Vulnerability Assessment

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.

Report

Date : November 14th 2023 - January 14th 2024 (3 Months. You may put an actual date for this).

System Desrcription

The database server runs on Debian Linux with 1TB of memory and powerful CPU processor. It hosts a MySQL database management system. The network connection uses IPV4 address, yet the security measure uses SSL instead of TLS.

Scope

The scope of this report covers the current access controls of the system. It was conducted from November 14th 2023 to January 14th 2024. The risk analysis of the information system is based on NIST SP 800-30. Alternatively, please have a look on other versions published by NIST.

Purpose

The database server stores large amounts of data. The data could be customer, campaign, analytic, that can track performance and personalize marketing efforts. Due to its nature, the system has to be secured from unauthorized personnels.

Risk Assessment

Threat source	**Threat Event**	**Likelihood**	**Severity**	**Risk**
Hackers	Sensitive information is leaked to public due to exfiltration	3	3	9
Former employees	Sensitive information is leaked to public or sold to competitors by the former employees	2	3	6

Threat source	Threat Event	Likelihood	Severity	Risk
Current employees	Disrupt operation activities	2	3	6
Customer	Alter information	1	3	3

Approach

Threat source and events were identified based on likelihood of incidents due to open access permissions. The severity was measured against the impact on day-to-day operational needs. Some hackers might publish this information on the internet and bring down the organization's reputation. As for former employees, there was a case when they left the company and sold the confidential information to the competitors. While it might not happen easily, the severity is high. In addition, the current employees might disrupt operation activities, while customer may alter the information to their heart's content.

Remediation Strategy

- Make it private to protect the confidentiality
- Implement Role-Based Access (RBA)
- Implement authentication, authorization, and audit on the business practices to ensure only authorized users can gain access to the database server
- Implement multi-factor authentication (SMS, email, ID card, employee card, etc.)
- Encrypt the data using TLS instead of SSL (TLS is the new version of SSL) to prevent users from the internet to gain access to the database server