Kevin Hamzaj 2687959

Cybersecurity II

Module 11

19 November 2023

**Module 1 :** I chose number 8 (Financial compromise: PAYMENT CARD) attack vector because it represents a major and widespread cybersecurity threat that can have serious consequences for individuals, companies, and institutions. Payment card data breaches and financial compromises have been increasing in recent times, resulting in financial losses, damage to reputations, and legal repercussions for victims. I am not too familiar with the details of this, so I am very excited to go into depth on this topic!

**Module 2 :** Name and Date of Attack: Target Data Breach, First reported in December 2013

How the Attack was Detected:

The attack was initially detected when the US Secret Service informed Target about suspicious activity related to credit card data.  
Target's internal security systems also detected anomalies but failed to raise significant alarms.

How the Attack was Analyzed:

Target's cybersecurity team worked with third-party forensics experts to analyze the breach.  
They discovered that hackers gained access to Target's network through a third-party HVAC vendor's credentials.  
The attackers installed malware on Target's point-of-sale (POS) systems to steal payment card data during transactions.

How the Attack was Contained:

Target took immediate steps to contain the breach, including shutting down the unauthorized access points and removing the malware from their systems.  
They also enhanced their network security and revised their access management policies to prevent future breaches.

How the Attack was Eradicated:

Target cooperated with law enforcement agencies in the investigation, which ultimately led to the identification and apprehension of the individuals responsible for the attack.

**Module 3 :** The three HIPAA Technical Controls discussed Access Control, Audit Controls, and Encryption and Decryption play a crucial role in thwarting financial compromise cyber attacks, specifically those targeting payment methods. By implementing these controls effectively, healthcare organizations can enhance their cybersecurity posture and protect patient data from unauthorized access and financial loss. It is essential for healthcare entities to continuously assess and update their security measures to stay ahead of evolving cyber threats in the digital age.

**Module 4 :** Outcome 1: Financial Loss and Theft This is the most damaging outcome. A successful financial compromise can result in substantial financial losses for individuals or organizations.

Outcome 2: Reputation Damage Financial compromises can lead to reputational damage, particularly for businesses.

Outcome 3: Legal and Regulatory Consequences A financial compromise can result in legal and regulatory consequences, including fines, penalties, and legal action.

Outcome 4: Operational Disruption Financial compromises can disrupt business operations.

Outcome 5: Customer Trust Erosion While similar to reputation damage, erosion of customer trust is distinct.

**Module 5:**

Phishing Emails:

Delivery Method: Phishing emails are crafted to appear as legitimate communications from banks, payment processors, or financial institutions.

Means of Compromise: When recipients click on links in these emails or download malicious attachments, they might be redirected to fake login pages or have malware installed on their devices.

Contribution: Phishing emails are the initial point of contact for attackers. They trick individuals into revealing their payment information or installing malware, which can then be used to compromise financial transactions.

Malware:

Delivery Method: Malware can be delivered through various means, including malicious email attachments, infected websites, or compromised software downloads.

Means of Compromise: Once malware infects a system, it can monitor keystrokes, capture data entered during online banking sessions, or gain control of the device.

Contribution: Malware is a direct means of compromise. It enables attackers to steal sensitive financial data, including usernames, passwords, credit card numbers, and banking credentials. This stolen information can then be used to commit fraudulent financial activities.

SQL Injection:

Delivery Method: SQL injection attacks target vulnerable websites or web applications with poorly protected input fields.

Means of Compromise: By injecting malicious SQL code into input fields, attackers can manipulate databases and retrieve sensitive payment data stored within them.

Contribution: SQL injection attacks directly compromise the security of payment systems. Attackers can gain unauthorized

access to databases containing payment information, potentially leading to data breaches and financial losses.

**Module 6 :** Technology 1:Behavioral analytics Definition: Behavioral analytics is a technology that uses artificial intelligence to analyze user behavior and identify patterns that may indicate malicious activity.

How it impacts Financial Compromise, Payment Method: Behavioral analytics can be used to detect financial compromise attacks by identifying unusual patterns in user behavior, such as:

Multi-factor authentication (MFA)

Definition: Multi-factor authentication (MFA) is a security measure that requires users to provide two or more factors of authentication to gain access to an account or system.

Tokenization

Definition: Tokenization is a security measure that replaces sensitive data with a unique token. The token can be used to make transactions without exposing the underlying data.

**Module 8 :** The strike had a huge impact. The hack affected approximately 10,000 consumers and is estimated to have cost $1 million. The attack was launched because of a flaw in our payment processing systems. The attacker took advantage of this flaw to gain access to our systems and steal credit card information. To prevent such assaults in the future, some things that can be done are to repair the flaw in our payment processing systems. Multi-factor authentication should be implemented for all users that have access to our payment processing systems. Regularly audit the security of our systems and networks. Monitor systems for unusual activity and respond quickly to any notifications. Educate personnel on best security practices. This was a terrible situation, but you have to be determined to learn from our mistakes and improve our security posture. Steps must be taken to mitigate the impact of the assault, prevent such attempts in the future, and contact customers who have been affected.

**Module 10 :** Account Takeover Indicators

Description: Account takeover indicators involve unauthorized access to user accounts, potentially leading to financial compromise. Indicators may include multiple failed login attempts, changes in account details (password, email address), or unexpected login locations.

Relation to CAM: In the case of financial compromise through payment methods, gaining control of user accounts allows attackers to manipulate payment information, make unauthorized transactions, or exploit stored payment details. If an attacker successfully takes over an account associated with a payment method, they can initiate transactions on behalf of the legitimate user, leading to financial losses.

Monitoring Strategy: Implementing multi-factor authentication (MFA) is a fundamental measure to strengthen the security of user accounts. Monitor and log failed login attempts, tracking changes in account details, and set up automated alerts for suspicious activities. For instance, multiple failed login attempts within a short period or account access from unusual locations can trigger alerts. Regularly review access logs and employ behavioral analytics to identify anomalies in user behavior that may indicate an account takeover.