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?*

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker	*Can install software designed to collect (sniff) network traffic. A "man-in-the-middle" attack is also possible.*	*3*	*3*	*9*
Employee	*Can alter or delete data that is critical to day-to-day business operations.*	*2*	*3*	*6*
Competitor	*Obtain sensitive information via exfiltration*	*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. Based on a quality assessment, the public access vulnerability to the database makes the organization particularly susceptible to outside threats. This easy access significantly raises the likelihood of outside threat actor exploitation, going from the practice of techniques to deliberate sabotage of this company's reputation and operations. Additionally, the lack of robust access controls and audit logs raises the risk of internal mistakes or even malicious actions by employees.

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.

Authentication, authorization, and auditing (AAA) plus strong passwords, role-based access controls, and multi-factor authentication highly mitigates the risk of an actor stealing the identity of an employee or conduct actions posing like one.

IP allow-list would make it more difficult to an outside threat actor connect to the database denying a connection immediately.

Encryption of data in motion using TLS mitigates the risk known as “man-in-the-middle”, that is the act of intercept and modify data packages in transit (mostly to try to impersonate an authenticated user to the system), to take place because of the encapsulation and encryption adopted.