Short Research Paper #1 - Equifax Breach

Brandon Zachary Pearson

Old Dominion University

CYSE-300 - INTRODUCTION TO CYBERSECURITY

Professor Malik A. Gladden

September 10, 2023

Over the years there have been numerous cybersecurity breaches amongst widely known companies. While there is a lot of money put forth to prevent cyber-attacks it is still possible even to Fortune 500 companies. With the ever-changing landscape of the internet, it can be hard for companies to stay up to date on new hacks or exploits. This is further made worse due to the fact that companies are implementing more online features to keep up with the times. The rapid development of features can cause a lack of security with each new feature. A notifiable breach happened in 2017 to the credit reporting agency Equifax.

The Equifax breach was able to be committed due to the consumer complaint web portal that Equifax had on their website. This feature was able to be exploited which allowed attackers to gain access to Equifax's internal network. Attackers made use of a known vulnerability in the Apache Struts web application framework using the complaint portal as their entrance. Once they were able to breach the network, they had free rein to access private data on customers. This was only made worse due to the lack of encryption when it came to storing user data. Which made it even easier for attackers to exfiltrate personally identifiable information about the users. This breach lasted from early May to late September and impacted over 157 million users (Equifax Data Breach Settlement, 2020).

To further the issue the vulnerability that was exploited had a patch released on March 7th by the Apache Software Foundation. The cyber team at Equifax was directed to install the patch but after running a scan they determined nothing needed to be patched (epic.org). This mistake left the portal in a vulnerable state until July 29th. The vulnerability was called "Apache Struts CVE-2017-5638". The lack of awareness to implement the patch regardless of being made aware of the vulnerability is another mistake Equifax made. If Equifax updated the system with the patch that was released then it would have prevented attackers from entering the network.

The Equifax breach went on to have lasting effects on over 157 million users. Exposing users' private data such as social security numbers, home addresses, credit card numbers, and other continental information. Leaving users' information leaked out to the rest of the internet and potentially leading to the data being exploited. This could have lasting impacts on users' lives due to the failure of Equifax to protect their information. This breach left a stain on the reputation of Equifax and cost them a significant amount of money. Having to deal with lawsuits and fines for not meeting abiding policies. While this breach exposed a massive issue when it comes to companies and data storage. It brought about discussions on data privacy and how companies should be held to a higher standard when it comes to storing data. The events that occurred brought to light just how significant it is that companies put efforts into protecting their users.

Ultimately, this breach was a net negative to all those that were impacted. Upon the reports coming out, it was evident that Equifax made critical mistakes. These mistakes could have been prevented if they had patched the breach when notified of the update. Furthermore, Equifax should have had further safeguards within its system to deter unauthorized users. This could have been through encryptions or by having a better monitoring and detecting system. The lack of due diligence by Equifax only furthered the severity of the breach.

References

Epic.org. 2020. "Testimony and Statement for the Record of Marc Rotenberg, President, EPIC." https://epic.org/privacy/data-breach/equifax/

Equifax Data Breach FAQ: What happened, who was affected, what was the impact?. CSO Online. (2020, February 12). https://www.csoonline.com/article/567833/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html

Equifax Data Breach Settlement: Am I affected?. Home | Equifax Data Breach Settlement. (n.d.). https://www.equifaxbreachsettlement.com/

Equifax. 2020. "Data Breach Settlement." https//www.equifaxbreachsettlement.com/

Erickson, S. L., Stone, M., Serdar, G., & Pfeffer, B. (2023). When Crisis Victims Are Not Customers: SCCT and the Equifax Data Breach: JMI. Journal of Managerial Issues, 35(2), 170-194. http://proxy.lib.odu.edu/login?url=https://www.proquest.com/scholarly-journals/when-crisis-victims-are-not-customers-scct/docview/2824079552/se-2

Lieber, R. (2017, September 22). Why the Equifax breach stings so bad. The New York Times. https://www.nytimes.com/2017/09/22/your-money/equifax-breach.html