The Target Data Breach (2013)

Marie Madeleine Anita Bekono

Old Dominion University

CYSE 300

Dr. Joseph Joe Kovacic

08/10/2023

The Target Data Breach (2013)

Introduction

In late 2013, Target Corporation, one of the largest retailers in the United States, became the victim of a devastating data breach that exposed the private and financial information of tens of millions of customers. On November 27, cybercriminals installed malware on Target's point-of-sale systems that allowed them to steal debit and credit card data from buyers at over 1,000 Target shops throughout the vacation shopping season. By the time Target detected the breach over a month later on December 15, the hackers had accessed as much as forty million credit and debit card accounts, encrypted PINs for debit cards, names, addresses, smartphone numbers, and e-mail addresses for as many as 70 million clients. The Target information breach changed into one of the biggest ever retail cyberattacks and highlighted the vulnerabilities of major businesses to cyber threats despite security measures in the region. The incident significantly damaged Target's popularity and earnings.

Cybersecurity vulnerabilities

The predominant cybersecurity vulnerability that enabled the massive data breach turned into Target's lack of the right segmentation between extraordinary elements of its network. The outlets had set up a $1.6 million malware detection tool through the protection organization FireEye that flagged the initial breach. However, Target had no longer set up the tool to monitor its factor-of-sale systems and payment card reader network one at a time from the rest of its corporate structures. So, while hackers infiltrated the payment network, the tool did not locate the anomaly. Furthermore, Target had no regulations to quarantine or delete potentially malicious documents (Shu et al., 2017). Moreover, while Target acquired multiple signals from each FireEye and its anti-malware systems, it did not act on them or check out further. Target additionally did

not use end-to-end encryption for card information, permitting hackers to enter credit score and debit card information by breaching a part of the machine. These vulnerabilities led to hackers being capable of passing freely within Target's network and stealing valuable customer Information.

Threats

The principal threat actor that exploited the vulnerabilities in Target's community was a complicated organization of cybercriminals engaged in an ongoing worldwide hacking operation to steal payment card records. This institution applied a complicated malware called a RAM scraper, which allowed them to get entry to the memory of point-of-sale systems and scrape credit and debit card information as it was being processed. The malware was spread inside Target's network via compromised dealer credentials. The hackers had taken advantage of getting entry to Target's structures by breaching the Fazio Mechanical network, a refrigeration contractor that worked with Target. From there, they leveraged Fazio's trusted dealer to get the right of entry to enter Target's corporate community and navigate to the payment systems (Manworren et al., 2016). Additionally, the hackers exploited Target's lack of network segmentation and monitoring to steer clear of detection while exfiltrating huge quantities of monetary and personal consumer data over weeks. The sophisticated malware and multi-step attack vector allowed the cybercriminals to carry out one of the largest retail data breaches.

Repercussions

The Target information breach had massive financial, felony, and reputational repercussions for the company. Financially, Target estimated overall losses of around $292 million, which includes expenses for criminal fees, software updates, purchaser reimbursement, and reduced sales. Its earnings dropped 46% in the fourth quarter of 2013 compared to the previous

12 months. Target additionally faced over 90 lawsuits from banks, shareholders, and clients searching for damages, ultimately settling a main elegance-motion suit for $10 million in 2015. From a legal point of view, Target was discovered to no longer be compliant with industry records protection standards such as PCI DSS at the time of the breach. The company agreed to enforce more potent cybersecurity measures beneath consent decrees with country and federal organizations (Plachkinova et al., 2018). Reputationally, Target suffered fundamental backlash and agreed with issues with clients for permitting their non-public and economic records to be compromised. The enterprise's CEO, in the end, resigned because of the breach fallout. The Target case highlighted the significance of cybersecurity due diligence and compliance for shops handling consumer data. It served as a warning call to prevent comparable attacks.

Cybersecurity measures

Target should have carried out numerous key cybersecurity practices to bolster its defenses and prevent the breach.

- ✓ Firstly, the right network segmentation with firewalls between the payment device network and the rest of Target's infrastructure could have contained the malware. Secondly, strengthening supplier entry to controls and monitoring third-party partners may have prevented the preliminary foothold hackers gained.
- ✓ Target must deploy end-to-end encryption of payment card information to make stolen credit card numbers unusable. More rigorous monitoring of its anti-malware equipment and quicker reaction to indicators should have also detected the breach faster.
- ✓ Regular security audits, retaining software patched and up to date, tremendous employee cybersecurity schooling, and compliance with charge industry records protection standards are other crucial measures.

- ✓ Additionally, having clear incident reaction plans to deactivate compromised charge structures quickly and notify clients quicker could have greatly mitigated the results. Despite having sure cybersecurity equipment in the area, Target needed to adhere to basic safety hygiene practices and lacked comprehensive, layered protection.
- ✓ Implementing current cybersecurity frameworks can assist stores like Target in constructing organizational resilience, retorting successfully to threats, and guarding customer Information.

Conclusion

The 2013 Target data breach became a seminal incident highlighting the growing peril of cyberattacks in opposition to primary organizations. The breach resulted in the loss of extremely sensitive payment cards and personal data of up to 110 million Target customers throughout the height of the holiday shopping season. Though Target had sure cybersecurity measures in place, vulnerabilities like inadequate network segmentation and supplier oversight allowed hackers to gain access and exfiltrate large quantities of monetary information undetected for two weeks. The breach became a watershed moment that cost Target over $290 million in damages and multiplied the rush for shops to revamp fee safety and infrastructure. Additionally, it underscored the want for robust cybersecurity standards and practices to prevent future attacks. While data breaches remain unfortunate, the Target case served as a critical lesson for companies to become aware of and resolve protection gaps or face the danger of compromising consumer conviction and their bottom line.

References

Manworren, N., Letwat, J., & Daily, O. (2016). Why you should care about the Target data breach. *Business Horizons*, *59*(3), 257–266.

Plachkinova, M., & Maurer, C. (2018). Security breach at target. *Journal of Information Systems Education*, *29*(1), 11-20.

Shu, X., Tian, K., Ciambrone, A., & Yao, D. (2017). Breaking the target: An analysis of target data breach and lessons learned. *arXiv preprint arXiv:1701.04940*.