Vulnerability Assessment Report

14th January 2025

System Description

The server hardware consists of a powerful CPU processor and 128GB 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 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 used to store large amounts of customer data, purchase data and item data. This data is used to analyze customers buying trends and patterns which the marketing team can use to build effective campaigns and promotional material. It is critical to secure this system because of its regular use for business operations and to meet the compliance standard in regard to storing PII.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*
Employee	*Alter business-critical information/operations*	*2*	*3*	*6*
Hacker	*Exfiltrate sensitive information.*	*3*	*3*	*9*
Customer	*Alter/delete critical information*	*1*	*3*	*3*

Approach

Evaluated the risks related to how the organization stores and manages data. Identified potential threats and considered the likelihood of these issues or incidents occurring. Paid special attention to the open access system, where too many people can access sensitive information. Also analyzed the critical impact on the business if an issue or incident occurred. Considered the compliance regulations that need to be met to store and manage PII (Personally Identifiable Information) and assessed how potential issues could affect the organization's reputation and finances.

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.