Vulnerability Assessment Report

29th November 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. 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*	*3*	*3*	*9*
Employee	*Disrupt critical operations*	*2*	*3*	*6*
Customer	*Alter/Delete critical information*	*1*	*3*	*3*

Approach

The evaluation assessed risks associated with the business's data storage and management protocols. It identified possible threat origins and occurrences based on the probability of a security breach due to the information system's unrestricted access permissions. The potential severity of incidents was balanced against their impact on daily operational requirements.

Remediation Strategy

Deploying authentication, authorization, and auditing protocols guarantees restricted access to the database server, permitting only authorized users. This encompasses reliable password structures, role-centered access management, and multi-layered authentication to restrict user permissions. Employing TLS encryption for data in transit rather than SSL enhances security. Furthermore, employing IP allow-listing for corporate offices prevents unauthorized internet users from connecting to the database.

Alexander Lungu