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. Plus, the scope of this assessment only relates to the confidentiality, availability, and integrity of the data on the server—not the physical security of the server or its related IT systems.

Purpose

The database server is valuable to the business because the company stores information on it where employees of the company regularly query, or request, data from the server to find potential customers. It is important for the business to secure the data on the server to ensure the confidentiality, availability, and integrity of the data of potential customers that employees regularly query. If the database server were disabled by a Denial of Service (DoS) attack, this may finanically and reputationally impact the company in a negative manner,

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
E.g. Competitor	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*
Former Employee	Alter data in a way that negatively impacts the company	*2*	*3*	*6*

Hacker	Conduct Denial of Service (DoS) attacks. Send automated, excessive requests to overwhelm the system's operating capabilities	*3*	*3*	*9*
Nation state	Exploit cyber resources	*2*	*3*	*6*
Hacktivist	Perform reconnaissance and surveillance of organization	*1*	*3*	*3*

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.

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. Implentation of Defense in depth approach to reduce risk assoiacted with a publicly accessible database server. This includes moving the publicly accessible database server into the internal network behind a gateway server where only authorized users access it.