Vulnerability Assessment Report

22nd July, 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 i nteracts 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 April 2025 to June 2025. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

This database is a centralized system used by on-site and remote workers which stores large amounts of data that are regularly accessed. The server contains customer information - Personally Identifiable Information (PII)-, campaign data, and analytics that can be used to track performance and personalize marketing efforts, and yet it is open to the public. This database is important to the company as it is useful for its growth and has an impact on its public-facing reputation. The data must be secured because a breach of customer data can impact the company both financially and from a reputationally if that PII were to be leaked. It is also important to protect against the possibility of a ransomware attack by a malicious actor or actors. If the server were to be disabled, the ability of its employees would be severely compromised as it is used multiple times a day by multiple users.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Outsider	*A malicious actor gains access to the database and initiates a ransomware attack.*	*3*	*3*	*9*
Standard user	*Wrong or inaccurate data gets added or edited as this is a public server*	*1*	*2*	*2*
Customer	*Able to access, change, or delete their data or that of someone else*	*1*	*2*	*2*

Approach

The reason behind the listed risks is that this is a server that is of high value to the company but is currently open to the public. The focus of this was on its data management. This openness allows anyone to gain access to information about customers and therefore has a high impact on business productivity and their reputation. The risk factors were determined based on the likelihood of a security incident . The severity values were based on the potential impact on both day-to-day operations , regulatory concerns and the reputation of the company.

Remediation Strategy

Recommendations are as follows : A need for stronger user authentication, authorization and data auditing measures is noted. As such, the server should no longer be open to the public but should have as a baseline strong password or Two Factor (2FA) or Multi Factor (MFA) Authentication to allow access to its data. User groups and roles should also be established to better enable access controls on who is allowed access to certain areas of the data and for how long . As many employees are remote, a VPN should be set up and added to each employee system to better control who can see and access the server.

The data on the server should also be encrypted using hashing and in particular Secure Hashing (SHA)SHA-1 at aminimum but recommend SHA-224 as this concerns customer data.

Doing this will improve the overall security of the company by ensuring that the data that is needed both for the employees to function and is available to only them and that the customer's PII is protected.