Vulnerability Assessment Report

1st January 2024

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 2024 to August 2024. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The database server is a valuable asset to business; this is where customers information and business products are stored. It must be protected at all levels, if compromised it can lead to fine and loss of customer trust. This can spoil the reputation of the company and reduce business productivity.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Employee	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Hackers	*Perform reconnaissance and surveillance of organization*	*2*	*3*	*6*
Hacktivist	*Delete the entire information in the database*	*3*	*3*	*9*

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 were weighed against the impact on day-to-day operational needs.

Remediation Strategy

In order to secure the database server system some security control has to be put in place; the database should be kept private. Firewall should be installed to keep out intruders from accessing the database server. Only specific employment should be able to access it with least privilege and MFA should be enabled.

The use of a firewall will prevent an attacker from gaining access into the system, if they do the MFA will prevent single password login into the system.

This assessment will help the organization avoid paying fines and help to grow business continuity.