James Soto

7-13-2023

CS-405 Secure Coding

5-1 Case Study: Triple A and Defense in Depth

**Name of case and link:**

The Equifax Data Breach

<https://en.wikipedia.org/wiki/2017_Equifax_data_breach>

**Date of case:**

The breach was discovered on July 29, 2017 but took place between May and July 2017.

**Why did this case make the news?:**

This case made the news because it was one of the largest data breaches ever recorded, impacting over 147 million people in America, over 15 million people in Britain, and around 19,000 in Canada. The breach involved sensitive information being stolen including names, social security numbers, birth dates, addresses, and driver's license numbers.

**Type of security or data breach or combination:**

This was a data breach that was a result of both network and application security vulnerabilities.

**Why was this company a target?:**

Equifax is one of the three largest consumer credit reporting agencies in the United States, held massive amounts of sensitive and personally identifiable information on millions of customers.

**Immediate threat(s):**

The immediate threat was to the consumers whose data was compromised, making them susceptible to identity theft and financial fraud.

**Potential threat(s) if the vulnerability goes unresolved:**

If not resolved, the vulnerability could have allowed for further breaches and increased exposure of sensitive information of millions of customers around the globe who use Equifax in one of the 24 countries where Equifax operates, potentially affecting the broader financial industry and damaging consumer trust.

**Which policy or policies will help prevent this type of attack?:**

The breach occurred due to a known vulnerability in the Apache Struts web application framework that wasn't patched in a timely manner. The new security patch was released on March 7, 2017, and the hackers began targeting websites that had failed to update Struts to the newest patch. Developers at Equifax could have prevented this breach by ensuring that all system components were up to date, following a thorough patch management protocol that ensured all patches were successfully updated and installed, and utilizing vulnerability scanning tools to identify and find any weaknesses.

**Authentication:**

To prevent unauthorized access to the sensitive data proper authentication methods must be put in place. To add an extra layer of protection to the system companies could add multi-factor authentication, biometric authentication, QR code scanning, OTP (one-time passwords) like Microsoft authenticator. Not only does this add another layer of protection, these methods are also user friendly.

**Authorization:**

To reduce the chances of threats or the mishandling of data, proper authorization controls ensure that only approved personnel have access to sensitive data.

**Accounting (or Auditing):**

To prevent breaches by catching the issues before they are exploited regular audits can help detect abnormalities and potential vulnerabilities.

**Defense in depth:**

This strategy involves implementing multiple layers of security controls throughout an information system. In Equifax's case, better network segmentation, web application firewalls, intrusion detection/prevention systems, and regular vulnerability scanning could have possibly prevented the breach or at least minimized its impact.