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 important for the business as it communicates with other servers on the network, should anything happen to this database or its server hardware, the other servers will no longer be able to communicate with it. That is also why steps should be taken to protect the database itself in case of events such as human, technological or environmental threats. Should these threats manage to damage or impede the database, data loss can occur, alongside any financial complications due to the other servers not having access to the database.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker	*Threat source alters or deletes data that is critical to day-to-day business operations.*	*3*	*3*	*9*
DDoS	*Threat source sends automated, excessive requests to overwhelm the system's operating capabilities.*	*2*	*2*	*4*
Building fire	*The hardware that runs the server is completely destroyed due to a fire*	*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.

The three threat sources I identified; Hacker, DDoS and Fire, I believe are the most immediate threats to the business. The business's hardware is the one thing keeping the servers and database running, and should anything happen to the hardware, it could significantly affect business operations. For example, a building fire, if there isn't proper fire prevention and protection, damage to the business hardware and building itself will be costly. A DDoS attack can prevent normal business operation for a few days, and a hacker gaining access to the database to alter or delete critical data could seriously put the business and anything that relies on it at risk.

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*
    - *Should an internal user have more access than required, decide to abuse their power, or have its account compromised via password brute forcing, it could allow a hacker to alter or delete data and compromise internal systems.*
- *Defense in depth*
    - *Having the business's data behind multiple layers of defense can benefit tremendously in deterring or even preventing outside threats.*
- *Having proper safety systems*
    - *Proper physical security and systems can prevent things like an intruder gaining physical access to the server hardware, or having fire prevention systems to mitigate or prevent any possible harm to the hardware.*