**Scenario**

**Review the following scenario. Then complete the step-by-step instructions.**

**You are a newly hired cybersecurity analyst for an e-commerce company. The company stores information on a remote database server, since many of the employees work remotely from locations all around the world. Employees of the company regularly query, or request, data from the server to find potential customers. The database has been open to the public since the company's launch three years ago. As a cybersecurity professional, you recognize that keeping the database server open to the public is a serious vulnerability.**

**You are tasked with completing a vulnerability assessment of the situation to communicate the potential risks to decision makers at the company. You must create a written report that explains how the vulnerable server is a risk to business operations and how it can be secured.**

**Vulnerability Assessment Report**

**1st January 20XX**

**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](https://docs.google.com/document/d/1Fc4L2azQlnUM-8r43PU9mYlT30BnxTwdjAMqpT7JeZk/edit?resourcekey=0-Q-XglnC3Li7JPK2hIvMkVg#heading=h.hvbcmqwzo9do) 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?*

*1. The employees of the company uses data from the server to find potential customers*

* *Why is it important for the business to secure the data on the server?*
* *1. It is important because employees who work remotely can easily access the remote database server*
* *How might the server impact the business if it were disabled?*

*1. The company might no longer have access to the data needed to find potential customers*

**Risk Assessment**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| *E.g. Competitor* | *Obtain sensitive information via exfiltration* | *3* | *3* | *9* |
| Customers | Alter/ Delete critical information | 2 | 3 | 6 |
| Hacker | Install persisent and targeted network sniffers on organisational information systems | 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? The risks were measured on the fact that the server has been opened to the public for a long time which gives the gives the threat sources access that could potentially harm the business*
* *How were you deriving the likelihood and severity scores of each risk? I accessed the scores based on the access permissions of the information system*
* *What were the limitations of the assessment? There weren't any limitations*

**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? Implementations of controls such as encryption of data in transit using TLS, Multifactor authentication systems, and also use of stronger passwords*
* *Are there security controls that can reduce the risks you evaluated? What are those controls and how would they remediate the risks? The controls mentioned above will limit users to access only information they need*
* *How will the results of the assessment improve the overall security of the system? The assessment will help the business to take realistic decisions that will ensure the safety of their assets in the future*