Vulnerability Assessment Report

1st January 2024

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 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 company's remote database server is a centralized system that stores and manages a large amount of data. It handles customer, marketing campaigns, and analytic data, with the goal of allowing the e-commerce company to analyze it later in order to personalize its marketing. This server is exposed to the public, which represents a significant vulnerability, as this system is critical to the company's operations.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Employee	*Disrupt mission-critical operations*	*2*	*3*	*6*
Former employee	*Obtain and leak sensitive information to the public, or sell it to competitors*	*2*	*3*	*6*
Customer	*Alter/Delete critical information*	*1*	*2*	*2*
Hacker	*Obtain and leak sensitive information via exfiltration*	*3*	*3*	*9*

Approach

The measured risks considered the data storage and management methods of the business. Each potential threat event was determined by the likelihood of a threat occurrence with an open access information server. The severity of each potential threat event was weighed against the risks to day-to-day operational needs. In the first place, some hackers could access the sensitive information and publish it to decrease the company's reputation or sell the information. Regarding the current employees, due to human error, they could alter important information or even delete it. The former employees could steal that information and sell it to another company. FInally, due to open access to all data, a customer could alter that information involuntarily.

Remediation Strategy

- Implementation of authentication, authorization, and auditing mechanisms to ensure that only authorized users access the database server.
- A good method to implement this is by installing IAM (Identity and access management) technology, which includes:
    - pre-shared keys,
    - 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.