Vulnerability Assessment Report

1st January 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 2023 to August 2023. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

An organization's database is a very valuable resource of the organization. It stores relevant information for the company to achieve its objectives in a complete and timely manner. Being such a valuable resource, its security must be of the highest priority, since if the information contained therein were to be leaked to the public, the commercial and reputational damage could be irreparable.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Disrupt mission-critical operations*	*3*	*3*	*9*
System administrator	*Alter/delete critical information*	*2*	*3*	*6*
Hacker	*Perform reconnaissance and surveillance of organization*	*3*	*3*	*9*

Approach

An organizational database should not be publicly accessible. This is a major vulnerability. The risk exists that the information contained in that database (which is indispensable for the operation) could be altered, distributed, or destroyed. In addition, as appropriate access controls are lacking, the likelihood of threats becoming real impacts on the organization increases. Competitors, hackers, employees or customers could gain access and misuse the information. Such a valuable asset cannot be left unprotected.

Remediation Strategy

I suggest a solution with a hierarchical flow. That is, management should establish policies that reflect a much more robust security posture than the current one. Restricting access to the database to only those who need it and only when they need it is a good first step. At the operational level, it is recommended that employees be trained as much as possible to foster a culture of respect for the privacy and integrity of other people's information. At the technical level, it is suggested to encrypt communications between the server containing the database and the users requesting information from it. If a multifactor authentication policy is also implemented, an additional layer of security is added.