Analyze a vulnerable system for a small business

Scenario

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.

A vulnerability assessment of the situation can help you communicate the potential risks with decision-makers at the company. You must create a written report that clearly explains how the vulnerable server is a risk to business operations and how it can be secured.

System Description

The company stores information on a remote database server. The server is accessible to the public, which means that anyone could potentially access the data. The data includes customer names, addresses, and credit card numbers.

Scope

This vulnerability assessment focuses on the confidentiality, availability, and integrity of the data on the server. The assessment does not include the physical security of the server or its related IT systems and 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

The purpose of this vulnerability assessment is to identify and assess the risks associated with public access to the database server. The assessment will also recommend security controls that can be implemented to mitigate these risks.

Risk Assessment

The following table summarizes the risks identified in this assessment:

Threat Source	Threat Event	Likelihood	Severity	Risk
Malicious insiders	Gain unauthorized access to the server and exfiltrate the data.	3	3	9
Cybercriminals	Launch a denial-of-service attack against the server, making it unavailable to legitimate users.	2	3	6
Phishing attacks	trick employees into clicking on malicious links, which could lead to the compromise of their credentials and the server.	1	3	3

The overall risk of the public access to the database server is high. The risks of unauthorized access, denial-of-service attacks, and phishing attacks are all significant.

Approach

The following security controls can be implemented to mitigate the risks identified in this assessment:

- Implement a firewall to restrict access to the server to authorized users only.
- Implement strong authentication and authorization mechanisms to prevent unauthorized access to the server.
- Encrypt the data on the server to protect it from unauthorized access.
- Implement a web application firewall to protect the server from denial-of-service attacks.
- Train employees on phishing attacks and how to avoid them.

Remediation Strategy

The following security controls should be implemented as soon as possible to mitigate the risks identified in this assessment:

- Implement a firewall to restrict access to the server to authorized users only.
- Implement strong authentication and authorization mechanisms to prevent unauthorized access to the server.
- Encrypt the data on the server to protect it from unauthorized access.

The other security controls can be implemented on a phased basis, depending on the resources available.

Conclusion

Public access to the database server poses a significant risk to the confidentiality, availability, and integrity of the data. The security controls outlined in this report can be implemented to mitigate these risks.