Vulnerability Assessment Report

8th May 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 2025 to August 2025. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The server is used to store customer, campaign, and analytic data that can later be analyzed to track performance and personalize marketing efforts. It is critical to secure the system because of its regular use for marketing operations. The purpose of this vulnerability assessment is to determine if the current access controls allow the database server to be exploited by malicious groups or outsider threats by obtaining sensitive information via exfiltration or by altering or deleting critical information. This ensures the business maintains an excellent reputation and avert any additional expenses by preventing malicious attacks.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	Perform reconnaissance and surveillance of organization	3	2	6
Hacker	Obtain sensitive information via exfiltration	3	3	9
Customer	Alter/delete critical information	1	3	3

Approach

The threat sources were chosen due to the server being open to the public for 3 years. This means the greatest threats are human. Competitors can access the server to steal customers, contacting them first, and robbing the company of its potential business. Hackers can obtain PII of potential customers from the database, ruining the company's reputation; however, hackers could also obtain sensitive information about employees that can cause much greater harm if they gained access to the network. Customers could alter information about their dealings with the company to steal goods and services or delete information about themselves and other customers.

Remediation Strategy

The database server has already been open to the public for 3 years; that threat cannot be fixed. However, implementing authentication, authorization, and auditing mechanisms to ensure that only authorized users access the database server would reduce the likelihood and severity of threats. I recommend using strong passwords, role-based access controls, and multi-factor authentication to limit user privileges. Finally, encrypt data in motion using TLS.