Vulnerability Assessment Report

3rd August 2023

System Description

The server hardware consists of a powerful CPU processor and 128 GB of memory. It runs on the latest version of the 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 August 2023 to October 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 and manages critical company data, such as customer information, sales records, inventory data, and other important business-related information.

Securing data on a server is of paramount importance for businesses because securing data on a server is essential to safeguard sensitive information, maintain compliance with regulations, preserve reputation and trust, ensure business continuity, and prevent financial losses. Businesses that prioritize data security demonstrate their commitment to responsible data stewardship and contribute to long-term success.

A disabled server can have cascading effects that impact multiple aspects of a business's operations, leading to financial losses, decreased productivity, damaged reputation, and potential legal liabilities. As a result, maintaining the availability and reliability of the server is crucial for the business's overall stability and success.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker	• *Obtain sensitive information via exfiltration*	*3*	*3*	*9*

Employee	● *Disrupt mission-critical operations* ● *Accidentally download malicious software to the company PC*	*2*	*3*	*6*
Customer	● *Misuse of resources* ● *Malicious intent* ● *Data breaches*	*1*	*3*	*3*

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.

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.