Vulnerability Assessment Report

1st January 20XX

System Description

A potent CPU processor and 128GB of RAM make up the server gear. It is powered by the most recent Linux operating system and has a MySQL database management system installed. It is set up to communicate with other servers on the network and has a reliable IPv4 network connection. SSL/TLS encrypted connections are one type of security measure.

Scope

This vulnerability assessment's scope is related to the system's present access controls. The evaluation will take place between June 20XX and August 20XX, 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	*Acquire confidential data through exfiltration*	*3*	*3*	*9*
Employee	*Interrupt actions that are vital to the mission*	*2*	*3*	*6*
Customer	*Modify or remove important data*	*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

To guarantee that only authorized users have access to the database server, processes for auditing, authentication, and authorization must be implemented. Limiting user privileges can be achieved by the use of multi-factor authentication, role-based access limits, and secure passwords. TLS encryption of data in transit as opposed to SSL encryption. To stop arbitrary internet users from connecting to the database, corporate offices can employ IP allow-listing.