Vulnerability Assessment Report

1st January 20XX

System Description

128GB of memory and a potent CPU processor make up the server hardware. It hosts the MySQL database management system and utilizes the most recent Linux operating system. It communicates with other servers on the network and is set up with a reliable network connection using IPv4 addresses. SSL/TLS encrypted connections are among the security precautions.

Scope

The system's current access controls are included in the scope of this vulnerability analysis. Between June 20XX and August 20XX, three months will be covered by the evaluation. The information system's risk analysis is based on NIST SP 800-30 Rev. 1.

Purpose

Large volumes of data are stored and managed by a centralized computer system called the database server. In order to track performance and tailor marketing initiatives, the server is utilized to store customer, campaign, and analytics data. The system must be secured because marketing efforts frequently use it.

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 methods for data management and storage were taken into account while calculating risks. The likelihood of a security incident given the open access rights of the information system was used to determine potential threat sources and occurrences. The severity of prospective incidents and their effect on ongoing operating requirements were compared.

Remediation Strategy

To ensure that only authorized users access the database server, authentication, authorization, and auditing methods must be put in place. To do this, employ multi-factor authentication, role-based access controls, and strong passwords to restrict user privileges. data in transit encryption using TLS rather than SSL. IP allow-listing to corporate premises helps stop unauthorized internet users from accessing the database.