Ethical Hacking and Cyber Security Report: Equifax 2017

Abstract

Equifax is one of the largest credit reporting agencies in the world, and at one point they lost over 143 million accounts to hackers after Equifax left an exploit unpatched for months. This paper will demonstrate many of the reasons why this breach occurred, how it occurred, the steps Equifax took afterwards to fix the issue and what could have been done differently to ensure that breaches of this size are far less likely to happen.

Introduction

In March of 2017, one of the largest breaches ever recorded occurred when a group of hackers managed to use an exploit to steal the data of around 143 million Equifax customer accounts. While there were no reports of identity fraud resulting from the attack, this could have been devastating for Equifax customers. Breaches of this size are very rare and should be very concerning to anyone in the security field. However, these breaches are becoming more common over time, as will be shown later in this paper.

This report will detail how the breach occurred in the first place, with a detailed timeline of events that showed each step of the breach, and the individual circumstances that resulted in the breach remaining undiscovered for weeks. The subsequent section will detail ways in which this breach could have either been prevented or discovered far earlier. Finally, this report will detail the consequences of the breach, how Equifax has compensated their customers who are affected, and the steps the company has taken to reduce the risk of a breach occurring again.

Who is Equifax?

Equifax is a consumer credit reporting agency. Their main purpose is to use customer data provided by banks and analyse it. They use the transformed data to inform banks about which customers can be trusted for loans, mortgages, and similar services. This data takes the form of a credit score, which the banks then assign to individual customers. Customers don't usually see their credit score directly; it tends to be a direct transfer between the credit reporting agency and the banks themselves. However, many credit reporting agencies allow customers to check their credit score by paying a small fee. Due to this, Equifax also holds information on credit cards and other payment methods, as customers that want to check their credit score need to pay Equifax. An estimated 200,000 accounts held by Equifax had credit card information, so when Equifax was breached, this information was stolen as well.

This all means that Equifax holds very specific data on millions of customers, more than 40% of the United States(Fruhlinger, J., 2020), and is a prime target for hackers. Equifax operates in 24 countries and employs approximately 11,000 employees (Equifax.co.uk. n.d).

Equifax, Experian and TransUnion are three of the United States largest credit reporting agencies (Investopedia. 2021). Due to this, they have the lion's share of consumer accounts, and many of those accounts are given to them by banks, rather than customers directly asking for these credit reporting agencies to handle their data.

The Breach

Apache Struts is a web framework system that handles, among other things, HTTP requests for both small- and large-scale websites. Struts is open-source and is a Java-based development framework that is employed by thousands of businesses worldwide. One such business is Equifax. Prior to the 7th of March 2017, there was an exploit found within the framework wherein attackers could include custom code in the HTTP content header of a pull request when interacting within a website. Using this custom code, attackers were able to send and execute their own code within the Struts system, resulting in an incredibly dangerous exploit. The exploit was given the name CVE-2017-5638, and was documented on multiple websites, including the Internet Storm Center (Ullrich, J., 2017.). Apache was made aware of this exploit and at once got to work on a patch, which was released on the 7th of March. This patch swiftly put a stop to any attackers utilising the exploit, if every user of Apache Struts installed the patch.

Unfortunately, whomever oversaw updating the Apache Struts system for Equifax did not do so, even though reportedly their administrators were all told to apply the patch on the 9th of March, 2 days after the patch was released. On March 15th, A scan was reportedly undertaken to find all the unpatched systems, though it appears to have failed somehow, resulting in the administrators believing that the patch was applied. In the end, many of the internal Equifax systems were left vulnerable to the exploit.

Over the next few weeks, reportedly a small group of hackers noticed that Equifax hadn't applied the patch to many of its servers and started to infiltrate the system. They first started to test the waters by making slight changes, and then started to create their own backdoors that would allow them to access the system without using the exploit in the future. This type of attack made it exceedingly difficult to trace and is one of the reasons that it took the engineers at Equifax months to fully find. The hackers started to create more backdoors, until they had fully infiltrated the system, encrypting the data that they stole on the system as they continued. Over the first few weeks, they managed to recover millions of user accounts, reportedly over 143 million, which means that this was one of the largest data breaches in history.

Of those 143 million accounts, there were over 200,000 accounts that had linked credit cards, and most breached accounts had full names, addresses, birth dates, driver's licence numbers and even social security numbers. Thankfully, of those 200,000 accounts, none reported issues of identity theft afterwards, although they were offered compensation by Equifax, which will be detailed later in the report.

Why was the breach so successful?

There were many reasons why the breach wasn't discovered for a long time. One such reason is that the attackers would encrypt and decrypt their work as they analysed Equifax's data. This aided them in the long run, as Equifax's servers encrypt and decrypt most of its traffic all the time, so engineers didn't see anything out of the ordinary for the traffic that was being analysed. However, the internal tools that re-encrypted traffic would normally use a public key certificate, which was part of another reason why the infiltration took so long to notice. Public key certificates are published by third parties and are a primary way to verify that users are who they claim to be. As Equifax didn't have a public key certificate, they didn't notice that the re-encrypted traffic didn't have the same signature as it should have, leading them to ignore most encrypted traffic.

