Vulnerability Assessment Report

1st August 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 database server functions as a central computer system designed for the storage and management of extensive data volumes. This server serves the purpose of housing customer, campaign, and analytic data, which can subsequently undergo analysis to monitor performance and customize marketing endeavors. Securing this system is of paramount importance due to its frequent utilization within marketing operations.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Malicious Actor	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Employee	*Disrupt critical operations*	*2*	*3*	*6*
Customer	*Alter/Delete critical information*	*1*	*3*	*3*

Approach

Evaluated risks encompassed the business's data storage and management protocols. The identification of possible threat origins and occurrences relied on assessing the probability of a security breach in light of the information system's unrestricted access permissions. The seriousness of potential incidents was balanced against their effect on everyday operational requirements.

Remediation Strategy

Deploying authentication, authorization, and auditing mechanisms is crucial to guarantee that solely sanctioned users gain entry to the database server. This encompasses the adoption of robust passwords, access controls grounded in user roles, and multi-factor authentication to curtail user rights. Employing TLS for data in transit encryption instead of SSL enhances security. Moreover, implementing an IP allow-listing approach confines database access to corporate offices, averting unsanctioned internet-based users from establishing connections.