Vulnerability Assessment Report

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

Purpose

Consider the following questions to help you write:

- *How is the database server valuable to the business?*
- *Why is it important for the business to secure the data on the server?*
- *How might the server impact the business if it were disabled?*

The database server stores all customer information and confidential data that the company uses to track employee accounts and access specific levels of information. The business needs to maintain the security of the database because data stored in the database may be sensitive, causing the business to lose access to accounts, including the server itself, and competitors can access data that may cause plagiarism or conflict in the future. If the server were disabled, the company would lose access to all customer information and employee accounts. This will lead the company to lose the trust of all customers and employees. Customer requests will not be fulfilled. Employees would not be able to complete any task required to fulfill customer requests.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
E.g. Competitor	*Obtain sensitive information via*	*3*	*3*	*9*

	exfiltration			
Customer	Obtain sensitive information via exfiltration	1	2	3
Hacker	Alter/delete critical information	3	3	9
Malicious software	Perform reconnaissance and surveillance of the organization	3	3	9

Approach

This section documents the approach used to conduct the vulnerability assessment report. It is important to be clear and concise when writing your approach. A transparent summary of your approach helps stakeholders understand that the assessment is credible and that the results can be used to make informed decisions.

Consider the following questions to help you write an approach section:

- *What was your rationale for selecting the risks that you evaluated?*
- *How were you deriving the likelihood and severity scores of each risk?*
- *What were the limitations of the assessment?*

One of the most apparent threats is the customers because they are familiar with the company and the products they carry. Therefore, with an open database server, the customer has access to all product information, including employee information, which they can take advantage of if they, for example, want early access to products. Hackers are an obvious threat because an insecure database provides hackers who are unsupportive of the company/business the opportunity to sabotage with little work required. Lastly, malicious software can be placed on the server at any time by attackers to monitor and watch the business's every move.

Remediation Strategy

This section provides specific and actionable recommendations to remediate or mitigate the risks that were assessed. Any recommendations that you make should be realistic and achievable. Overall, the remediation section of a vulnerability assessment report helps to ensure that risks are addressed in a timely and effective manner.

Consider the following questions to help you write a remediation strategy:

- *Which technical, operational, or managerial controls are currently implemented to secure the system?*
- *Are there security controls that can reduce the risks you evaluated? What are those controls, and how would they remediate the risks?*

- *How will the results of the assessment improve the overall security of the system?*