Vulnerability Assessment Report

16st 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 September 2023 to November 2023. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The database server contains information important to the company. It is critical that proper security measures are in place as it is valuable information to the company. Server down time would impact the business productivity.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Employee	*Alter/Delete critical information*	*1*	*3*	*3*
Hacker	*Obtain sensitive information via exfiltration*	*2*	*3*	*6*
Competitor	*Perform reconnaissance and surveillance of organization*	*2*	*3*	*6*

Approach

There is a risk that an employee might alter or delete critical information as employees/customers regularly access data from the server. As the database has been open to the public since the company's launch three years ago, competitors might have been assessing potential vulnerabilities over time using various tools. A hacker might also conduct a Denial of Service attack (DOS) which would impact business information availability. 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 were 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. IP allow-listing to corporate offices to prevent random users from the internet from connecting to the database.