Equifax Breach

Contents

Overview 2
Presentation of Equifax 2
Causes that provoked this attack 2

What strategies should adopt by Equifax 3

Lessons learned 5

Overview

Presentation of Equifax

Equifax is a multinational credit reporting agency, founded in 1899 and headquartered in Atlanta, Georgia. One of three major US credit reporting agencies, including Experian and Transunion (known together as "the big three").

Equifax holds information of million consumers and business around the world. It sells both commercial credit reports and consumer credit reports to banks, insurance, firms, healthcare and others institutions. Additionally, it sells credit monitoring services, including credit fraud and identity theft prevention services. So Equifax knew enough on the economic life of millions people around the world particularly United State, Canada and British Citizens.

Causes that provoked this attack

To better understand this cyber-breach let's examine the different phase of this attack before that occur.

- First the **reconnaissance** and **research phase.** While this phase the hackers seek to understand the IT infrastructure and figure out what strategies to put in place. For this phase they can use tools to scan the network, use social network to understand behavior of some employees and others media to stay connected with the information about Equifax.
- The second phase is **Weaponization**. They launch attack depending of information that they got while the first phase. In this case the information were the non-update of the Apache Struts an open-source web application framework develop by a third party and the non-renewal of SSL certificate. So they use this vulnerabilities to launch attack.
- The third phase is the **Gaining Access**. By using this vulnerabilities they can get access to the Equifax database.
- 4th Phase is **Exploitation**. After getting access to the IT infrastructure of Equifax, they develop application (malware or others system) that can help them to exploit this vulnerability

- The last phase is **Exfiltration**. They have stolen valuable information of millions consumers and business in the Equifax database.

To resume, they used a vulnerability in an Apache Struts version that is an open-source web application framework develop by a third party to access to the credit system that this application handle, for after exploit this vulnerability to steal Personally identifiable information (PII) of the millions consumers (Non encryption of valuable data).

What strategies should adopt by Equifax

Security is a chain each link in the security chain is very important so design and implement a good security policy become mandatory. And Equifax security team supposed to have on mind the security goals: Confidentiality, Integrity and Availability because all procedures that they are going to implement through the policy security have to meet the security goals. So NIST and ISO 27001 are two good frameworks that they should use to design the policy security and help them to meet the security goals. In addition, Equifax should have a team and budget that allow it to meet security goals and to ensure the protection of the valuable information. The team would be divided and four departments: Security Engineering and Asset Security, Security Operation Center, Emergency Operation and Incident Management and Program Management.

1) Protect, Defend, and Prevent

Department	Activity
Identity and Access Management	Ensure the IAAA (Identification, Authentication, Authorization, Accountability) for all assets in the organization
Applications Security	Ensure the management and the configuration for the applications and software
Security Engineering	Address security throughout the development and acquisition lifecycle.

2) Monitor, Detect, and Hunt

Department	Activity
Security Operations Center	Monitor, detect, analyze and eliminate anomalies in the computer system (virus and malicious code)

3) Respond, Recover, and Sustain

Department	Activity
Emergency Operation and Incident Management	Ensure that Equifax continue to work after an attack. By performing the following actions: 1) Detect 2) Analyze 3) Respond and Recover from security incidents

4) Govern, Manage, Comply, Educate, and Manage Risk

Department	Activity
Program Management, Governance, risk and compliance	Develop, implement, and maintain an information security program and plan

- Offensive Security

To have one step from the hackers you have to know how they think and try to think them. Every 6 months Equifax should engage a pen-test team to try if they can hit Equifax IT infrastructure from inside and outside.

  - Inside

By simulating attack from inside by giving to the pen-test team information on the IT infrastructure to see if Equifax is protected from its employees.

- Outside

The Pen-test team will have as mission to see how it can get access to Equifax Infrastructure by using the different phase of cyberattack presented in the prior paragraph.

Lessons learned

This attack could be avoided if the Equifax IT security team had applied the principles of NIST framework: Identify, prevent, detect, respond and recover. Why this assuming?

First of all, there was a lack of Comprehensive IT Asset Inventory, the IT security team was not able to "identify" the location of the server on which running Apache Struts when the flaw have been detected by the vendor. The reason there was not a complete IT Asset Inventory. Secondly, they did not perform a risk assessment to know what data were more valuable and the server that contained these data. Furthermore the Compliance for PCI-DSS did not meet because the data encryption for the PII do not respected because the hackers had not any problems to read the stolen data.

The second point is "protect/prevent". Given they did not know where find out the server that contained the Apache Struts so the maintenance was impossible at time. The renewal of SSL certificate was not performed in time because the monitoring was not performed by the IT security team.

The third point is "detect". They did not use adequate tools to monitor the IT infrastructure to detect in time vulnerabilities.

The fourth and fifth point are "respond" and "Recover". There was no plan to respond and recover when Equifax hit by this cyberattack. One of important point is the communication and the only employee who knew of Equifax's use of Apache Struts in the online dispute portal was not included on the GTVM distribution list and did not receive news of the vulnerability. The senior manager who oversaw this lead developer and his team received the alert but failed to relay the information.

As I love to say, Security is a chain and every link in this chain is important, so don't miss anything because this is the small details that hackers exploit to occur a crucial attack.

Sources:

https://sevenpillarsinstitute.org/case-study-equifax-data-breach/

https://en.wikipedia.org/wiki/2017_Equifax_data_breach

https://www.cylumena.com/insights/stages-of-cyber-hack/

https://www.equifax.com/about-equifax/who-we-are/