Vulnerability Assessment Report

3rd November 2023

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 functions as a central computer system responsible for storing and overseeing extensive volumes of data. This server is employed to house customer information, campaign details, and analytical data, facilitating subsequent analysis for performance tracking and personalized marketing initiatives. Ensuring the security of this system is imperative due to its consistent utilization in various marketing operations.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker (Outside)	*Exploiting the open database to gain unauthorized access.*	*3*	*3*	*9*
Employee (Insider)	*Deliberate disruption of mission-critical operations.*	*2*	*3*	*6*
Competitor	*Utilizing technical capabilities for a Denial-of-service attack.*	*2*	*3*	*6*

Approach

The selected threat sources and events in the vulnerability assessment were carefully chosen to address potential risks to the e-commerce platform. The unauthorized access threat from an external hacker reflects the risk associated with the public accessibility of the database, emphasizing the need for robust security measures to protect sensitive information. The insider threat from an employee acknowledges the internal risk of deliberate disruptions, underscoring the importance of internal security protocols. Furthermore, the consideration of a competitor leveraging technical capabilities for a denial-of-service attack recognizes the external risk to business continuity, necessitating proactive measures to safeguard against potential disruptions. This approach aims to provide a holistic evaluation of internal and external vulnerabilities critical for maintaining the integrity and functionality of the e-commerce platform.

Remediation Strategy

Addressing the identified risks involves implementing targeted security controls tailored to the nature of each threat. For the unauthorized access threat from external hackers, enforcing the principle of least privilege ensures that access rights are strictly limited, minimizing the potential impact of a successful breach. Adopting a defense-in-depth strategy adds layers of protection against the insider threat, safeguarding critical operations even in the event of internal security lapses. For both external and insider threats, instituting multi-factor authentication (MFA) enhances access security. Additionally, employing a robust Authentication, Authorization, Accounting (AAA) framework establishes comprehensive control over user access, mitigating the risk of deliberate disruptions. These strategic security measures collectively contribute to a resilient defense against the identified threats.