Vulnerability Assessment Report

21st March 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. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

Conducting a vulnerability analysis is helpful to identify the attack surfaces of the business. Since employees of the company regularly query data from the database server to find potential customers, the database server is very valuable to the business since it contains potential customers' information. It's important for the business to secure the data on the server so competitors or malicious actors won't steal the information for other uses. If the server is disabled, the business will not have access to customers' information. Also, if a data breach happens, the business may face reputation damage and even lawsuit.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Customer	*Change critical information*	*2*	*3*	*6*
Malicious software	*Hackers may use malicious software to steal customers' PII for sale on the dark web or for identity theft.*	*3*	*3*	*9*
Power outage	*Power outage may lead to inaccessibility of information, which affects business's normal operation.*	*1*	*3*	*3*

Approach

I identified the following threat sources: employees, malicious software, and power outages. Customers may change critical information either accidentally or intentionally, since the database is open to the public. Such actions can compromise the business's database. The likelihood of this occurring is 2, and the severity is 3. Malicious software could be used to steal customers' information for sale or identity theft, damaging the business's reputation. The likelihood and severity of this threat are both 3. A power outage would disrupt the normal operations of the business. While this is not very likely to happen, if it does occur, the business will be unable to operate. Consequently, the likelihood is 1, and the severity is 3.
This assessment is limited as we have not yet conducted a vulnerability assessment, meaning we are unaware of the business's attack surfaces. Therefore, the risk assessment may not be accurate. We need to identify which assets require more protection to better assess the risks.

Remediation Strategy

Technical controls such as SSL/TLS encrypted connections are implemented to secure data during transfer. Security controls such as access control and MFA (multi-factor authentication) add an additional layer of security to the system. Since MFA requires at least two methods to verify a user's identity, it protects information from being accessed by malicious actors who may have obtained employees' login information. Implementing the principle of least privilege also protects information. Access to the database should be granted based on a "need to know" basis, and employees' access should be determined by their roles. This ensures that employees' access is based on RBAC (role-based access control). Even if the system is breached, the limited access on users' accounts will buy the organization some time to stop the attacker.