Brijen Jayeshbhai Shah

Vulnerability Assessment Report

Mar 28, 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 Dec 2023 to March 2024. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The database server serves as a centralized computing system responsible for storing and overseeing substantial data volumes. It functions as the repository for customer details, campaign information, and analytical data, which are subsequently utilized for performance monitoring and tailoring marketing strategies. Ensuring the security of this system is paramount due to its frequent utilization in 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 assessment of risks involved an evaluation of the data storage and management protocols within the business. Identification of potential threat sources and events was conducted by assessing the probability of a security breach considering the unrestricted access permissions of the information system. The severity of potential incidents was then compared against their impact on the business's daily operational requirements.

Remediation Strategy

The implementation of authentication, authorization, and auditing mechanisms aims to restrict access to the database server solely to authorized users. This involves employing robust password policies, role-based access controls, and multi-factor authentication to manage user privileges effectively. Additionally, data transmission security is enhanced by encrypting data in transit using TLS protocol, replacing less secure SSL. To further bolster security, IP allow-listing is enforced, restricting access to the database server only from corporate office networks and preventing unauthorized connections from the internet.