Vulnerability Assessment Report

1st January 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 2023 to August 2023. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The database contains all the essential information to the business including company's critical data, customer's PII and transactions. For this reason it's one of most valuable assets and need to be secure from any threat because a shutdown of the server or a critical attack will affect all the business continuity and can provoke financial damages, customer's distrust and important data leaks.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*
Employee	*Is tricked by email to click on link and provide credentials*	*2*	*3*	*6*
Hacker	*Execute a DoS attack*	*1*	*3*	*3*
Communications	*Communications provider shut*	*1*	*3*	*3*

	down on the server location			
Malicious Software	*Malicious software introduced in the network*	*1*	*3*	*3*

Approach

As an E-Commerce company with all the employees working remotely the threats are limited to server accesses or to the server's local events. I considered the attempt to steal credentials from an employee, a DoS attack and malicious software delivery as the main problems to handle in this case because it is the only way to voluntarily affect the company. About involuntarily events, the company works with a remote server so with all the employees needing to be constantly connected to that, the main threat can be a problem with communications or with the communication's provider.

Remediation Strategy

Implementation of authentication mechanisms to ensure that only authorized users access the database server like MFA. IP allow-listing to corporate offices to prevent random users from the internet from connecting to the database. Implementation of Defense in Depth to avoid DoS attacks or malicious software. To prevent issues with communications, discuss with the provider to find an alternative in case of failure.