Vulnerability Assessment Report

13th July 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 July 2024 to September 2024. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The remote database is key for the business since many employees work remotely from all around the world. The employees use the database to query information from the customers, but since it is a public database this represents a major security issue for the company. If an attack occurs to the public open database it could cause the server to shutdown impeding employees to find new customers until the problem is solved.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*
Malicious software	*Injection of malware*	*3*	*3*	*9*
Temperature controls	*Failure in temperature controls leading to hardware damages*	*1*	*3*	*3*

Approach

The threats were chosen based on the potential impact that could have in the open public database case. In the competitor exfiltration case it can cause competitive disadvantage and losses in business. Malicious software compromises the data integrity and leads to reputational damage. A temperature control issue is likely to happen but can result in complete data loss and also hardware damage.

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.