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 assessment is to measure the possible vulnerabilities that might happen. This server is a database server for an e-commerce company that stores all data in it. If the database server were to go down, all network/services connected will go down and rendered offline. It is important to keep the database encrypted and only authorized users are able to access the server.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Malicious threat actor	*Encrypt database server and ask for a ransom*	*3*	*3*	*3*
Alter/Delete critical information	*Threat source alters or deletes data that is critical to day-to-day business operations.*	*3*	*3*	*3*
Install persistent and targeted network sniffers on organizational	*Threat source installs software designed to collect (sniff) network traffic over a continued period of time.*	*1*	*3*	*3*

information systems.				

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 likelihood of threat actors deleting or altering information is a lot more common since the database is accessible to anyone.

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.