Vulnerability Assessment Report

Analyzing a Vulnerable System for a Small Business

Wendy Alayon
07/07/2024 **@syszern**

Vulnerability assessment report

Scenario

As a newly hired cybersecurity analyst for an e-commerce company, the company stores information on a remote database server due to remote working arrangements for its global employees. The server regularly serves data queries from employees seeking potential customers. Since its launch three years ago, the database has been accessible to the public. Recognizing the seriousness of this issue, securing the database server is crucial.

The task involves conducting a vulnerability assessment to outline the risks posed by the open server. A written report must detail how this vulnerability jeopardizes business operations and propose measures for securing the server.

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 database server functions as a centralized system responsible for storing and managing extensive datasets, including customer information, campaign details, and analytics. These data are crucial for tracking performance and personalizing marketing efforts. Securing this system is imperative due to its regular use in supporting essential 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

The risks assessed took into account how data is stored and managed within the business. Identification of potential threat sources and events relied on assessing the probability of security incidents due to the open access permissions of the information system. Additionally, the severity of potential incidents was evaluated in relation to their impact on daily operational requirements.

Remediation Strategy

The measures implemented include authentication, authorization, and auditing mechanisms to restrict access to the database server to authorized users only. This involves employing robust password policies, role-based access controls, and multi-factor authentication to restrict user privileges. Data transmission is secured using TLS encryption instead of SSL to protect data in transit. Additionally, IP allow-listing is configured to permit access only from corporate offices, thereby preventing unauthorized users from connecting to the database server over the internet.