Vulnerability Assessment Report

1st January 20XX

System Description

The server hardware consists of a powerful CPU processor and 128GB of memory. It runs on the latest version of Linux operating system and hosts a MySQL database management system. It is configured with a stable network connection using IPv4 addresses and interacts with other servers on the network. Security measures include SSL/TLS encrypted connections.

Scope

The scope of this vulnerability assessment relates to the current access controls of the system. The assessment will cover a period of three months, from June 20XX to August 20XX. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The database server is a centralized computer system that stores and manages large amounts of data. The server is used to store customer, campaign, and analytic data that can later be analyzed to track performance and personalize marketing efforts. It is critical to secure the system because of its regular use for marketing operations.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Conduct man-in-the-middle attacks*	*2*	*3*	*6*
Operating System	*Installation of malicious software to locate and acquire sensitive information*	*3*	*3*	*9*
Hacker	*Conduct DoS attack*	*3*	*3*	*9*

Approach

Risks were measured considering the data & management of the database server. Potential threat sources and events were established based on the likelihood of a security incident on an open access database server and the severity was assessed based on the impact of day-to-day operations.

Remediation

Consider the following questions to help you write a remediation strategy:
Implementing the AAA framework for anyone who is to access the database (employees only) to mitigate the risk of data theft. Introducing multi-level defenses, firewall for the network and VPN's for the remote employees. I would also suggest endpoint protection to secure data and systems.