Vulnerability Assessment Report

1st January 2025

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?*

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*
Aging Parts	*Deteriorate parts and cause failures*	*1*	*3*	*3*
Employee	*Accidental leakage of information*	*2*	*3*	*2*

Approach

These risks are somewhat standard concerns that a company should have. A competitor could access the information and minimal to significant impact on their company, though it is hard for them to infiltrate. Aging hardware could cause parts to deteriorate and would cause an expensive repair and loss, though unlikely. Lastly, an employee can unknowingly or accidentally leak information, though with proper power separation, the risk and exposure can be mitigated.

Remediation Strategy

A general use of MFA and restriction/separation of powers would help significantly. Additionally, performing maintenance on the software and hardware would help mitigate risks. Lastly, maintaining proper online security helps.