Case Study

Identity Theft

Equifax

© Copyright IBM Corp. 2023

Attack Category: Identity Theft

1. The Equifax data breach falls under the category of a large-scale cyber attack involving the theft of sensitive personal information. It is considered one of the most significant data breaches in history.

2. The breach resulted in the exposure of personal data belonging to approximately 147 million consumers.

Company Description and Breach Summary

Equifax is one of the largest credit reporting agencies in the United States, responsible for collecting and maintaining vast amounts of consumer credit information. In September 2017, Equifax announced that it had suffered a data breach, where hackers gained unauthorized access to their system, compromising sensitive consumer data.

Timeline

1. May to July 2017: Hackers exploited a vulnerability in Equifax's website application, specifically in Apache Struts, a software framework used for building web applications.
2. July 29, 2017: Equifax discovered the breach and took immediate steps to contain it.
3. September 7, 2017: Equifax publicly disclosed the data breach and revealed the extent of the stolen data, including Social Security numbers, birth dates, addresses.
4. September 8, 2017: Equifax faced severe public backlash and criticism for its handling of the breach, including delays in disclosing the incident and inadequate security practices.
5. September 15, 2017: Equifax announced the resignation of its CEO, Richard Smith, in the wake of the breach.
6. Ongoing aftermath: Equifax faced numerous legal actions, investigations, and regulatory scrutiny from government agencies due to the breach.

Vulnerabilities

The Equifax data breach was attributed to several vulnerabilities that contributed to the attackers' ability to compromise sensitive consumer data. Here is an overall summary of the four vulnerabilities:

Vulnerability 1

Unpatched Software: Equifax failed to apply necessary security patches promptly, leaving their systems vulnerable to known exploits, such as the Apache Struts vulnerability.

Vulnerability 2

Weak Security Controls: Insufficient security measures, such as inadequate access controls and weak passwords, contributed to the attackers' ability to gain unauthorized access to sensitive data.

Vulnerability 3

Lack of Network Segmentation: Insufficient network segmentation allowed the attackers to move laterally within Equifax's systems, accessing and exfiltrating sensitive data.

Vulnerability 4

Inadequate Incident Response: Equifax's incident response process was criticized for being slow, poorly coordinated, and lacking effective communication.

Costs and Prevention

Costs	Prevention
1. Expenses to investigation 2.Expenses to legal fee 3.Expenses to customer support 4.Expenses to security improvement The financial costs associated with the Equifax data breach were significant. Equifax estimated that it spent around $1.4 billion in response to the breach.	1.Regular Patch Management 2Strong Access Controls 3Network Segmentation 4.Incident Response Readiness 5.Continuous Monitoring Overall, the Equifax data breach served as a stark reminder of the importance of proactive security measures, prompt patching, and comprehensive incident response planning to protect sensitive consumer data