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 is valuable because it allows employees to work all around the world because it's stored in the cloud. It's important to secure the data because the database contains information that competitors could use in addition to the resources they have, that we don't. If the server were disabled, business operations would be tough to continue because the database relates to how potential customers are found

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Competitor	*Use the public information for their business benefit*	*3*	*1*	*3*

System Admin	*Alter/Delete critical information*	*1*	*3*	*3*

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 the threats above because they all come from different backgrounds. Hackers have malicious intentions, competitors have personal goals in mind, and system admins represent internal threats. I think these are significant threats because they show how threats can present themselves in various ways.

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 think the number one thing to do is not have the data be open to the public. This will manage the competitors' threat. As for hackers, hopefully the non-public database will discourage them from looking at the information. However, general security measures should be added just in case to prevent any hackers from attempting to steal information about customers, which could include PII. As for system admins, separation of duties could prevent one person from having too much power within the database.