Vulnerability Assessment Report

27th December 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 June 20XX to August 20XX. 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 is valuable to this e-commerce company because it contains potential customer data that is used to generate business and revenue. Data on the database server must be secure because 1) it contains personal information of potential customers and 2) if the data is lost or stolen then it could affect business and profit generated by the company due to a loss of potential customers. From the scenario explained, if the server were to be disabled it would severely impact the company because they would lose the source that they use for their potential customers.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Exfiltrate potential customer information*	*3*	*3*	*9*
Hacker	*Infiltrate and steal personal information of potential customers*	*3*	*3*	*9*
Employee	*Disgruntled employee steals information after being terminated or reprimanded*	*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?*

The threat sources that I chose to evaluate were all human. The reason for choosing these human threat sources is because the database server is open to the public and can therefore be accessed easily by nearly anybody. The likelihood of any of these threat sources is at a 3 (three), again, because the database is open to the public so it is highly likely to be accessed. Since there was only a brief scenario description and predetermined information, the vulnerability assessment is only surface level and not very in-depth.

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?*

Currently, there are no technical, operational, or managerial controls in place to secure the system and that leaves the system exposed to many threats. First and foremost, the database server should not be open to the public and should require some form of authentication, preferably Multi-factor authentication (MFA), to be accessed. Secondly, the principle of least privilege should be used to ensure that potential customer information is only being accessed by employees who need it and only for the amount of time that is absolutely necessary. After the employee is done with the customer information they should lose access immediately. Implementing just these two security measures will **vastly** improve the security of the database server and the customer information within.