Vulnerability Assessment Report

1st June 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 January 2024 to March 2024. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The server is used by the employees to find data related to potential customers and is valuable since many employees work remotely from all over the world. It is crucial that the business secure the data on the server as otherwise, Personally Identifiable Information (PII) or even Sensitive PII (SPII) could be leaked, lost, or altered. Additionally, this could include payment card information, which falls under PCI DSS; therefore, the business must comply with these regulations. If the server were to be compromised in any way, the e-commerce business might have to halt operations until the server is restored, which would have a significant financial impact.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*
Hacker	*Conduct Denial of Service (DoS) attacks*	*3*	*1*	*3*
Malicious Software	*Alter/Delete critical information*	*2*	*3*	*6*

Approach

Risks considered the data storage and management methods of the business. The likelihood of a threat occurrence and the impact of these potential events were weighed against the risks to day-to-day operational needs.

The threat sources listed are the most likely to initiate threat events against the public server since no access controls are currently in place. An everyday hacker can easily conduct a DoS attack, affecting business operations for a short period of time, while a competitor could gain access to sensitive information. The loss of sensitive information is much more severe and could result in regulatory consequences, so if any threat source were to install malicious software on the server, it could result in similar events. The alteration or deletion of critical information would be equally severe and cause time, financial, and reputation losses.

Remediation Strategy

Implementation of authentication, authorization, and auditing mechanisms to ensure that only authorized users access the database server. This includes using strong passwords, role-based access controls, and multi-factor authentication to limit user privileges. 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.

Additionally, implement a public key infrastructure (PKI) to prevent exfiltration of sensitive information. Having proper configuration and management of a firewall and its rules to mitigate DoS attacks. IDS/IPS installation to detect and prevent malicious signatures from reaching the server and deploying malicious software.