Vulnerability Assessment Report

5th October 2023

Carried out by Chidubem Onochie-Onyetenu

System Description

The server has a high-performance central processing unit (CPU) and 128 gigabytes of memory. It runs the Linux operating system and hosts a MySQL database management system. It is configured with a stable network connection using Internet Protocol version 4 (IPv4) addresses and interacts with other servers on the network. Security measures include Secure Sockets Layer and Transport Layer Security (SSL/TLS) encrypted connections.

Scope

This assessment covers the current access controls of the system, from October 2023 to January 2024. NIST SP 800-30 Rev. 1 guides the risk analysis of the information system.

Purpose

The database server is a centralized computer system that stores and manages large amounts of data. It holds customer, campaign, and analytics data, which the company analyzes to track performance and personalize its marketing efforts. Securing the server is critical because marketing operations rely on it every day.

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

This assessment considered the company's data storage and management procedures. Threat sources and threat events were identified by how likely a security incident is, given the server's open access permissions. The severity of each potential incident was weighed against its impact on day-to-day operations. Each risk score is the likelihood multiplied by the severity, with both rated from 1 (low) to 3 (high).

Remediation Strategy

Implement authentication, authorization, and auditing mechanisms so that only authorized users can access the database server. This includes strong passwords, role-based access control, and multi-factor authentication to limit user privileges. Encrypt data in transit using Transport Layer Security (TLS) instead of Secure Sockets Layer (SSL). Allow-list the Internet Protocol (IP) addresses of corporate offices so that random users on the internet cannot connect to the database.