Vulnerability Assessment Report

1st January 20XX

System Description

The server is equipped with a high-performance CPU and 128GB of memory. It operates on the latest Linux operating system and hosts a MySQL database management system. The server maintains a stable network connection using IPv4 addresses and interacts with other servers on the network. Security measures include SSL/TLS-encrypted connections to protect data in transit.

Scope

This vulnerability assessment focuses on evaluating the current access controls of the system. The assessment covers a three-month period, from June 20XX to August 20XX. Risk analysis was conducted following the NIST SP 800-30 Rev. 1 framework to ensure a structured and comprehensive evaluation of the information system.

Purpose

Consider the following questions to help you write:

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	*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 vulnerability assessment focused on analyzing the system's data storage and management practices. Potential threats and events were identified based on the likelihood of security incidents resulting from the current access permissions. The severity of each potential incident was assessed relative to its impact on day-to-day operations. This structured approach ensures that the assessment results are credible and can guide informed decision-making by stakeholders.

Consider the following questions to help you write an approach section:
Risks that were measured considered the data storage and management procedures of the business. Potential threat sources and events were determined using the likelihood of a security incident given the open access permissions of the information system. The severity of potential incidents was weighed against the impact on day-to-day operational needs.

Remediation Strategy

1. **Authentication, Authorization, and Auditing:**
    - Implement strong password policies and multi-factor authentication.
    - Use role-based access controls to restrict user privileges to only what is necessary.
    - Enable auditing and logging to monitor access and detect unauthorized activity.
2. **Encryption:**
    - Encrypt data in transit using TLS instead of SSL to strengthen data protection.
3. **Network Access Control:**
    - Implement IP allow-listing for corporate offices to prevent unauthorized external access.

By implementing these strategies, the organization can reduce the likelihood and impact of security incidents, ensuring the database server remains secure and operationally resilient.