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

Consider the following questions to help you write:

- *How is the database server valuable to the business?*
- *Database server contains all the data that a company owns and it is lcondiered next to life*
- *Why is it important for the business to secure the data on the server?*
- *In order toperform business, they need user data to work on such as a client*
- *How might the server impact the business if it were disabled?*
- *They won't be able to run the business*

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
E.g. Competitor	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*
Employee	*Insider threat*	*1*	*3*	*3*
Hardware issu e	*Leakage or data loss due to electrical*	*2*	*3*	*6*

Approach

Risks considered the data storage and management methods of the business. The likelihood of a threat occurrence and the impact of these potential events were weighed against the risks to day-to-day operational needs.The main reason i choosed competitor,hardware and Employee as a threat because,as soon as the word for database loss in heard into the market , this all the first person who have devil;s mind would strat doing the bad attempts to gain access and sell the same thing into black market

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.

1.backing up data

2. Multi factor authentication

3. Principle of least privilege works here.