Vulnerability Assessment Report

26th October 2023

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 2023 to August 2023. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The purpose of the vulnerability assessment is to make sure that the server's functions are not affected by circumstances or event that could compromise the confidentiality, integrity and availability of the information stored in the database. The database is an essential instrument, and it is used daily by the business to provide services to the customers. It is fundamental that all sensitive information is kept safe by applying the right security measures and prevent any threats from exploiting vulnerabilities. Were the server disabled, the company could incur in monetary loss and reputational damage.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker	*Obtain sensitive information through exfiltration.*	*3*	*3*	*9*
Employee	*Alter/Delete critical information.*	*2*	*3*	*6*
Competitor	*Disrupt mission-critical operations.*	*1*	*3*	*3*

Approach

Risks that were measured considered the data storage and management procedures of the business. Potential threat sources and events were determined using the likelihood of a security incident given the open access permissions of the information system. The severity of potential incidents was weighed against the impact on day-to-day operational needs.

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.