Vulnerability Assessment Report

24st September 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

Consider the following questions to help you write:

- *How is the database server valuable to the business?*
  Customer information and details (PII) are hosted on this server. Customers are the fuel for the business.

- *Why is it important for the business to secure the data on the server?*
  People established trust in the company to protect their data therefore it is a big plus for the company as for credibility and to protect these assets. Furthermore it should also reflect the minimum industry requirements.

- *How might the server impact the business if it were disabled?*
  Business interruption would cause financial damage, the image of the company would drop in the eyes of the customers and reduce credibility in the eyes of the employees as well.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
E.g. Competitor	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*
Internal Threat	*Obtain/Change/Delete sensitive information via exfiltration*	*2*	*2*	*4*
External Threat's	*Conduct Denial of Service (DoS) attacks.*	*3*	*3*	*9*

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.

Competitor
Since the Database is open the competitors this can allow access through Malware to these sensitive PII files. Threat source installs malicious software on organizational systems to locate and acquire sensitive information.
Threat level Medium

Internal Threat
Due to the open source system employees could easily access, change or delete data. Threats arising from individuals or groups who might purposefully or accidentally exploit cyber resources. For example, they might alter data in a way that negatively impacts the company. Alternatively, they might intentionally steal data and damage business equipment.

External Threats
Threat source sends automated, excessive requests to overwhelm the system's operating capabilities. Threat source compromises the integrity of information in such a way that prevents the business from carrying out critical operations.

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.