Vulnerability Assessment Report

20th February 2024

System Description

The server hardware consists of a powerful CPU processor and 128GB of memory. It runs on the latest version of the 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 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:

- The database server is very valuable to the business because it is widely used by most of the employers of the companies since they all work from remote locations all over the world.
- The data on the server is very important because the remote employees get information about the customer from the database. Any disruption to that data will cause huge damage to the business. Hence, the data on the server is important to keep secure from malicious threat actors.
- If the server is disabled, the employees of the company won't get access to the information about the customer which eventually causes the business a huge loss.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	Obtain sensitive information via exfiltration	1	3	3
Hardware and Software	Failure of equipment due to aging, resource depletion.	1	3	2

Operational environments, and natural hazards	Accidental, non-human factors might cause damage to the database server.	1	2	2

Approach

The first threat source “Competitor” is selected because the possible threat event will occur to obtain sensitive information via exfiltration. This threat source has less likelihood to happen, but it has high risk and severity if it is exploited. The second threat source “Hardware and Software” is selected because the possible threat event will cause the failure of equipment due to aging, and resource depletion. This threat source has less likelihood but it has high severity and moderate risk if exploited. It is said that it has a moderate risk because no database server is kept out-of-date. After all, it is continuously monitored and updated. The third threat source is the operational environment and natural hazards because they could cause possible threat events like accidental non-human factors that might cause damage to the database server. This threat source is considered as having less likelihood to happen because the natural calamities are not frequently happening and the database server will be kept in a place where the likelihood to happen is less. Yet, we need to prepare if it happens, hence they’re considered as moderate severity and risk.

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.