Shannon Hensley

PCI Compliance: Is it Enough?
PCI DSS, Target, and Kaptoxa

On Dec. 19, 2013 the following message was released from Target Stores:

> "We wanted to make you aware of unauthorized access to Target payment card data. The unauthorized access may impact guests who made credit or debit card purchases in our U.S. stores from Nov. 27 to Dec. 15, 2013. Your trust is a top priority for Target, and we deeply regret the inconvenience this may cause. The privacy and protection of our guests' information is a matter we take very seriously and we have worked swiftly to resolve the incident.
>
> We began investigating the incident as soon as we learned of it. We have determined that the information involved in this incident included customer name, credit or debit card number, and the card's expiration date and CVV.
>
> We are partnering with a leading third-party forensics firm to conduct a thorough investigation of the incident and to examine additional measures we can take that would be designed to help prevent incidents of this kind in the future. Additionally, Target alerted authorities and financial institutions immediately after we discovered and confirmed the unauthorized access, and we are putting our full resources behind these efforts." (Steinhafel)

The breach of security came at the height of the Christmas shopping season with first estimates posted by Target Dec. 19, 2013 as “approximately 40 million credit and debit card accounts may have been impacted” (Target) Later, it was revealed that as many as 110 million of Target customers could have been effected. As reported by Torey Van Oot of NBC News, “an ongoing internal investigation into the hack found that the breach also included names, mailing addresses, phone numbers or email addresses for 70 million customers. Some of the personal information stolen was obtained by the store prior to the breach.” (Van Oot)

The breach occurred in store point of sale systems only; online Target.com users were not affected. (Krebs on Security) According to Krebs, “The type of data stolen — also known as “track data” — allows crooks to create counterfeit cards by encoding the information onto any card with a magnetic stripe. If the thieves also were able to intercept PIN data for debit transactions, they would theoretically be able to reproduce stolen debit cards and use them to withdraw cash from ATMs.” (Krebs on Security)

Ongoing investigations point to the fact that the breach many have originated with Fazio Mechanical Services, a small, Pittsburgh based, heating and refrigeration contractor which has a data connection with Target for the purpose of billing. (Shaer)

The malware reportedly involved in the breach has been named “Kaptoxa”, and is thought to be of Russian origins because “Some parts of the malware code were written in Russian, and BlackPOS, the malware from which this latest malware derived, was originally developed by a Russian cyber-crime master, according to Tiffany Jones, an executive at online security firm iSIGHT Partners.” (AP)

More on Kaptoxa from Kim Zetter of Wired.com:

> “The tool monitors memory address spaces used by specific programs, such as payment application programs like pos.exe and PosW32.exe that process the data embossed in the magnetic strip of credit and debit cards data. The tool grabs the data from memory because some companies transmit card data via a secured channel inside their corporate network, which would prevent the attackers from sniffing the data in transit.”
>
> “The siphoned data is stored on the system, and then every seven hours the malware checks the local time on the compromised system to see if it’s between the hours of 10 a.m. and 5 p.m. If so, it attempts to send the data over a temporary NetBIOS share to an internal host inside the compromised network so the attackers can then extract the data over an FTP — file transfer protocol — connection.” (Zetter)

So how did this breach happen? Are there not safeguards in place to keep this exact scenario from happening?

Yes there are.

On September 7, 2006 by the major credit card companies (American Express, Discover, MasterCard, and Visa) formally launched the security standards known as the Payment Card Industry Data Security Standard.

The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that ALL companies that process, store or transmit credit card information maintain a secure environment. Essentially any merchant that has a Merchant ID (MID). (PCI Compliance Guide)

According to Oracle the core concepts of PCI DSS are “a set of principles and specific requirements around which various aspects of the security standard are covered.” (Oracle)

These guiding principles are:

- Build and maintain a secure network
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy

With the PCI DSS principles and policies set in place by the major credit card companies where does the blame for the Target breach fall: Target or on the major credit card companies? It is a little disconcerting to know that Target was in complete compliance with PCI DSS.

"Target was certified as meeting the standard for the payment card industry in September 2013. Nonetheless, we suffered a data breach." Target Chairman, President, and Chief Executive Officer Gregg Steinhafel was quoted as saying. (Mello Jr.)

