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?*
- *Why is it important for the business to secure the data on the server?*
- *How might the server impact the business if it were disabled?*

The database server is very valuable to the business as it stores important information that the employees use regularly. It is important that the business secures the data on the server to prevent information from being stolen, which could lead to financial loss and detriment to the business' reputation. If the server was disabled, every day business activities would slow down, even coming to a halt.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
E.g. Competitor	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*
Hacker	*Conduct Denial of Service (DoS) attacks.*	*2*	*3*	*6*
Employee	*Alter/Delete critical information*	*1*	*2*	*2*

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.

I chose competitors, hackers, and employees, as they are all human threats that could easily access the database due to it being public. Anyone can access the public database, and this vulnerability can be easily exploited and lead to large financial loss, detriment to reputation, and can harm individuals whose SPII might be stored on the database.

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.

I recommend closing off the database server from the public, and only allowing people in the internal network to access the database. This would include role-based access controls, so that only authorized users can access the database. Additionally, I recommend implementing multi-factor authentication to further limit user privileges.