Justin Goncalves

8/14/24

Vulnerability Assessment Report

Activity Overview:

In this activity, you will conduct a vulnerability assessment for a small business. A vulnerability assessment is the internal review process of an organization's security systems. You will evaluate the risks of a vulnerable information system and outline a remediation plan.

Scenario

Review the scenario below. 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.

Nist SP 800-30 Rev. 1:
https://docs.google.com/document/d/1BZT1Jb_uusqt6SZFI_4QbDKPYeRDZVfgp7RcUM-1ubY/edit?resourcekey=0-eOFLaW_cH0iUGXZSmV9ULw#heading=h.hvbcmqwzo9do

Follow the instructions to complete each step of the activity.

Vulnerability Assessment Report

14th August 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. 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

The purpose of this vulnerability assessment is to evaluate the security risks associated with the publicly accessible database server used by the e-commerce company. The database server is critical to the business as it stores sensitive customer and company data, which is regularly accessed by employees worldwide. Securing this server is essential to protect the company from data breaches, ensure the continuity of business operations, and maintain customer trust. If the server were compromised, it could result in severe financial and reputational damage to the company.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
External Attackers	*Data Breach: External attackers gain unauthorized access to sensitive customer and company data stored on the server.*	*3*	*3*	*9*
Inside Threats	*Data Exfiltration: An insider downloads and shares confidential data without authorization, either intentionally or due to carelessness.*	*2*	*3*	*6*
Business Competitors	*Denial of Service (DoS) Attack: A competitor launches a DoS attack to overwhelm the server, causing a disruption in the company's operations.*	*2*	*2*	*4*

Approach

The three specific threat sources and events were selected based on their relevance to the e-commerce company's operations and the potential impact they could have on the business. A data breach is a significant risk due to the sensitive information stored on the server, making it a prime target for external attackers. Data exfiltration by insiders is a concern because employees have access to valuable data that could be leaked intentionally or accidentally. Lastly, a denial of service attack by competitors could severely disrupt the company's operations, leading to financial losses and damage to its reputation.

Remediation Strategy

To remediate and mitigate the identified risks, the following security controls should be implemented:

1. **Principle of Least Privilege** - Restrict access to the database server to only those employees who absolutely need it for their work. This will minimize the risk of data exfiltration and reduce the attack surface for external threats.
2. **Multi-factor Authentication (MFA)** - Implement MFA for all users accessing the server to ensure that even if credentials are compromised, unauthorized access is prevented.
3. **Defense in Depth** - Apply multiple layers of security controls, including firewalls, intrusion detection systems, and regular security audits, to protect against both external and internal threats.

These measures will strengthen the security of the company's database server and reduce the likelihood and impact of potential security incidents.