Scenario :: Vulnerability Assessment for a small business

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.

Report

Technical Composition -

System - Powerful Server with CPU processors of 128GB memory.

OS - Latest Version of Linux(Open Source)

OS last patch update : **J**anuary 17th 2023(01/17/2023)

Database - MySQL(Open Source)

Database Version - 18.1.9

Network Connection - IPv4 Type

Network Encryption Type - SSL/TLS

Scope -

The purpose of this report is to submit to the small business the vulnerability it currently faces for the access control for the system(database server).

The assessment will be covered for 6 weeks from the starting of july 2023 to 2nd week of August 2023. The risk assessment will be conducted as per the guidelines of NIST-SP 800-30 Rev.1 **

Purpose -

The database server is a centralized computer system that stores and manages large amounts of data. The server is used to store customer, campaign, and analytic data that can later be analyzed to track performance and personalize marketing efforts. It is critical to secure the system because of its regular use for marketing operations.

Risk Assessment -

Threat Source: The attack surface which can be exploited by a malicious actor.

Risk(s): A potential risk to the organization's information systems and data.

Threat Event: A vulnerability which is to be explioted that might lead to a security incident.

Likelihood: Score from 1-3 of the chances of a vulnerability being exploited. A 1 means there's a low likelihood, a 2 means there's a moderate likelihood, and a 3 means there's a high likelihood.

Severity: Score from 1-3 of the potential damage the threat would cause to the business. A 1 means a low severity impact, a 2 is a moderate severity impact, and a 3 is a high severity impact.

Risk: How quickly a risk should be addressed to avoid the potential incident. Use the following formula to calculate the overall score: **Likelihood x Impact Severity = Risk**

Threat source	**Threat event**	**Likelihood**	**Severity**	**Risk**
Hacker	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Employee	*Disrupt mission-critical operations*	*2*	*3*	*6*
Customer	*Alter/Delete critical information*	*1*	*3*	*3*

Approach -

Risks that were measured considered the data storage and management procedures of the business. Potential threat sources and events were determined using the likelihood of a security incident given the open access permissions of the information system. The severity of potential incidents were weighed against the impact on day-to-day operational needs.

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.