Vulnerability Assessment Report

3 March 2024

System Description

The server is equipped with a potent CPU processor and 128GB of memory. Operating on the most recent version of the Linux operating system, it serves as the host for a MySQL database management system. Its network configuration ensures a steadfast connection via IPv4 addresses, facilitating interaction with other servers on the network. Security is reinforced with SSL/TLS encrypted connections.

Scope

The vulnerability assessment will focus on evaluating the existing access controls of the system. This assessment will span a three-month period, from June 20XX to August 20XX. The risk analysis of the information system will adhere to the guidelines outlined in NIST SP 800-30 Rev. 1.

Purpose

The database server serves as a central hub for storing and managing extensive datasets. It holds crucial information such as customer details, campaign data, and analytics, which are instrumental in monitoring performance and tailoring marketing strategies. Given its pivotal role in marketing operations, securing the system is paramount to safeguarding sensitive data and ensuring uninterrupted business functions.

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

Risk assessments were conducted by evaluating the data storage and management protocols within the business. Potential threat sources and events were identified based on the likelihood of security incidents occurring due to the open access permissions of the information system. The severity of these potential incidents was assessed by considering their impact on day-to-day operational requirements.

Remediation Strategy

To enhance security, the following measures will be implemented for the database server:

Authentication, Authorization, and Auditing Mechanisms: Robust authentication mechanisms, such as strong passwords and multi-factor authentication, will be enforced to verify the identity of users. Role-based access controls will be implemented to assign privileges based on job roles. Additionally, auditing mechanisms will be put in place to monitor and record user activities for accountability.

Encryption of Data in Motion: Data transmission will be secured by using Transport Layer Security (TLS) encryption instead of Secure Sockets Layer (SSL) to protect data while it's in transit. This ensures that sensitive information remains encrypted and unreadable to unauthorized parties during communication between clients and the server.

IP Allow-listing: Access to the database server will be restricted to specific IP addresses associated with corporate offices. By implementing IP allow-listing, unauthorized access attempts from random users on the internet will be prevented, reducing the risk of unauthorized access and potential security breaches. By implementing these measures, the security of the database server will be significantly enhanced, mitigating risks associated with unauthorized access and data breaches.