Noah Salafranca

Professor Zehra

CS 462

Blog

11/28/23

In the holiday season of 2013, one of the largest American retail corporations was hit with a shocking and damaging cybersecurity attack. During the busy Black Friday and Christmas shopping spree, Target Corporation faced a massive data breach that exposed millions of customer's personal and financial information to hackers. The Target incident was one of the most significant cybersecurity breaches in the past decade. As a result, it has a long-lasting influence on the business landscape and led to our current cybersecurity practices. This research paper will dive into the background of the Target breach, cybersecurity vulnerabilities, threats, consequences, measures that could have prevented or alleviated the incident, and how the breach changed the cybersecurity landscape.

With 1,948 locations nationwide today, Target has established a reputation for providing affordable home goods, apparel, groceries, and more. Nevertheless, Target had a disastrous data breach near the end of November 2013 that resulted in the loss of almost 110 million consumers' financial and personal data. Hackers were able to install malware into Target's security and payment systems. The malware could steal information from every credit card used at all 1,797 U.S. stores (Manworren et al., 2016). The Target data breach went down after hackers gained access to credentials from a company called Fazio Mechanical Services, a third-party contractor that worked on Target's heating, ventilation, and air conditioning services. With the network of Fazio Mechanical Services compromised, the hackers could use it as a pathway to Target's payment systems. Once inside Target's network, the hackers went through Target's payment system to gain access to and infect the devices used to process debit and credit card transactions

Noah Salafranca

Professor Zehra

CS 462

Blog

11/28/23

with malware, the point of sale, or POS terminals. As the malware moved through the point-of-sale terminals, it worked secretly, gathering private information, including names, credit card numbers, and expiration dates. This incident made Target's weaknesses in its network security processes clear, which also clarified the necessity for more robust cybersecurity measures to secure sensitive data.

Through the utilization of advanced technology, cybercriminals could execute the data breach. The malicious software used was a type of malware called memory-parsing or RAM scraper malware. The malware was created to avoid detection by security systems and exploit network defenses' vulnerabilities. The attack specifically targeted the protocols used to transmit payment data. As a result, this covered the protocols used for communication between the central servers that process transaction data and the point-of-sale terminals. The malware could sneak into and intercept data from the system's random access memory (RAM), where unencrypted data is momentarily kept during transactions. Ultimately, the attackers' use of this cutting-edge technology emphasizes how cyber dangers constantly change and how cybersecurity measures must be continuously improved.

Target's most significant security flaw was the lack of encryption at the point-of-sale terminals. For processing purposes, the data is momentarily decrypted during a transaction. Because encryption was not in place, the attackers had a brief opportunity to intercept the private data. Another vulnerability that was exploited was Target's inadequate network architecture.

Noah Salafranca

Professor Zehra

CS 462

Blog

11/28/23

Target's network architecture needed to be properly segmented. The attackers could gain access and quickly move through the network, eventually reaching the point-of-sale (POS) systems.

Additionally, Target had another vulnerability to address, which was weak authentication protocols. The credentials of Target's HVAC vendor, Fazio Mechanical Services, were taken in the first intrusion. Consequently, this revealed flaws in the authentication procedures, such as weak passwords and inadequate access controls. With the system weaknesses of third-party HVAC providers being taken advantage of, it also draws attention to the risks that linked networks create. Companies frequently depend on various third-party providers, and any holes in their security might be used to infiltrate the target company's network. Furthermore, Target's initial vulnerability was due to the need for proper employee training on cybersecurity threats. The first breach was influenced by social engineering. Employees of Fazio Mechanical Services have unintentionally assisted in the breach by falling for phishing or other social engineering techniques. Employees who have received thorough training are better equipped to spot questionable activity and report it.

The main threat that exploited these vulnerabilities was phishing attacks. Phishing is a cyber threat involving using fake messages that aren't what they seem to steal sensitive information. Such sensitive information could be account passwords, credit card information, and other personal information. Phishing creates fake communication by impersonating a reliable source to scam the victim into inadvertently giving up their confidential information. In these fake messages, standard phishing techniques include statements that are too good to be true,

Noah Salafranca

Professor Zehra

CS 462

Blog

11/28/23

urgent messages, hyperlinks, attachments, and unusual senders. Messages too good to be true usually consist of winning prizes that prompt the victim to enter their information. Urgent messages give a sense of urgency to the victim in their statement. As a result, it will lead the victim to click a link or download something malicious out of desperation. Finally, hyperlinks are fake links that direct you to a different site than expected. For example, a hyperlink could be a link that looks like a well-known, trusted site but is slightly misspelled by one letter.

