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 company operates with a remote database server to accommodate its globally distributed workforce. Employees frequently access and query the server to retrieve information about potential customers for business operations. Ensuring the security of the server is essential to maintain regular business activities.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Customer	*Alter/Delete critical information*	*2*	*2*	*4*
Hacker	*Conduct "man-in-the-middle" attacks.*	*3*	*3*	*9*

Approach

Risks were evaluated , considering the potential risks associated with an open database accessible not only by employees but also by the public. Likelihood and severity scores were assigned based on the threat level each threat posed to the company.

Remediation Strategy

Robust security measures for its database, including proper authentication and authorization protocols for users/employees. Access control measures and password policies to regulate database access. Additionally, the system should be configured to permit access only from the company's employees' subnet, enhancing security. Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) in place to identify and thwart unauthorized attempts to access the database.