storing employees data and it is used to find potential customers. It is important to improve secure valuable data contained in this database. In case of database compromise company activity could be stopped and user credentials could be stolen.

# Risk Assessment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| *E.g. Competitor* | *Obtain sensitive information via exfiltration* | *1* | *3* | *3* |
| *E.g. Hacker* | *Alter/Delete critical information* | *2* | *3* | *6* |
| *E.g. Hacker* | *Obfuscate future attacks.* | *2* | *2* | *4* |

# Approach

Risks considered the data storage and management methods of the business. Organization stores data in database publicly accessible which expose business on threat events like:

* Critical information is altered or deleted
* Sensitive information may be easily stolen from database
* Potential advanced persistent threat may obfuscate their future attacks using this attack surface.

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

Considering risks we recommend:

* Implementing AAA framework to ensure only authorized users can access database storage
* Implementing principle of least privilege and separation of duties to further reduce attack surface
* Proper maintenance of backup systems in case of data alteration or removal
* Encryption of data in motion using TLS instead of SSL