Vulnerability Assessment Report

18th November 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 June 2024 to August 2024. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The database server is a central system that holds a large amount of data, including customer information, campaign details, and analytics. This data is used to evaluate performance and create more personalized marketing strategies. Protecting the server is important because it plays a key role in everyday marketing operations.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker	*Disrupt mission-critical operations.*	*3*	*3*	*9*
Networking	*Install persistent and targeted network sniffers on organizational information systems.*	*2*	*2*	*4*
Communications	*Conduct "man-in-the-middle" attacks.*	*2*	*1*	*1*

Approach

These risks are considered due to the network connection and security measures. The likelihood of a threat occurrence and the impact of these potential events were weighed against the risks to day-to-day operational needs.

Remediation Strategy

Implementation of authentication, authorization, and auditing mechanisms to ensure that only authorized users access the database server. This includes using strong passwords, role-based access controls, and multi-factor authentication to limit user privileges thereby limiting the amount of data a potential sniffer can capture, as it requires users to authenticate themselves before gaining access to network resources.