**Assumptions of the Organization**:

The target organization is a medium-sized retail store located in a midsize city and is open 7 days a week. The majority of customers are located within the city, with a small percentage of customers coming from outside the city. The store has an online presence and offers online ordering and payment as well as in-store pickup. The store has two physical locations, one in the city and one in a suburban area. The store also has an online presence, which includes an e-commerce website, a mobile app, and social media accounts. Additionally, the store has a loyalty program, which customers can use to earn rewards and discounts.

**Attack Tree:**

According to the ENISA Threat Landscape 2022-2023, there are eight prime threats, which are categorized under the prominence and the impact of their threat materialism. Mainly, Ransomware, malware, social engineering threats, threat against availability: DOS, internet threats, threats against data, Disinformation Mis information and supply-chain attacks. In addition, among all the listed prime treats, at the time of reporting period, Ransomware and threats of availability are ranked top.

.

Diagram

Description automatically generated

Figure 1 ENISA Threat Landscape 2022 - Prime threats

The main motivation for the treat actor is to gain the access to store data by performing various malicious acts with the help of existing vulnerabilities. Here, the data can be obtained by either accessing into store network or insider threats. Mostly insider threats can be occurred through human errors. Furthermore, a threat actor can perform any malicious acts through gaining access to the store network, online network and their customer data by exploiting their each vulnerabilities respectively. An attacker can perform malware attack by authorized access, if the store network has vulnerabilities such as weak passwords, unpatched data, or unsecured network. In the other hand, and threat actor mostly perform malicious acts by taking the advantage of website vulnerabilities. Such as SQL injection, XSS, social engineering and DDos Attacks. Through the social engineering attacks, and threat actor can manipulate the data from the customers by performing phishing attacks, such as email phishing and smishing. Where smishing is technique used gain the personal or financial data via SMS. Additionally , ransomware is one of the most top attack, which can be exploited via botnet attacks and threat actors can perform amplification attacks, where an attacker generates the high volume of packets to the target network by carry out DDoS attack. Moreover, attacker obtain the customer data by performing Brute force attack, user account hijacking of online account and threats against data. In the current treat landscape, threat against data is one of the popular threats used by the attackers. It is the threat against the target by collection of data to gain the unauthorized access and manipulation of data via unencrypted data by interfacing with the system behaviour.

The attack tree shown below outlines possible methods of attacking the retail store. It begins with the root node, which is the goal of the attacker, which is to gain access to the store's data.

Insider Threats

Access Physical Store Locations

Gain Access to Store Data

Obtain Customer Data

Gaining Access to Online Store

Gaining Access to Store Network

Human Errors

Exploiting Web Application Vulnerabilities

Access Customer data

Exploiting Network Vulnerabilities

Exploiting Software Vulnerabilities

Brute-Force Attack

Password Guessing

Attacks

Exploit Weak Passwords

Exploit SQL Injection

Credential Stuffing Attacks

User Account Hijacking

Exploit Unsecured Network Connections

Threats against data

Exploit Unpatched Software

Exploit Unencrypted Data

Exploit Cross-Site Scripting

Exploit Unencrypted Data

Exploit Unauthorized Access

Exploit Unprotected Wi-Fi Networks

Email Phishing

Phishing Attacks

Social Engineering

Smishing

Exploit Unauthorized Access

Ransomware

Botnet Attacks

Distributed Denial-of-Service (DDoS) Attacks

Amplification Attacks

Malware

**Security Recommendations:**

To protect the store's data, the following security measures should be implemented:

1. Implement access control measures at the physical locations of the store, such as keycard access and CCTV surveillance.

2. Regularly review and update the store's software and systems, including patching any known vulnerabilities.

3. Implement strong password policies, such as multi-factor authentication, complexity requirements, and password rotation.

4. Ensure that all data is properly encrypted, both in transit and at rest.

5. Scan the network regularly for any unauthorized access or vulnerabilities.

6. Ensure that the store's Wi-Fi connection is secure, with strong encryption and authentication.

7. Regularly review and update the store's web applications, such as e-commerce site and mobile app, for any vulnerabilities.

8. Implement access control measures for customer data, such as multi-factor authentication for access and encryption for data in transit and at rest.

9. Educate employees and customers on safe online practices, such as using strong passwords, avoiding phishing attacks, and not sharing sensitive information.

These security techniques, methods, controls, and procedures are designed to protect the store's data from unauthorized access and exploitation of vulnerabilities. By implementing these security measures, the store can protect its data and ensure that it is not compromised.

By implementing these security measures, the store can protect its data and ensure that it is not compromised. Furthermore, these measures can help mitigate the threats outlined in the attack tree, such as the exploitation of software and network vulnerabilities, and the unauthorized access of data. With these measures in place, the store can be better prepared to defend against potential attacks and protect its data.