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 holds all of the company's information in regards to their customers and research operations. The importance of database security is critical because the likelihood and severity of a threat event equate to a higher risk. If the server were compromised or disabled, the day to day operations would shut down immediately, and the business would be held liable for not properly protecting the accessibility of their customer data.

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	*3*	*3*	*9*

Employee	*Alter/Delete critical information*	*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 biggest threat, based on the risk score, is a hacker's ability to disrupt normal business operations since the database allows public remote access. A hacker would have no problem with conducting a DDoS attack and overloading the server, which calculates to the highest risk level of 9. The same goes for a disgruntled employee who already has open access and knowledge of the server's 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.

Principle of least privilege would ensure that users within the company are granted only the minimum level of access and authorization to complete the tasks necessary for normal business operations. This would prevent a disgruntled employee from being able to conduct anything malicious out of bad faith. In addition, this would reduce the overall risk of hackers having the ability to openly exploit the threat and performing things such as DDoS attacks.