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 stores and manages large amounts of data. This data is used for tracking customer spending habits, market trends, marketing personalization. Many departments in the business depend on the data to function, thus any interruption would have a severe impact on the business.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Customer/Employee	*Alter/Delete critical Information*	*2*	*3*	*6*
Employee/Customer	*Disrupt mission-critical operations*	*2*	*3*	*6*

Approach

With the database being open to the public, the potential threats have many opportunities to affect our database. Given the open nature of our database, the likelihood and severity of a security event is high.

Remediation Strategy

First, our database should only be accessible by authorized users. We need to implement the AAA framework and the principle of least privilege to help reduce users from having unneeded access to systems that don’t meet the scope of their duties.