Vulnerability Assessment Report

17th January 2025

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 acts as the main system for managing and storing large amounts of data. It holds critical information such as customer records, campaign specifics, and analytics, enabling analysis for tracking performance and tailoring marketing efforts. Given its central role in finding potential customers, maintaining the security of this server is crucial, in order to stop business disruption.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Complete a Distributed Denial of Service attack (DDoS)*	*1*	*3*	*3*
Hacker	*Target the open database to gain unauthorised access to the data, which they could either sell on to a competitor or complete a ransomware attack*	*3*	*3*	*9*
Employee	*Deliberate or accidental deletion of the database or contents*	*2*	*3*	*6*

Approach

The identified threat sources and events in the vulnerability assessment were specifically selected to target potential risks to the e-commerce platform. Although the likelihood of a competitor using a Distributed Denial of Service (DDoS) attack is relatively low due to ethical considerations, it has occurred in other industries where competition is intense. A DDoS attack could severely disrupt business operations and impact continuity. The risk of unauthorized access by a hacker underscores the dangers of having a publicly accessible database, stressing the importance of strong security measures to safeguard sensitive data. Additionally, the potential threat of an employee accidentally or intentionally deleting data highlights the necessity of having reliable system backups in place to prevent data loss. This approach ensures a comprehensive evaluation of both internal and external vulnerabilities, which is vital for maintaining the integrity and smooth functioning of the e-commerce platform.

Remediation Strategy

Mitigating the identified risks requires the implementation of specific security measures designed to address the unique characteristics of each threat. To safeguard against DDoS attacks or similar threats, it's crucial to continuously monitor network traffic to detect abnormal patterns early, allowing for a swift response. Intrusion Detection Systems (IDS) play a key role in this, as they can also identify suspicious behavior from employees or authorized users, such as accessing sensitive data they don't typically use or performing unauthorized actions. This helps mitigate the risk of insider threats. Additionally, implementing a backup system ensures protection against the accidental or intentional deletion of data by an employee. Backups are also invaluable in the event of a cyberattack or system failure, helping maintain business continuity. Enforcing Multi-Factor Authentication (MFA) further strengthens security by preventing unauthorized access, whether from hackers, disgruntled former employees, or competitors. Together, these strategic measures provide a comprehensive defense against the identified risks.