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

Consider the following questions to help you write:

- *How is the database server valuable to the business?*
- *Why is it important for the business to secure the data on the server?*
- *How might the server impact the business if it were disabled?*

The database server is the most valuable asset because it stores the company's information which employees utilize daily. The server has been public since the company's launch but it is a serious security vulnerability. Anyone outside the company can access customers' data without their consent and use or edit it maliciously. It is also an access point that hackers can use to access the company's network and resources. If any of these events occurred it would negatively impact the company's reputation and finances.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Obtain sensitive information via exfiltration.*	*2*	*3*	*6*

Hacker	Conduct "man-in-the-middle" attacks.	*3*	*3*	*9*
employee	Alter/Delete critical information	*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.

The top three threats to the database server because of its public access are competitors, hackers, and employees. There is a low likelihood that an employee could delete or alter critical information because there is no user permissions management on the public server. And with the server being public there is a higher likelihood that competitors could use data exfiltration to steal sensitive information. The most concerning risk is a hacker conducting “man-in-the-middle” attacks on remote workers to steal sensitive information because of the greater likelihood and high severity. The server must change from public to exclusive accessibility to secure the company’s assets.

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.

My proposed remediation strategy to improve the server’s security uses the authentication, authorization, accounting (AAA) framework, and defense-in-depth strategy. The AAA framework would combat data exfiltration and unauthorized changes with user privileges to prevent unauthorized access to data and user activity logs to track suspicious activity. The defense-in-depth strategy can reduce “man-in-middle” attacks by adding multi-factor authentication to the AAA framework-required login system. It can also prevent “man-in-the-middle” attacks by adding a firewall with an intrusion detection and prevention system to the database server. These solutions will fix the vulnerability of our current public server.