Vulnerability Assessment Report

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

Purpose

This database holds significant value, both for the internal operations of the company and for a potential attacker, as it contains the list of potential clients. The risk of the database being stolen or deleted could lead to a total shutdown of the company, resulting in substantial losses and even possible bankruptcy.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
E.g. Competitor	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*
Hacker	*Alter/Delete critical information*	*2*	*3*	*3*
Hacker	*Install persistent and targeted network sniffers On organizational information systems.*	*1*		
Hacker	*Conduct Denial of Service (DoS) attacks.*	*2*	*3*	*3*

Hacker	*Disrupt mission-critical operations.*	*1*	*2*	*3*
Hacker	*Conduct "man-in-the-middle" attacks.*	*1*	*2*	*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.