Vulnerability Assessment Report

1st January 2025

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 202 to August 2025. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The company's primary database is stored in a remote server because many of its employees are remote workers. The database is constantly accessed or queried by the employees to get information. The database is a centralized computer system and contains a lot of data. The database is significantly useful for the company as it stores customer and campaign data that can be analyzed to perform personalized campaigns. Since this database is used frequently by employees of the company to perform analysis and operations, it needs to be secured.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Obtain sensitive information via exfiltration*	*3*	*2*	*6*
Employee	*Disrupt marketing operations*	*2*	*3*	*6*
Storage	*Any damage to data could make it unretrievable since there are no backups*	*2*	*3*	*6*

Approach

Since the database is publicly accessible, the organization's competitor will also be able to access the database. This can leak the company's campaign insights and marketing strategies to the competitors. Leaking confidential information, such as company performance and marketing strategies, to the competitor can cause severe financial losses to the company. The likelihood of obtaining the information is high because the database is publicly accessible and this is a moderately severe threat because it can cause some serious financial losses. An employee can also mishandle the data and hinder operations from occurring within the database. This can hinder the company from functioning successfully. Damage to the remote data server can lead to data loss, and since there are no additional backups to the database, the lost data could potentially never be recovered. This is a severe threat because loss of data can severely hinder company's operations.

Remediation Strategy

The organization should make the database secure and give access to only employees who need the data. The company should follow the principle of least privilege where employees should only be given the necessary access to perform their work and not any more. This ensures that employees don't have access to all the resources within the company and minimizes an employee being a threat source. Configuring a firewall or encrypting the database at rest is the best way to protect the database from public access. Additionally backing up the data in multiple data centers is a good practice because it supports failover. For example, if the database in the primary location failed, then we could easily retrieve data from the backups.

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.