AN ANALYSIS OF THE TJX DATA BREACH

This document contains a summary of the 2007 TJX Data Breach.

Jordan Patterson

2024

Analysis of the TJX Data Breach

Jordan Patterson

Introduction

Summary of Events

The TJX data breach occurred in 2007 and remain as one of the largest and most important in terms of security breaches and served as a milestone in sense of security awareness. TJX, the parent company of TJMAXX, Marshalls and Homegoods, was targeted by a group of cybercriminals who took advantage of a weak network security environment and were able to steal the information of around 94 million accounts and approximately 80 Gb of sensitive data.

The breach was discovered in 2007, however its is believed that intruders have been inside the company's network since 2005. The attackers breached the security of the network of at two Marshalls stores in Miami and then installed a sniffer program to capture sensitive information which allowed them to collect large amounts of sensitive information, including debit/credit card data (CCV and expiration dates) and personal information of costumers (addresses, driver license).

The incident was one of the first high profile attacks since the implementation of the Payment Card Industry Data Security Standard (PCI DSS) in June 2005. After the attack, it was discovered that TJX was non-compliant with 9 out of the 12 requirements stablished by the PCI DSS, this included misconfigured wireless network, improper anti-virus protection, weak intrusion detection, use of usernames and passwords that were easily cracked, and improper patch procedures and log maintenance.

Identified vulnerabilities.

After the attack, the company conducted internal investigations and external forensics investigation which identified the following main vulnerabilities on TJX infrastructure:

1. Use of a weak security algorithm such as WEP for its wireless connection
2. Lack of network segmentation of the cardholder data from the rest of the TJX network.
3. Lack of encryption which caused all the sensitive cardholder data to be stored in plaintext.
4. Lack of a continuous monitoring of the network and audit logs.
5. Lack of proper firewall implementation

Analysis of the TJX Data Breach

Jordan Patterson

Key Critical Controls as outlined in CIS Critical Security Controls v8.

The following controls are suggestions sourced from CIS Critical Security Controls V8 that could have prevented or lessened the impact of the TJX breach.

1. Use of Secure Network Management and Communication Protocols

Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).

- **Attack Vector:** Weak wireless encryption.

- **How this control would prevent a similar attack:** In the case of the TJX breach, threat actors were able to gain access to the stolen data by accessing TJX's wireless network because it was using weaker form of encryption, WEP. If TJX had been using WPA (available in 2003) or WPA2 (available in 2004), the attackers may not have been able to gain entry to the network, stopping the breach at its source.

2. Establish and Maintain a Secure Network Architecture

Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.

- **Attack Vector:** Unsecure network architecture.

- **How this control would prevent a similar attack:** If TJX's network had been properly segmented, the attackers would not have been easily able to move laterally across the network, install malware or sniffing programs, gain access to servers, databases, and other critical resources.

3. Encrypt Sensitive Data at Rest

Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.

- **Attack Vector:** Unencrypted or weakly encrypted stored data.

- **How this control would prevent a similar attack:** TJX was found to have been storing data using a previously deprecated and vulnerable encryption standard as well as storing credit/debit card data completely in plaintext with no encryption whatsoever. Had TJX properly encrypted all data at rest using proper encryption methods, customer data may have still been accessed but would be unreadable and unusable by the threat actors.

4. Conduct Audit Log Reviews

Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.

- **Attack Vector:** No frequent log reviews.

- **How this control would prevent a similar attack:** After further investigation, it was found that TJX had threat actors for nearly 18 months before they were discovered. If audit logs had been reviewed regularly, or at all, the breach and any other further anomalies would have been detected much sooner, limiting the damage and impact of the breach.

5. Implement and Manage a Firewall on Servers

Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.

- **Attack Vector:** No proper firewalls in place.

- **How this control would prevent a similar attack:** The proper implementation of Firewalls at key point on the network, such as points where a major change in the network occurs or at each office or store could have stopped the threat actors from not only gaining access to the network but also from moving across it. A proper firewall implementation along with the regular log reviews suggested above would have alerted TJX to the intrusion attempts much sooner, if not right away.

Analysis of the TJX Data Breach

Jordan Patterson

Sources

The 18 CIS Critical Security Controls (cisecurity.org)

TJX data breach: At 45.6M card numbers, it's the biggest ever | Computerworld

The TJX Hack: A Case Study in Retail Cybersecurity | LinkedIn

Case Study: TJ Maxx's Data Breach | by Edwin Covert | Medium

⇉Security Breach in TJX Company Essay Example | GraduateWay

TJX Breach Could Have Been Avoided - Information Technology Planning, Implementation and IT Solutions for Business - News & Reviews - BaselineMag.com

Wi-Fi Protected Access - Wikipedia