Vulnerability Assessment Report

19th February 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 20XX to August 20XX. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

This vulnerability assessment aims to evaluate the security of the company's database server. The server stores and manages various important business-critical data and is an essential component of the company's daily operations. Therefore, securing the system is of paramount importance. Any compromise or disruption to the server could disrupt operations and lead to data breaches, reputational damage, and potential legal repercussions.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Employee	*Disrupt mission-critical operations*	*2*	*3*	*6*
Customer	*Alter/Delete critical information*	*1*	*3*	*3*

Approach

My approach was to assess and measure the risks based on the company's data storage and management processes. Since the information system had open access permissions, I identified potential threat sources and events by considering how likely a security incident could happen. Then, I evaluated the severity of potential incidents against their impact on the company’s daily operations.

Remediation Strategy

There are several measures that the company can put in place to make for an effective remediation strategy. Firstly, the implementation of authentication, authorization, and auditing mechanisms to ensure that only authorized users access the database server. These include the use of strong passwords, role-based access controls, and multi-factor authentication to limit user privileges. The company can also consider encrypting its data in motion using TLS instead of SSL. Last but not least, only white-list corporate offices’ IP to prevent random users from the internet from connecting to the database.