Vulnerability Assessment Report

1st October 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 October 2023 to December 2023. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The database server is a centralized computer system that stores and manages large amounts of data. 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.

Risk Assessment

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

Approach

The risks were assessed by evaluating the data storage and management procedures within the business. Potential threat sources and events were identified by analyzing the likelihood of security incidents occurring due to the open access permissions in the information system. The severity of potential incidents was carefully evaluated in relation to their impact on the day-to-day operational requirements.

Remediation Strategy

The implementation involves deploying authentication, authorization, and auditing mechanisms to safeguard the database server, ensuring access is restricted to authorized users. This encompasses the use of robust measures such as strong password protocols, role-based access controls, and multi-factor authentication to restrict user privileges effectively. Additionally, data in transit is secured by employing TLS encryption instead of SSL. Furthermore, IP allow-listing is enforced for corporate offices to prevent unauthorized connections from random internet users to the database.