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

Hello everyone! The reason I am conducting this vulnerability assessment, besides it being standard routine for cyber security, is that it has been brought to my attention that the remote database server utilized by the company has been open to the public for the past three years. The database is essential to daily operations, and for employees to access information and materials to do their work. It is critical to secure the server; while the last three years of good luck could continue, it is very likely that one single threat could bring the business to its knees. The ramifications for this to occur, would be severe and numerous. To name a few: the reputation of the company could be irreversibly damaged, serious financial damage if the server is brought down for multiple days, and legality could also come into question in the aftermath, potentially creating an issue with the law.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	Perform reconnaissance and surveillance of organization	*2*	*3*	*6*
Hacker	Obtain sensitive information via exfiltration	*3*	*3*	*9*
Advanced persistent threat (APT)	Conduct Denial of Service (DoS) attacks	*2*	*3*	*6*

Approach

Here I have identified three threat sources and corresponding threat events that range from very likely to almost certain if the database remains public. First competitors could find themselves encouraged with the lack of security and use this public access to perform reconnaissance and surveillance of the company, being able to easily anticipate how best to perform against the company. Next is the almost certain scenario being that a hacker(s) obtains sensitive information via exfiltration, leaving things as-is renders it easy pickings for them to do just that. And lastly, if any threat source has gained unauthorized access, they could install themselves as an advanced persistent threat and conduct constant denial of service (DoS) attacks.

Remediation Strategy

To remediate these vulnerabilities, I propose the following. 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.