Case Study:
Equifax Data Breach of 2017

A Comprehensive Analysis
of the Attack Category and
Impact on the Company

Attack Category: Sophisticated Cyber Intrusion Leading to Massive Data Breach

Company: Equifax Inc. and its Customers, Consumers, and Stakeholders

Prepared by: Alexander Alexandrov

in/alexander-alexandrov-463332207

Attack Category / Data Breach

The **Equifax** data breach in 2017 was a significant cybersecurity incident that exposed the personal information of approximately 147 million individuals. The attack targeted Equifax, one of the largest credit reporting agencies in the United States. The breach was a result of a combination of vulnerabilities and exploitation techniques, including a web application vulnerability in the Apache Struts framework. **Attack Vector:** Exploitation of Apache Struts vulnerability (CVE-2017-5638) through a web application

Approach of Attack: Infiltration of Equifax's network by exploiting a known vulnerability in the Apache Struts web application framework, allowing unauthorized access to sensitive data. Through this initial compromise, they were able to move laterally, escalate privileges, and gain access to a vast amount of sensitive data.

The Equifax data breach was a notable incident that highlighted the impact of successful cyberattacks on large-scale organizations and the potential risks associated with the compromise of sensitive personal information. Some relevant statistics and insights related to this type of attack and the industry include:

- According to the IBM X-Force Threat Intelligence Index 2018, the financial services sector, which includes credit reporting agencies like Equifax, experienced the highest number of attacks compared to other industries.
- The breach exposed a wide range of personal information, including names, Social Security numbers, birth dates, addresses, and in some cases, driver's license numbers. This incident highlighted the value of such information to cybercriminals and the potential consequences for affected individuals.
- The Equifax breach served as a wake-up call for organizations to reassess their cybersecurity practices and prioritize the protection of customer data. It prompted increased scrutiny and regulation in the industry, emphasizing the need for robust security measures and proactive vulnerability management.

Please note that the above information is based on general knowledge and public sources:
Equifax data breach FAQ: What happened, who was affected, what was the impact? | CSO Online

Company Description and Breach Summary

Equifax is a global data and analytics company headquartered in the United States. It collects and manages vast amounts of consumer and business data, including credit information, employment history, and personal details, which are used by financial institutions, lenders, and businesses for various purposes, such as credit assessments and identity verification.

Breach Summary: In 2017, Equifax experienced a significant data breach that resulted in the unauthorized access and theft of sensitive information belonging to approximately 147 million consumers. The breach exposed highly confidential data, including names, social security numbers, birth dates, addresses, and in some cases, driver's license numbers. Additionally, credit card numbers of around 209,000 individuals were compromised.

The breach occurred through a vulnerability in the Apache Struts web application framework, specifically the CVE-2017-5638 vulnerability. Attackers exploited this vulnerability to gain unauthorized access to Equifax's systems and establish a foothold within the network. The attackers were able to maintain a persistent presence within the network for a considerable period before the breach was discovered.

The breach not only impacted consumers whose personal information was compromised but also had far-reaching consequences for Equifax as a company. It resulted in significant reputational damage, legal and regulatory consequences, and financial losses for Equifax and the affected individuals.

Sources:
•Equifax. (n.d.). About Equifax. Retrieved from https://www.equifax.com/about-equifax/
•Equifax Inc. (2017). Equifax Announces Cybersecurity Incident Involving Consumer Information. Retrieved from https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628

Timeline

1. March 2017: The Apache Struts vulnerability (CVE-2017-5638) was publicly disclosed, highlighting the need for immediate patching.

2. May 2017: Equifax became aware of the Apache Struts vulnerability but failed to patch the affected systems promptly.

3. May to July 2017: Attackers exploited the vulnerability to gain unauthorized access to Equifax's systems.

4. July 29, 2017: Equifax discovered the data breach and initiated an investigation.

5. September 7, 2017: Equifax publicly disclosed the data breach, leading to significant public outcry and scrutiny.

Sources: Equifax Inc. (2017). Equifax Announces Cybersecurity Incident Involving Consumer Information. Retrieved from https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628

Overall Vulnerabilities Summary

The Equifax data breach exposed several vulnerabilities within the organization's security infrastructure. These vulnerabilities contributed to the successful exploitation of the system by malicious actors.

