Tanya Gonzalez
Vulnerability Assessment Report
1st of September 2023

Vulnerability Assessment Report

System Description

The server hardware consists of a powerful CPU processor and 128GB of memory.It has a MySQL database management system and is powered by the most recent version of the Linux operating system. It communicates with other servers on the network and is set up with a reliable IPv4 network connection. SSL/TLS encrypted connections are among the security precautions.

Scope

This vulnerability assessment's scope is related to the system's present access controls. The evaluation will take place between June and August of 2023, a span of three months. The information system risk analysis is based on NIST SP 800-30 Rev. 1.

Purpose

Large volumes of data are managed and stored by a centralized computer system called the database server. In order to track results and tailor marketing campaigns, the server is utilized to store customer, campaign, and analytical data. Because the system is regularly used for marketing operations, security is essential.

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 business's data storage and management practices were taken into account while measuring risks. Based on the possibility of a security incident considering the information system's open access rights, potential threat sources and events were identified. The impact on regular operational requirements was considered in relation to the seriousness of prospective incidents.

Remediation Strategy

Setting in place auditing, authentication, and permission systems to guarantee that only people with permission can access the database server. To restrict user privileges, this involves utilizing multi-factor authentication, role-based access controls, and secure passwords. use TLS rather than SSL for data encryption while in transit. IP allow-listing to business offices blocks arbitrary internet users from gaining access to the database.