Vulnerability Assessment Report

18th July 2023

System Description

The server hardware is equipped with a high-performance CPU processor and 128GB of memory, enabling efficient processing capabilities. It operates on the latest version of the Linux operating system and serves as a host for the MySQL database management system. The server is configured with a reliable network connection using IPv4 addresses and maintains seamless communication with other servers within the network. To enhance security, the server implements SSL/TLS encrypted connections, ensuring the protection of data during transmission.

Scope

This vulnerability assessment focuses on evaluating the effectiveness of the current access controls implemented within the system. The assessment will encompass a duration of three months, specifically from June 2023 to August 2023, allowing for a comprehensive examination of the security posture during this timeframe. To guide the risk analysis of the information system, the assessment aligns with the guidelines provided by NIST SP 800-30 Rev. 1, ensuring a systematic and rigorous evaluation process.

Purpose

The database server serves as a centralized computer system responsible for storing and managing substantial volumes of data. It specifically holds customer, campaign, and analytic data, which are utilized for various purposes such as performance tracking and personalized marketing efforts. Given its integral role in supporting marketing operations, ensuring the security of this system becomes paramount. By safeguarding the database server, the company can protect sensitive data, maintain data integrity, and uphold the confidentiality and privacy of customer information.

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 assessment of risks took into account the data storage and management procedures employed by the business. To identify potential threat sources and events, the likelihood of security incidents was assessed, taking into consideration the open access permissions granted to the information system. Furthermore, the severity of potential incidents was carefully evaluated in relation to the impact they may have on day-to-day operational requirements. This approach enables a comprehensive understanding of the risks faced by the organization, allowing for targeted mitigation measures and informed decision-making to enhance overall cybersecurity posture.

Remediation Strategy

To address the vulnerabilities and enhance the security of the database server, the following remediation measures are recommended:

Implementation of robust authentication, authorization, and auditing mechanisms to enforce strict access controls. This includes the utilization of strong passwords, role-based access controls (RBAC), and multi-factor authentication (MFA) to limit user privileges and ensure that only authorized individuals can access the database server.

Adoption of Transport Layer Security (TLS) encryption for data in motion instead of Secure Sockets Layer (SSL). This stronger encryption protocol enhances the confidentiality and integrity of data during transmission, safeguarding it from unauthorized interception or tampering.

Implementing IP allow-listing to restrict access to the database server from specific corporate office IP addresses. By allowing only trusted sources to connect to the server, the risk of unauthorized access from random internet users is mitigated.

These remediation strategies collectively strengthen the security posture of the database server, fortifying it against potential threats and reducing the risk of unauthorized access or data breaches.