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 a valuable resource for remote employees to access potential customer information. Because this server hosts information that may be of value to competitors or nefarious threat actors, as well as being public facing, it is critical to secure it from attacks. The possibility of a downed service would halt the work of remote employees and their ability to seek new customers, negatively impacting the business revenue.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
DoS or DDoS	Threat source sends automated, excessive requests to overwhelm the system's operating capabilities.	*2*	*3*	*6*
Competitor, Hacker, Nation state, Employee	Obtain sensitive information via exfiltration	*2*	*3*	*6*

Competitor, Hacker, Nation state, Employee	Perform reconnaissance and surveillance of organization	*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. Most security threats would be attacks on the server, given its public posture. This could range from script-kiddies to nefarious threat actors to nation state actors, given the business this organization conducts.

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.