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 purpose of this vulnerability assessment report is that this database server is not used by any malicious actors that may compromise the company. This data is valuable to the business because if any of the data were to be lost, customers will not be able to access and use our platform. If our data gets leaked by anyone, we may lose customers' trust and they may never use our product again. This server must be kept online as much as possible to prevent the loss of new customers and revenue.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
E.g. Competitor	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*

System Admin	Alter/Delete critical information	*3*	*3*	*9*
Nation State	Install persistent and targeted network sniffers on organizational information systems.	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.

These threat sources were chosen because if a competitor were to obtain information from us, it would lead to more competitors and affect our customers. Another thing that could happen is that critical information can be altered or deleted by a system admin, or a past disgruntled system admin. This can affect operations that are critical to our business and cause us to lose revenue. We considered that a nation state could install network sniffers on our systems, and decided that this is something important to consider because having foreign countries getting our data could lead to customer information being used against us.

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.

Our company should employ the principle of least privilege, so that employees have enough privilege to conduct their job. This can avoid accidental document leaks, data deletion, etc. We could implement separation of duties, to make sure multiple employees have specified roles.