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 is used by multiple remote workers from all around the world. These employees regularly access the data from the server to find potential customers. It is important to the working of the business that the server remains operational. If the server were to be disabled, a lot of employees would no longer be able to function.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacktivist	Denial of Service attack	*3*	*2*	*6*
Thief	Eavesdropping on sessions to steal data	3	*3*	*9*
Customer	Alter/Delete critical information	*2*	*2*	*4*

Approach

The database seems to be public, so it can be accessed and eavesdropped on by anyone. To illustrate how badly this can go wrong, I have picked three threat sources that would cause considerable financial and reputational damage.

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.