The public key certificate reportedly wasn't renewed for at least 10 months before the breach, which is not very common for such a large company. The expired public key certificate wasn't discovered until July 29th 2017, nearly five months after the initial breach. Even after the infiltration was discovered, not much action was taken immediately, as many of Equifax's engineers were preoccupied with an investigation by the security firm Mandiant (FireEye. N.d.). Mandiant was brought in by Equifax to help seal the breach, assess the damage, and help prevent further breaches from occurring. However, there were reportedly large differences of opinion between many of the higher employees of each company, and most progress that was being undertaken to seal the breach was halted while the two companies were disputing.

Finally, on September 8th of 2017, Equifax publicised the breach. This was months after first discovering the breach, and many more months after the breach began. Throughout early August, many Equifax top executives sold large amounts of stock in the company, presumably to minimise losses when the breach was made public. Later, all but one of these top executives were cleared with charges of insider trading. It was not clear why many of the top executives had sold so much stock at the same time, but as all but one was cleared, it can be deduced that it was for reasons other than insider trading. Even if those executives were cleared, there were many more that were fired and replaced. This was very likely due to how disastrous the breach could have been, and many critics were vocal about the lack of safety mechanisms in place at the company, especially as the public key certificate was left unrenewed for so long.

What happened afterwards?

Once the breach was publicised, Equifax set up a secondary website, "equifaxsecurity2017.com" to establish a central area where potentially affected people could seek information about their accounts and check if they were affected. However, this attempt backfired when many people just assumed that the website was a phishing scam and ignored it, because the name of the website is very similar to those used by phishing scammers that attempt to trick people into releasing private data. This disaster wasn't improved by an official Equifax

social media account accidentally directing customers to the wrong website, “securityequifax2017.com”, which fortunately was caught immediately and just redirected customers to the official website.

In terms of improving its security, Equifax spent over $1.4 billion cleaning up their systems and upgrading their defences. Furthermore, by July of 2019 Equifax was required to spend a further $1.38 billion in class action lawsuits to compensate customers for the breach.

What should have been done differently?

The initial breach was caused by employees not patching the systems frequently enough to cover the exploit, and the patch that would have saved the company billions of dollars was not applied when it should have been. Keeping all systems up to date against all malicious attacks is necessary for any company, especially during the fast-paced nature of today’s world of ever-changing threats. This includes consistently checking on the public key certificate, as it went over a year without being renewed. This is not acceptable for most small businesses, never mind companies that hold such a large stake in a country’s population.

Furthermore, when the breach was discovered, they should have immediately done as much as they could to fix the issue and assess the situation, especially when so many accounts were at stake.

Conclusion

In conclusion, Equifax a a company made multiple mistakes over a period of six months that allowed over 143 million user accounts to be stolen. This could have been avoided if, firstly, Equifax had kept their systems up to date, secondly, they had renewed their public key certificates, and lastly, acted as soon as a threat was discovered. If Equifax had done this, then they would not have had to spend billions of dollars in compensation to millions of people. Furthermore, in the future, Equifax employees should ensure that they are vigilant of threats and should continue to improve as much as they can.

References

Fruhlinger, J., 2020. Equifax data breach FAQ: What happened, who was affected, what was the impact?. [online] CSO Online. Available at: <https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html> [Accessed 24 March 2021].

Equifax.co.uk. n.d. Company Profile | About Us | Equifax UK. [online] Available at: <https://www.equifax.co.uk/about-equifax/company-profile/en_gb> [Accessed 24 March 2021].

Bloomberg.com. 2017. Bloomberg - Are you a robot?. [online] Available at: <https://www.bloomberg.com/news/features/2017-09-29/the-equifax-hack-has-all-the-hallmarks-of-state-sponsored-pros> [Accessed 20 May 2021].

Ullrich, J., 2017. InfoSec Handlers Diary Blog. [online] SANS Internet Storm Center. Available at: <https://isc.sans.edu/diary/22169> [Accessed 19 May 2021].

Bates, A. and Hassan, W., 2019. Can Data Provenance Put an End to the Data Breach?. IEEE Security & Privacy, [online] 17(4), pp.88-93. Available at: <https://ieeexplore.ieee.org/document/8755956> [Accessed 21 May 2021].

Clements, M. and Marinos, N., 2018. Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach. GAO-18-559. [online] U.S Government Accountability Office. Available at: <https://www.gao.gov/products/gao-18-559> [Accessed 17 May 2021].

FireEye. n.d. Cyber Security Experts & Solution Providers | FireEye. [online] Available at: <https://www.fireeye.com/> [Accessed 21 May 2021].

Investopedia. 2021. The Top 3 Credit Bureaus. [online] Available at: <https://www.investopedia.com/personal-finance/top-three-credit-bureaus/#citation-4> [Accessed 14 May 2021].