Analyze a vulnerable system for a small business

In this activity, I conducted a vulnerability assessment for a small business. I evaluated the risks of a vulnerable information system and outlined a remediation plan. A vulnerability assessment is the internal review process of an organization’s security systems.

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.

Task

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

Vulnerability Assessment Report

29th 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 2024 to August 2024. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

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	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 were assessed by looking at how the business stores and manages data. Threats and events were identified based on the likelihood of a security incident due to open access in the system. The seriousness of these incidents was then compared to how they would affect daily operations.

Remediation Strategy

1. Implement authentication, authorization, and auditing mechanisms for secure database access.
2. Use strong passwords and role-based access controls (RBAC) to limit user privileges.
3. Enforce multi-factor authentication (MFA) for additional security.
4. Encrypt data in transit using TLS (Transport Layer Security) instead of SSL.
5. Set up IP allow-listing to restrict database access to authorized corporate offices only.