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

The purpose of this vulnerability analysis is to assess the effectiveness of current access controls on the organization's MySQL database server, which operates on a powerful Linux-based infrastructure. The server holds critical business data and facilitates secure communication across the network using SSL/TLS encryption. Securing this data is paramount for protecting customer information, ensuring regulatory compliance, and maintaining business operations. A compromise or disablement of the server could lead to operational disruptions, data breaches, financial losses, and reputational damage. This assessment aims to identify vulnerabilities and mitigate potential risks to maintain system integrity.

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*
Privileged User (System Administrator)	*A system administrator with excessive access could accidentally or intentionally alter critical data, misconfigure access controls, or introduce vulnerabilities by changing system settings.*	*2*	*3*	*2*

Hardware Failure (Storage or Processing)	*The server's hardware, such as its storage or CPU, could fail due to aging or resource depletion, leading to data loss or system downtime, disrupting business operations*	*2*	*3*	*2*
Advanced Persistent Threat (APT)	*APT groups could target the server to exfiltrate sensitive data or compromise its operations over time by exploiting vulnerabilities in the operating system or database software.*	*1*	*3*	*2*

Approach

I selected the three specific threat sources—Privileged User (System Administrator), Hardware Failure (Storage or Processing), and Advanced Persistent Threat (APT)—because they represent significant risks to the business due to their potential to disrupt critical operations. A privileged user has direct access to sensitive data and system controls, making accidental or intentional misconfigurations a serious risk. Hardware failures, while less likely, can lead to substantial downtime and data loss. APTs, though rare, pose a severe threat by exploiting vulnerabilities over time, potentially causing long-term damage to the organization.

Remediation Strategy

To address the identified risks, several security controls can be implemented. For the threat posed by a privileged user, enforcing the Principle of Least Privilege ensures that individuals only have access to the data and systems necessary for their roles, minimizing potential damage from misconfigurations or misuse. To protect against hardware failures, implementing Defense in Depth through regular backups and redundant systems will help mitigate data loss and downtime. For Advanced Persistent Threats (APT), Multi-Factor Authentication (MFA) and the Authentication, Authorization, and Accounting (AAA) framework can enhance security by ensuring robust verification and monitoring of user access, reducing the likelihood of unauthorized exploitation.