So does this place the sole blame for the breach on the credit card companies and a weak PCI DSS? No not at all.

According to Kamesh Namuduri of the University of North Texas, “The PCI DSS forms the minimum set of requirements or the baseline for protecting customer information. A critical analysis of the requirements of compliance reveals that auditing for compliance purposes should not be viewed as a onetime or an ad hoc effort.” (Namuduri 45-51)

This one quote should be the lesson learned from one of the biggest, is not the biggest, point of sale system hacks in history. . The concept of the PCI DSS is a great one: protect cardholder and customer data, but he PCI DSS should be help as merely a baseline. The process of information security is an ongoing process that needs to be constantly revised and updated.

"Just because you pass a PCI audit does not mean that you're secure," said Eric Chiu, president and founder of HyTrust. "Clearly we saw that in the Target scenario." (Mello Jr.)

So who was to blame for the security breach at target? Perhaps both Target and the credit card companies hold an equal share. PCI DSS could be stronger and more comprehensive in its standards, more strict in its enforcement. Target could have viewed PCI DSS as a baseline and gone beyond its policies in creating a more secure POS network.

Hopefully all parties learned some lessons.

Citations

Steinhafel, Gregg. "a message from CEO Gregg Steinhafel about Target's payment card issues." *corporate.target.com*. Target Stores, 20 Dec 2013. Web. 9 Apr 2014. <https://corporate.target.com/discover/article/Important-Notice-Unauthorized-access-to- payment-ca>.

Target. "Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores." *pressroom.target.com*. Target Stores, 19 Dec 2013. Web. 09 Apr 2014. <http://pressroom.target.com/news/target-confirms-unauthorized-access-to-payment-card-data-in-u-s-stores>.

Van Oot, Torey. "Target: Data Breach Affected Up to 110M Shoppers." *NBC Bay Area*. NBC News, 10 Jan 2014. Web. 10 Apr 2014. <http://www.nbcbayarea.com/news/national-international/Target-Says-Data-Breach-Affected-70-Million-Shoppers-credit-monitoring-239600681.html>.

Krebs on Security. "Sources: Target Investigating Data Breach." *Krebs on Security*. Krebs on Security, 19 Dec 2013. Web. 10 Apr 2014. <http://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/comment-page-3/

Shaer, Matthew. "Target credit card breach may have originated with a small contractor." *The Christian Science Monitor*. The Christian Science Monitor, 07 Feb 2014. Web. 12 Apr 2014.

<http://www.csmonitor.com/Innovation/2014/0207/Target-credit-card-breach-may-have-originated-with-a-small-contractor>.

AP. "Kaptoxa malware with Russian code used to steal Target credit card data." *The Sydney Morning Herald*. The Sydney Morning Herald, 18 Jan 2014. Web. 12 Apr 2014. <http://www.smh.com.au/it-pro/security-it/kaptoxa-malware-with-russian-code-used-to-steal-target-credit-card-data-20140118-hv8vh.html>.

Zetter , Kim. "The Malware That Duped Target Has Been Found ." . Wired, 16 Jan 2014. Web. 14 Apr 2014. <http://www.wired.com/2014/01/target-malware-identified/>.

PCI Compliance Guide, . "PCI FAQs." *PCI Compliance Guide*. PCI Compliance Guide, n.d. Web. 12 Apr 2014. <http://www.pcicomplianceguide.org/pci-faqs-2/>.

* Oracle, . "Getting PCI DSS Compliance Right: How ." *An Oracle White Paper* . Oracle, n.d. Web. 13 Apr 2014. <http://www.oracle.com/technetwork/middleware/id-mgmt/pci-compliance-identity-v2-133468.pdf>.

Mello Jr., John P.. "Target Breach Lesson: PCI Compliance Isn't Enough." *Tech News World*. Tech News World, 18 Mar 2014. Web. 14 Apr 2014. <http://www.technewsworld.com/story/Target-Breach-Lesson-PCI-Compliance-Isnt-Enough-80160.html>.

* Namuduri , Kamesh. *Int. J. Auditing Technology*. 1.1 (2013): 45-51. Print. <http://www.inderscience.com/storage/f610125329114817.pdf>.