TARGET DATA BREACH

December 2013

WHAT HAPPENED

- Hackers broke into Target's network using a third parties information (Vijayan, 2014)
- Information collected from November 27th (Black Friday) - December 15th.
- Effected 110 Million target shoppers
- 11 gigs of data was stolen (Kassner, 2015)

WHAT WAS COMPROMISED?

- Customer information stolen:
  - Credit/debit card numbers, expiration and CVV
  - Emails
  - Names
  - Addresses

- Not Stolen
  - Pin Numbers
  - Social Security Numbers
  - Employee records

HOW TARGET WAS BREACHED

- A phishing email was sent to employees at Fazio Mechanical
- A trojan called Citadel was installed on the HVAC company computers and waited in hiding until discovering login credentials for Target networks.

HOW INFORMATION WAS STOLEN

- Through POS (point-of-sale) system
- Customer information from credit card is stored on POS memory
- Information from POS hardware is sent to POS application software
- Hackers used malware to “dump” user information every 7 hours
- Personal information sold on dark web
  (Manworren, Letwat, & Daily, 2016)

ATTACK STRATEGIES

- It's possible that attackers abused a vulnerability in the web application, such as SQL injection, XSS, or possibly a 0-day, to gain a point of presence, escalate privileges, then attack internal systems." (Kassner,2015)

ATTACK STRATEGIES CONT.

- Radichel in the SANS dissertation offers one theory. "We can speculate the criminals used the attack cycle described in Mandiant's APT1 report to find vulnerabilities," mentions Radichel. "Then move laterally through the network... using other vulnerable systems."(Kassner,2015)

ATTACK STRATEGIES CONT.

- Gary Warner, founder of Malcovery Security, feels servers fell to SQL-injection attacks. He bases that on the many similarities between the Target breach and those perpetrated by the Drinkman and Gonzalez data-breach gang which also used SQL injection.(Kassner,2015)

WHAT HAS TARGET DONE ?

- **The following measures have been implemented through out the company:**
  - Improved monitoring and logging of system activity
  - Installed application whitelisting POS systems and
  - Implemented POS management tools
  - Improved firewall rules and policies
  - Limited or disabled vendor access to their network
  - Disabled, reset, or reduced privileges on over 445,000 Target personnel and contractor accounts
  - Expanded the use of two-factor authentication and password vaults
  - Trained individuals on password rotation

(Ramos, 2014)

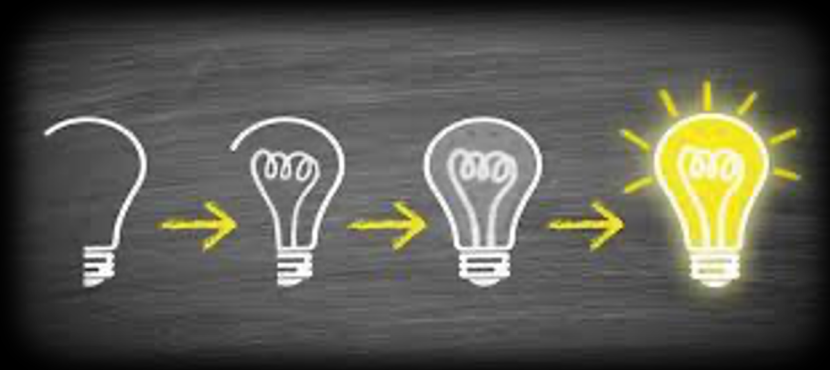
WHAT HAS TARGET DONE?

- Customers given 1 year of credit monitoring and Identity theft protection
- Over 90 settlements equally 202 million dollars
- 10 % discount the weekend following the release of breached data news

(Ramos, 2014)

WHAT THE WORLD LEARNED

- Organizations have to make security a priority
- Criminals have become more sophisticated
- System vulnerabilities make it difficult to detect attacks
- Companies need a contingency plan
  (Kenealy, 2014)



REFERENCES

Kassner, M. (2015, February 2). *Anatomy of the Target data breach: Missed opportunities and lessons learned* . Retrieved from ZDNet: https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/

Kenealy, B. (2014, MAY 12). ORGANIZATIONS STRUGGLE WITH EVOLVING CYBER THREATS. *BUSINESS INSURANCE*, p. 17.

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

Ramos, T. (2014, January 13). Target hack affected 30 million more customers than initially reported. *SNL Bank and Thrift Daily*.

Vijayan, J. (2014, February 6). *Target breach happened because of a basic network segmentation error* . Retrieved from COMPUTERWORLD: https://www.computerworld.com/article/2487425/target-breach-happened-because-of-a-basic-network-segmentation-error.html