📝 Project 2| Research on Major Cybersecurity Breach

BY OLANIYAN OLUSEGUN OYENIYI

Suggested Breach Research: Target Data Breach 2013

Overview of the Breach

Overview: Target Corporation is a leading American retailer, operating numerous stores across the United States and offering a wide array of products, from clothing to electronics.

Breach Timeline:

- **November 27 – December 15, 2013:** Cybercriminals infiltrated the network, compromising approximately 40 million credit and debit card accounts.
- **December 18, 2013:** Security expert Brian Krebs reported that Target was investigating a major data breach.
- **December 19, 2013:** Target confirmed the breach, revealing that customer names, card numbers, expiration dates, and CVV codes were stolen.
- **December 27, 2013:** Target disclosed that encrypted debit card PIN data had also been stolen.
- **January 10, 2014:** Target announced that up to 70 million additional customers had personal information compromised, including names, phone numbers, email addresses, or mailing addresses.

Breach Methodology: Attackers gained access to the targeted network by stealing credentials from a third-party vendor, Fazio Mechanical Services, a provider of HVAC systems. They installed malware known as Black PÒS on Target's point-of-sale (POS) systems, which harvested payment card data during transactions.

Impact Analysis:

- **Financial Impact:**
    - **Immediate Costs:** Target incurred approximately $61 million in expenses related to the breach response, including customer notifications, credit monitoring services, and legal fees.
    - **Long-Term Costs:** By the end of 2015, Target reported total losses of $290 million associated with the breach.
- **Reputational Damage:**
    - **Customer Trust:** The breach led to a significant decline in customer confidence, resulting in a 3-4% drop in transactions during the holiday season.
    - **Media Coverage:** Extensive media attention highlighted vulnerabilities in Target's security measures, further damaging its public image.
- **Operational Consequences:**
    - **Leadership Changes:** The breach contributed to the resignation of Target's Chief Information Officer in March 2014 and CEO Gregg Steinhöfel in May 2014.
    - **Security Overhaul:** Target undertook a comprehensive review and enhancement of its cybersecurity practices, including appointing a new Chief Compliance Officer.

Lessons Learned:

- **Exploited Vulnerabilities:**
    - **Third-Party Access:** Attackers exploited weak security practices of a third-party vendor to gain access to Target's network.
    - **POS System Vulnerabilities:** The use of outdated POS systems without adequate malware detection allowed the installation of Black PÒS malware.
- **Preventive Measures:**
    - **Vendor Management:** Implement stringent security requirements and regular assessments for third-party vendors.
    - **Network Segmentation:** Isolate sensitive systems, such as payment processing networks, from other parts of the corporate network.
    - **Advanced Threat Detection:** Deploy real-time monitoring and advanced intrusion detection systems to identify and respond to threats promptly.
- **Post-Breach Actions:**

- **EMV Technology Adoption:** Accelerated the implementation of chip-and-pin (EMV) technology to enhance payment security.
- **Security Training:** Enhanced employee training programs to recognize and respond to security threats effectively.

Shield's Guide Takeaway:

To bolster its cybersecurity defenses, Shield's Guide can apply the following recommendations:

1. **Enhance Third-Party Risk Management:**
    I) **Action:** Establish comprehensive security protocols for vendors, including regular security assessments and access controls.
    II) **Rationale:** Mitigates risks originating from third-party relationships, similar to the vulnerability exploited in the Target breach.
2. **Implement Network Segmentation:**
    I) **Action:** Divide the network into distinct segments to limit access to sensitive data and critical systems.
    II) **Rationale:** Contains potential breaches, preventing lateral movement within the network.
3. **Adopt Advanced Threat Detection Systems:**
    I) **Action:** Deploy sophisticated monitoring tools capable of detecting and responding to anomalies in real-time.
    II) **Rationale:** Facilitates early detection of malicious activities, reducing the window of opportunity for attackers.

By integrating these strategies, Shield's Guide can significantly strengthen its cybersecurity posture and reduce the likelihood of a breach similar to Target's 2013 incident.

Source:en.wikipedia.org