PES UNIVERSITY

UE19CS346
INFORMATION SECURITY

Assignment - 01
Target Case Study

Name : Suhan B Revankar
SRN : PES2UG19CS412
Section : G Section

1 .Target was vulnerable and not unlucky. The following supports the same:

- Fazio, an employee at Target who had opened the phishing mail, had enabled the hackers to steal his passwords. Fazio had used the free version of “Malwarebytes Anti-Malware”, a security product which prohibited corporate use. Target did not monitor the vendor’s security requirements.

- Target also ignored the vulnerabilities identified in the firm’s payment card systems and cash registers.

- Target did not make use of two-factor authentication which could have helped prevent the sensitive data from being stolen.

- Target did not have properly segmented networks which enabled the hackers to gain access to sensitive information like payment and card details of the customers. Hackers were able to move about the company’s internal network and even update the malware for other attacks which eventually led to more variants of the malware.

- Target had also ignored the initial security warnings it had received from FireEye which had detected the malware that was installed but hadn’t been activated yet.

The data breach could have been prevented if target did pay heed to the warning it received from FireEye.

2 . Target could have avoided this data breach by being more vigilant and not ignoring the signs of the breach.

- Two factor authentication

The use of two factor authentication could have helped in protecting sensitive data. Two factor authentication protects the data by implementing defense in depth.

- Network segmentation

The network should have been segmented disabling any route between an outsider contractor and the network for the payments.

- Acting on initial warnings

Target should not have ignored the initial signs and warnings it received from FireEye regarding the detection of a malware before it was even activated.

- Security checks on vendors

Target should have had security checks on its vendors like Fazio which could have helped prevent this breach to a great extent.

Target must have been over confident due to no such experiences in the past to not have taken the necessary precautions.

3 . Target’s response to the breach was below par considering it’s popularity among the people. Many customers were disheartened by Target’s response to the security breach.

Target had announced about the breach a week after it was contacted by the DOJ. Moreover, it was announced on its corporate website and not on the more frequented consumer website. Customers weren’t able to connect to Target’s hotline and when they did, they were redirected to a website which wasn't designed.

The board had issued an apology which wasn’t appropriate. Many customers also felt ill-equipped to protect themselves even after the CEO highlighted steps for the concerned customers to follow.

4 . Target’s board of directors were definitely responsible for the disastrous data breach that took place. It is their responsibility to take decisions based on information and perception which could help prevent such a reverse of fortune.

As a member of the board, I would ensure that the Information Security and Cybersecurity teams are vigilant, capable and hardworking and do their job with utmost sincerity.

I would specifically ensure strong security during peak times like christmas since it is the time the store will have most customers visiting. Regular security checks need to be done in order to ensure that all the security is in place and there is no compromise on customer privacy and information.

Strict action must be taken on anyone in this department taking their job lightly since it involves handling of sensitive information. A capable cybersecurity team is now needed to check all logs and ensure that such a mishap doesn’t occur again.

5 . Through the data breach at Target, it is evident that no matter how big or popular a company is, a security breach is very much possible and every company must do its best to ensure the security of the sensitive information it handles.

Prevention:

- Setting strong passwords difficult to decipher
- Security checks on vendors
- Two-factor authentication
- Use of VLANs for network segmentation
- Hashing of sensitive information
- Educating all employees and building awareness about security breaches.

Response:

- Containing the breach by limiting services, isolating the compromised networks, etc.
- Informing the necessary authorities about the attack
- Strong IT and cybersecurity team working on solving the issue and reducing its effect.
- Understanding that a security breach is possible anywhere and sending a polite apology to all the victims of the breach instead meaninglessly defending the company.

6 . As a director in relation to cybersecurity at my organization, I would conduct regular checks to ensure proper implementation of security measures. I would ensure that strong passwords are set and updated often.

- Two factor authentication (2FA) would be introduced to ensure defense in depth. Putting up firewalls and segmenting networks is a must to ensure better security.
- Regular software updates to ensure the software is able to tackle recent security threats would also be released. Employees must be trained and made aware of cybersecurity risks and various preventative measures.

7 . Companies should ensure usage of strong passwords and regular updation of passwords.

Two factor authentication should be implemented in order to ensure defense in depth.

Regular updates of software to ensure defense against latest security threats.Implementation of firewalls and segmentation of networks is a must.

The employees must be educated and made aware of the network and information security and they must be made aware of the response plan in case a threat is identified.

Post the breach, the company must focus on containing the breach by stopping all the services affected by the breach. Higher authorities must be informed about the same and immediate action must be taken. The victims affected by the breach must be informed about the same with utmost honesty and the company must focus on reducing the loss to their best extent.

*****