Vulnerability Assessment Report

25th September 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 June 2023 to August 2023. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The e-commerce company utilizes their database as a centralized location for consumer information that employees access remotely. This data is obtained to identify potential customers and generate reports on the company's marketing activities. It is important to ensure that the information within the database is secured for business continuity.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
APT	Alter/Delete critical information	*3*	*3*	*9*
Competitor	Disrupt mission-critical operations.	*2*	*2*	*4*
Employee	Perform reconnaissance and surveillance of organization	*1*	*3*	*3*

Approach

Risks considered the data storage and management methods of the business. Given the public access of the database, threat sources can come from APT's and Competitors. Internal security is also at risk because employees will be able to perform reconnaissance within the organization database and identify data that our competitors may want. 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. Apply principles of least privilege to prevent access to data from unauthorized individuals. Ensure that all logs relating to database access are set to the organizations SIEM so it can be monitored for suspicious activity.