Vulnerability Assessment Report

19th August 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 is a key component of the business operations as it contains all the data related to the business. E.g. Consumer information, confidential files, etc.*
- *It is crucial to keep data on the server protected if in any case there were any threats to the server all key information could be leaked and it could lead to a bad reputation for the business and financial costs to the business.*
- *Due to the nature of the business, which is an e-commerce business, this means the majority of our operations are carried out online. This means the majority of the business runs on servers, to store information and run online operations.*

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hackers	*Procuring confidential information*	*2*	*3*	*6*
Competitors	*Gaining important information about new products or company secrets*	*2*	*2*	*4*
Employee	*Disrupt internal operations*	*1*	*3*	*3*

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.

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.