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 remote database server is publicly accessible and is used to store company's information. The company's employees regularly query the database from different parts of the world for information about the potential customers. It is very important to protect the database from different threats that could jeopardize the server as it stores valuable information about customers, loss of which could result in serious damage to the company's business. If an attack manage to disable the server or cause data leak about the customers it could lead to catastrophic damage to company's operations and it's reputation. So it is of great importance for the company to assess the server for the potential vulnerabilities and ways to remedy those vulnerabilities to minimize the impact of an attack on company's operations.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker	*Obtain sensitive information via sniffing data packets over the network*	*3*	*3*	*9*
Employee	*Accidnetally alter or delete the*	*2*	*3*	*6*

	information critical for day-to-day operations			
Competitor	*Flood the server with IP requests with a DDoS attack*	*1*	*3*	*3*

Approach

Risks considered the remote data base server, and the public access to the database. 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. The database should be made private as public access to the database is a serious vulnerability that the threat actors could exploit. SSL/TLS encryprion should be used to protect data in transit. Firewall should be utilized to filter traffic going to and out of the database server. Employees should only have the access to the minimum resources to do the task. Multi-factor authentication and role-based access should be implemented for the employees to avoid risk of unauthorized remote access. Frequent vulnerability assessments should be enshrined in the company policy to keep the company's assets protected from the ever evolving threats.