Vulnerability Assessment Report

January 5, 2024

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 January to June. 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 assessed risks evaluated the data storage and management practices within the organization. Threat sources and potential events were identified based on the probability of security incidents due to the system's open access permissions. The severity of potential incidents was assessed relative to their impact on daily operational requirements.

Remediation Strategy

To secure the database server, I implemented authentication, authorization, and auditing measures. This involves employing robust passwords, role-based access controls, and multi-factor authentication to restrict user privileges. We also use TLS for encrypting data in transit, replacing SSL. Additionally, we restrict database access to corporate offices through IP allow-listing to prevent unauthorized connections from internet users.