Vulnerability Assessment Report

1st January 2025

System Description

The server, operating on the most recent version of the Linux operating system, is equipped with a high-performance CPU, 128GB of memory, and a MySQL database management system. The server utilizes IPv4 addresses for network connectivity and SSL/TLS encryption protocols for security purposes.

Scope

The scope of this vulnerability assessment is limited to the system's current access controls and encompasses the three-month period from June 2024 to August 2024. The risk analysis of the information system adheres to the guidelines established in NIST SP 800-30 Rev. 1.

Purpose

The database server, integral to marketing operations, stores and manages extensive customer, campaign, and analytic data. This data is essential for tracking performance and tailoring marketing initiatives, thereby emphasizing the critical importance of prioritizing the security of the database server.

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

When assessing risks, the organization's data storage and management procedures were taken into account. Potential threat sources and events were ascertained by evaluating the likelihood of a security incident, considering the information system's open access permissions. The severity of potential incidents was weighed against the impact on daily operational requirements.

Remediation Strategy

To enhance database security, implement the following measures:

- **Authentication, Authorization, and Auditing:** Enforce the use of strong passwords, role-based access controls, and multi-factor authentication to restrict user privileges and implement authentication, authorization, and auditing mechanisms. These will ensure that only authorized users can access the database server.
- **Data Encryption:** Utilize TLS encryption for data in motion (instead of SSL).
- **Network Security:** Implement IP allow-listing to restrict database access to corporate offices only and prevent access from unauthorized users.