Vulnerability Assessment Report

19 August 2024

System Description

The server utilizes a high-performance CPU with 128GB memory, running the latest Linux OS and MySQL database. Network configuration includes IPv4 addressing and SSL/TLS encryption for secure connections..

Scope

This evaluation focuses on system access controls over three months (June-August 2024), following NIST SP 800-30 Rev. 1 guidelines for risk analysis.

Purpose

The database server centralizes storage and management of customer, campaign, and analytical data for marketing operations, making security critical for 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

The assessment considered data management procedures and existing access permissions to determine likelihood of security incidents. Impact severity was evaluated against operational requirements..

Remediation Strategy

Implementation of robust authentication and authorization controls is essential, including strong passwords, role-based access, and multi-factor authentication. Additional measures include upgrading to TLS encryption and implementing IP allow-listing for corporate offices.