Vulnerability Assessment Report

1st January 2024

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.

The database server is invaluable to the business as it hosts critical customer and potential leads information, essential for sales and marketing. Ensuring the security of this data is vital to maintain the company's reputation, trust, and compliance with regulations like NIST framework. If the server were to be compromised, it could lead to significant financial loss, legal penalties, and irreversible damage to the company's reputation.

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*
Competitor	*Conduct DoS attacks*	*2*	*3*	*6*
Malicious Software	*Conduct Ransomware attacks*	*2*	*2*	*4*
Customer	*Alter/Delete critical information*	*1*	*3*	*3*

Approach

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 were weighed against the impact on day-to-day operational needs.

The threat sources and events were chosen based on the current configuration of the server and its public accessibility. A competitor could target the business to gain a market edge, while hackers may seek to exploit data for monetary gain. Additionally, the risk of malicious software altering or deleting vital data is considered as the server's open nature invites various forms of malware.

Remediation Strategy

To mitigate the identified risks, the implementation of authentication, authorization, and auditing mechanisms to ensure that only authorized users access the database server. This includes using strong passwords, biometrics, role-based access controls (RBAC), and multi-factor authentication (MFA) to limit user privileges, leveraging the Authentication, Authorization, Accounting (AAA) framework. Encryption of data in motion using TLS instead of SSL. IP allow-listing to corporate offices to prevent random users from the internet from connecting to the database. Deploying defense-in-depth strategies would add layers of security to the system, reducing the risk of a successful attack. Implementing public key infrastructure (PKI) will also further secure sensitive data from exfiltration.