Vulnerability Assessment Report

1st January 2025

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 purpose of this vulnerability assessment report is to have an internal review process of an organizations security systems. In other words, the purpose is to identity weak points and prevent attacks. The database server is valuable to the business because it manages large amount of data that consists of store data that can later be used for multiple reasons. Therefore by securing the data businesses can come back and use the following for multiple occasions when needed. If the server were to be disabled, there would be potential operational disruption, financial loses, customer impact, and data integrity.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker	*Obtain sensitive information via exfiltration*	*3*	*3*	*3x3=9*
Standard User	Alter/Delete critical information	*2*	*3*	*2x3=6*
Group	Perform reconnaissance and surveillance of organization	*1*	*2*	*1x2=2*

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. Therefore I selected these three threat sources because they pose significant risks to the organization due to their high likelihood of occurrence and potential impact on operations.Those being hacker, standard user, and group as they each have a likelihood of happening when working for an organization.

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. I would also install the use; principle of least privilege, to ensure that we minimize unauthorized access, MFA to further enhance protection and identification, and lastly AAA to monitor logs. I would also ensure to have a team meeting so that all employees are aware of the new security standards and systems.