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 database server is valuable to the business because it stores and manages important data like customer information, financial records, and operational details. Without it, the company couldn't handle daily tasks or make decisions based on data.

It is important for the business to secure the data on the server to protect sensitive information from theft or damage. If data gets leaked, it could lead to loss of trust from customers, legal problems, or financial losses.

If the server were disabled, it might impact the business by stopping operations completely, causing downtime that loses money and customers. Employees couldn't access needed information, and it could take time to recover, hurting the company's reputation.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	Obtain sensitive information via	1	3	3

	exfiltration			
Hacker	Perform reconnaissance and surveillance of organization	3	3	9
System administrator	Alter/Delete critical information	2	3	6
Advanced persistent threat (APT)	Install persistent and targeted network sniffers on organizational information systems	2	3	6
Malicious software	Conduct Denial of Service (DoS) attacks	3	2	6
Outages	Disrupt mission-critical operations	1	3	3
Hacktivist	Conduct "man-in-the-middle" attacks	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.

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.