Vulnerability Assessment Report

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

Purpose

The server is a centralized database that stores and manages large amounts of data. This system is regularly used for critical aspects of marketing operations for the company. These aspects include customer, analytical, and campaign data that is constantly being analyzed to marketing performance and customer specific personalized marketing campaigns.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Employee	*Insider, retaliation-based, threat*	*2*	*3*	*6*
Hacker	*DDoS attack that leaves vital servers unreachable*	*2*	*3*	*6*
Competitor	*Infiltrate company servers and extract sensitive data to gain an advantage*	*1*	*3*	*3*

Approach

Risks considered the data storage and management methods of the business. The likelihood of a threat occurrence and the impact of these potential events were weighed against the risks to day-to-day operational needs. The assessment focused on the three most likely origins and their potential impact.

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. Encryption of data in motion using TLS instead of SSL. IP allow-listing to corporate offices to prevent random users from the internet from connecting to the database.