

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](#) is used to guide the risk analysis of the information system.

Purpose

As we know the database is used by employees working remotely throughout the World and they regularly query, or request data from the Server to find potential customers hence it is a very important and the sole server of the company, so it needs to be protected. Also, it stores customers data which are sensitive and needs to be protected for customers security and business continuity. If any attack happens on the database, it will impact the business in a very severe manner hampering everyday tasks of the employees.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker	Obtain sensitive information via exfiltration	3	3	9
Storage	The capacity of the Storage may exceed after a period of time due to everyday tasks.	2	3	6
Customer	Alter/Delete critical information	1	3	3

Approach

Risks that were measured considered the data storage and management procedures of the business. Potential threat sources and events were determined using the likelihood of a security incident given the open access permissions of the information system. The severity of potential incidents were weighed against the impact on 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.