Vulnerability Assessment Report

25th July 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 July 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 is valuable to the business because it stores critical data that is used to run the business. This data could include customer information, financial information, product information, and employee information. If the database server were to be compromised, this data could be stolen or corrupted.*
- *It is important for the business to secure the data on the server because this data is confidential and valuable. If the data were to be stolen or corrupted, it could have a significant impact on customer trust levels, as well as financial losses.*
- *If the database server were to be disabled, it could have a significant impact on the business and it could cripple the business's ability to operate effectively.*

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Operational Environment	*Humidity controls are left unchecked*	*1*	*3*	*3*
Technological	*The aging of hardware as it gets older, could present security holes.*	*2*	*3*	*6*

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

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.