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

A company's server is crucial as it stores and manages vast amounts of data essential to the company's operations. Ensuring this data is safe and secure is paramount for maintaining a competitive edge and operational stability. Should the server be disabled, not only would business operations be affected, but essential data, confidential information, and other critical operational elements would also be compromised.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Employee	*Interrupt essential operations*	*2*	*3*	*6*

Customer	*Edit or delete critical information*	*1*	*3*	*3*

Approach

The assessed risks took into account the company's procedures for data storage and management. The probability of security incidents was evaluated based on the system's open access permissions, identifying potential threats and events. The potential impact of these incidents was then measured against their effect on the routine operational requirements of the business.

Remediation Strategy

The use of authentication, authorization, and auditing features guarantees that only permitted users can access the database server. This involves the adoption of strong passwords, access controls based on user roles, and multi-factor authentication (MFA) to restrict user access levels. Data being transferred is encrypted using TLS, upgrading from SSL for enhanced security. Additionally, IP allow-listing is implemented for corporate offices, blocking unauthorized internet users from accessing the database.