Vulnerability Assessment Report

26st October 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 July 2023 to October 2023. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The objective of this assessment is to verify the confidentiality, integrity, and availability of database assets relating to the server in question by investigating access controls of the information systems managing this database. It contains all information related to the company since it was created three years ago, meaning it has significant data that should be restricted, but the database is public. If the data was destroyed or stolen, the company could be in violation of many regulations and would lose valuable information about employees and customers.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker	*Obtain or destroy sensitive information via infiltration database management system.*	*3*	*3*	*9*
Employee	*Misuse or abuse permissions to make changes to the database management system and its data.*	*2*	*3*	*6*
Malicious	*Injected code to the linux*	*1*	*3*	*3*

Software	*management system of the database via network vulnerabilities.*			

Approach

The approach to this vulnerability assessment is from a perspective of likelihood. The three threat sources are the most likely sources given the organization's structure and its current vulnerabilities. The first is a hacker which is entirely possible given the fact that the database is public. Anyone who could exploit the linux management system would have full control over the database. The second is an employee due to the fact that they already have access to the full system. The principle of least privilege and separation of duties is not being implemented meaning any employee can do anything to the database, whether it be intentional or accidental. The third threat source would be malicious software, because the server is being accessed so much remotely and is not private there is a good chance that a network vulnerability with accompanying software would gain full unauthorized access to the system.

Remediation Strategy

What is needed is the use of tools to authenticate users that need access, and no one else. Also within the user pool there should be regular audits determining whether or not this user needs access to the database ensuring least privilege. A login system using multi factor authentication with different tiers of access and control would address these issues. Another actionable strategy is to implement a firewall filter for certain IP’s protecting the database’s network from the public.