The 2013 Target data breach significantly affected the corporation and its clients. The incident impacted a startling amount of consumers; the personal and financial information of almost 110 million people was exposed to credit and debit card information and customer records. A substantial financial loss came from this data breach as well. Target lost $18.5 million in the data breach and about $290 million, including fines, reimbursement, investigation costs, and other expenses. Target took a loss, and the customers also took a beating. Around 40 million customers were affected by the data breach, with their credit information stolen. Investigators found the stolen credit card information on the dark web for sale. Millions of dollars were spent on the litigation and settlements that followed, the investigation and mitigation of the breach, and other related expenses. Additionally, the hack significantly tarnished Target's credibility as a reliable shop. Sales fell off, and the brand's reputation was damaged due to the incident, reducing consumer trust and loyalty. The effects on Target and its clients are a reminder of the unfortunate outcomes that may result from a significant cybersecurity attack. However, the Target data

Noah Salafranca

Professor Zehra

CS 462

Blog

11/28/23

breach did bring about more awareness of cybersecurity. Eventually, cybersecurity procedures were strengthened.

The Target data breach in 2013 had far-reaching effects that are still felt in today's society. This data breach caused people to lose trust in businesses and spread awareness of the importance and need for cybersecurity measures. The attack revealed the vulnerability of financial and personal data in the modern digital world, serving as a wake-up call for both consumers and corporations. Since then, the increased knowledge of cybersecurity risks in the retail industry and beyond has had one of the most extensive effects. Consumers started to call for businesses to implement more robust security measures as they became more cautious about disclosing personal information.

Additionally, policies concerning the protection of data had to be improved. Businesses have significantly increased their investments in cybersecurity infrastructure, especially retail ones. It is now a standard protocol to utilize encryption technology, secure payment processing procedures, and regular network activity monitoring. Ultimately, the 2013 Target data breach had a significant social impact. It served as a reminder of the value of taking preventative measures for cybersecurity instead of responding to incidents after they happen.

Some measures that could have been taken to prevent or mitigate the incident are better cybersecurity training and procedures. For example, intrusion detection systems notify IT specialists and cybersecurity analysts of intrusions to execute the proper response. Establishing reliable monitoring systems that continuously evaluate network activity will help detect unusual

Noah Salafranca

Professor Zehra

CS 462

Blog

11/28/23

activity and possible security breaches. Additionally, if Target had segmented its network and responded to security alerts, hackers wouldn't have been able to steal sensitive information or at least had a more difficult time. When a company has a clear incident response strategy, it can act quickly to lessen the effects of security breaches. Furthermore, employees should be trained to recognize cybersecurity threats. Regular cybersecurity awareness training for employees contributes to developing a human firewall that protects against social engineering assaults. Along with training employees, implementing stronger authentication methods, such as multi-factor authentication, can provide an additional layer of security. If login credentials are hacked, the extra authentication can be the difference between an attack occurring.

The 2013 Target data breach can serve as a reminder of the cybersecurity threats that the world faces every day. The lessons from the Target data breach are still applicable as society strives to keep up with the ever-changing landscape of cybersecurity threats. Cybersecurity has become a prime concern for many companies and businesses. Businesses reevaluated their security procedures as a result of the attack, increasing spending on cybersecurity infrastructure and putting an increased emphasis on preventative measures. Since the stakes are so significant in this digital age, awareness must be raised by learning more about cybersecurity, recognizing threats, and understanding security measures so people can digitally protect themselves.

Noah Salafranca

Professor Zehra

CS 462

Blog

11/28/23

References

KnowBe4. (n.d.). *What is phishing?*. Phishing. https://www.phishing.org/what-is-phishing

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

Middleton, Bruce. “Target Data Breach—2013.” *A History of Cyber Security Attacks*, 1st ed., vol. 1, Routledge, 2017, pp. 119–124.

Rashid, Fahmida Y. “How Ram Scraper Malware Stole Data from Target, Neiman Marcus.” *PCMAG*, PCMag, 14 Jan. 2014, www.pcmag.com/news/how-ram-scraper-malware-stole-data-from-target-neiman-marcus .

The 2013 Target Data Breach & third-party risk management. Prevalent. (n.d.). https://www.prevalent.net/blog/the-2013-target-data-breach-a-lasting-lesson-in-third-party-risk-management/#:~:text=During%20the%202013%20holiday%20shopping,veritable%20Holy%20Grail%20of%20PII!