Here is an overall vulnerability summary for the Equifax breach:

Unpatched Apache Struts Framework:

The breach occurred due to a known vulnerability in the Apache Struts web application framework (CVE-2017-5638). Equifax failed to apply the necessary security patches, leaving the system susceptible to exploitation by attackers.

Inadequate Security Controls:

The breach highlighted weaknesses in Equifax's security controls and safeguards. Insufficient network segmentation, weak access controls, and inadequate monitoring and detection mechanisms allowed the attackers to navigate through the network and exfiltrate sensitive data

Slow Incident Response:

Equifax's incident response procedures were slow and ineffective in detecting and responding to the breach promptly. The attackers had access to Equifax's systems for several months before the breach was discovered, indicating a lack of proactive monitoring and

Poor Data Protection Practices:

The breach revealed shortcomings in Equifax's data protection practices. The stolen data was not adequately encrypted or protected, making it easier for the attackers to access and exploit the sensitive information.

Sources: Equifax Inc. (2017). Equifax Announces Cybersecurity Incident Involving Consumer Information. Retrieved from https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628

Costs and Prevention

•Sources:
Martinez, M. (2017). Equifax takes down web page after reports of new hack. Retrieved from https://www.cnn.com/2017/10/12/politics/equifax-hack/index.html
•King, R. (2017). What We Know and Don’t Know About the Equifax Hack So Far. Retrieved from https://www.wsj.com/articles/what-we-know-and-dont-know-about-the-equifax-hack-so-far-1505687375

Costs of the Equifax Data Breach

1. Remediation Costs: Equifax incurred expenses related to investigating the breach, mitigating the impact, and implementing security measures to prevent future incidents. This included hiring forensic experts, conducting internal investigations, and enhancing their cybersecurity infrastructure.

2. Legal and Regulatory Costs: Equifax faced numerous lawsuits and regulatory investigations following the breach. They incurred expenses related to legal defense, settlements, fines, and compliance with regulatory requirements.

3. Credit Monitoring and Identity Theft Services: Equifax offered free credit monitoring and identity theft protection services to affected individuals. The costs associated with providing these services, including credit monitoring subscriptions, added to the financial impact of the breach.

4. Reputational Damage: The breach severely impacted Equifax's reputation and customer trust. The company experienced a significant decline in its stock price and faced long-term reputational damage, which can have indirect financial implications.

While it is challenging to provide an exact monetary value for the overall costs, the Equifax breach is estimated to have cost the company hundreds of millions of dollars. The full extent of the financial impact may continue to unfold over time as legal proceedings and regulatory actions progress.

Prevention of Data Breaches

1.Patch Management: Implement a robust patch management process to ensure that software and systems are regularly updated with the latest security patches. Timely patching helps address known vulnerabilities and reduce the risk of exploitation.

2.Access Control and Authentication: Implement strong access control mechanisms, including multi-factor authentication, to restrict access to sensitive systems and data. This helps prevent unauthorized access and reduces the likelihood of attackers gaining control over critical assets.

3.Network Segmentation: Employ network segmentation techniques to isolate sensitive data and systems from the rest of the network. This helps contain potential breaches and limits the lateral movement of attackers within the network.

4.Encryption and Data Protection: Apply strong encryption mechanisms to protect sensitive data, both in transit and at rest. Encryption adds an extra layer of security and ensures that even if data is compromised, it remains unreadable and unusable to unauthorized individuals.

5.Employee Awareness and Training: Conduct regular cybersecurity awareness and training programs for employees to educate them about potential threats, social engineering tactics, and best practices for data protection. Well-informed employees are better equipped to identify and respond to potential security incidents.

Conclusions

The case study include a detailed report on the Equifax data breach, covering the breach summary, attack category, vulnerabilities, timeline, costs, prevention measures, and lessons learned. The security action plan would outline specific steps for enhancing security practices, such as improving patch management, network segmentation, security controls, and encryption measures.

The methodology would provide a framework for implementing the action plan, including governance, compliance, vulnerability management, threat management, and risk management processes based on ISO 27001.

As a result of the breach, Equifax faced intense scrutiny from regulatory bodies and implemented various measures to enhance its governance and compliance practices. The company also revised its vulnerability management, threat management, and risk management strategies to align with industry standards such as ISO 27001.