Case Study

Attack Category: Data Breach

Company/Affected parties: Equifax Inc.

© Copyright IBM Corp. 2023

Attack Category:
Name of category

A data breach is a grave cybersecurity incident where unauthorized individuals gain access to sensitive information, such as personal data, financial records, or intellectual property, without the consent or knowledge of the data owner or custodian. These breaches can occur through various means, including hacking, phishing attacks, or the inadvertent exposure of data due to inadequate security measures. The consequences of a data breach can be severe, encompassing financial losses, reputational damage, and potential legal liabilities. Protecting against data breaches demands vigilant cybersecurity practices, robust encryption, employee training, and constant monitoring to identify and mitigate vulnerabilities, as the ramifications of such breaches can be far-reaching and long-lasting.

Company Description and Breach Summary

Equifax is one of the three major credit reporting agencies in the United States, providing credit scores, reports, and other related services.Incident Summary:Between mid-May and July 2017, Equifax suffered a significant data breach where cybercriminals exploited a vulnerability in the Apache Struts web application framework. The breach exposed highly sensitive personal information of approximately 147 million consumers, including names, social security numbers, birth dates, addresses, and in some cases, driver's license numbers.

Timeline

1. Event 1
   Attackers exploited the Apache Struts vulnerability, gaining unauthorized access to Equifax's systems. (Date: Mid-May 2017)

2. Event 2
   Equifax discovered the unauthorized access during a security review. (Date: Late July 2017)

3. Event 3
   Equifax publicly disclosed the breach, alerting affected consumers and regulatory authorities. (Date: September 7, 2017)

4. Event 4
   Regulatory bodies and law enforcement agencies initiated investigations into the breach. (Date: September - October 2017)

5. Event 5
   Equifax CEO, Richard Smith, resigned amidst the fallout of the breach. (Date: September 26, 2017)

6. Event 6 Equifax faced numerous lawsuits, paid substantial settlements, and implemented security reforms to prevent future breaches. (Date: Ongoing)

Vulnerabilities

Apache Struts Vulnerability:

Equifax failed to patch a known vulnerability in Apache Struts despite the availability of a security patch. Attackers exploited this vulnerability to gain unauthorized

Inadequate Patch Management:

Equifax lacked an effective patch management system, leading to the failure to apply necessary security patches promptly.

Insufficient Network Segmentation:

Inadequate network segmentation allowed attackers to move laterally within Equifax's systems, accessing sensitive databases.

Weak Credential Management:

Weak or default credentials might have been exploited, allowing unauthorized access to critical systems.

Costs and Prevention

Costs	Prevention
including legal settlements, regulatory fines, providing identity theft protection and credit monitoring services to affected consumers. The company's reputation suffered, resulting in a loss of customer trust and a decline in stock value.	Regular Patch Management Employ strong network segmentation to limit lateral movement of attackers within the network. Implement advanced threat detection and monitoring systems to identify and respond to unauthorized access promptly. Response Plan: Develop and regularly update an incident response plan to handle breaches effectively if they occur.