Cybersecurity: Examining Adobe's 2013 Cyberattack

Raneem Alarian

Old Dominion University

CYSE 300: Introduction to Cybersecurity

Dr. Joseph Kovacic

January 16, 2024

Cybersecurity: Examining Adobe's 2013 Cyberattack

The 2013 Adobe data breach was one of the biggest cybersecurity incidents to take place in the 21st century. On October 3, 2013, Adobe announced that they had suffered a security breach in which attackers gained unauthorized access to customer data, including login credentials and encrypted credit card information. This incident impacted nearly 38 million active users, and the stolen data included customer names, encrypted credit and debit card numbers, expiration dates, and other personal information (Patel, 2023). The attackers also stole the source code for Adobe's ColdFusion, Acrobat, and other Adobe software.

Although the exact method used by the attackers was not initially disclosed by Adobe, it is known that the 2013 Adobe attack was exploited by cybercriminals who took advantage of certain vulnerabilities in Adobe's security infrastructure. First and foremost, a glance at Adobe's past cybersecurity incidents before the 2013 attack indicates that Adobe did not have strong cybersecurity measures to begin with. In 2007, a bug allowed hackers to access files on people's computers; in 2009, a vulnerability gave hackers backdoor access to people's computers; in 2012, hackers gained access to the company's security verification system via internal servers (Kawushika, 2023).

Adobe's approach to password security made it easy for hackers to crack passwords, with one in six passwords found to be easily cracked due to the use of hashing (Dubey, 2014). The inadequacy of Adobe's password security, which failed to meet industry requirements, allowed hackers to exploit these weaknesses. It is also believed that the shift from offering desktop licenses to providing software-as-a-service (SaaS) on the cloud exposed Adobe to vulnerabilities that were later exploited by the attackers (Kawushika, 2023). According to Adobe's Chief Security Officer Brad Arkin, the company, in its transition to a service delivery model, faced

challenges in integrating product engineering and IT security. Weaknesses in the system infrastructure and security systems were identified as contributing factors to the breach. The process of transitioning from desktop licenses to SaaS failed to adequately address and resolve major vulnerabilities in the infrastructure (Bell, 2018).

The 2013 Adobe incident had several repercussions. The attack resulted in a substantial blow to Adobe's reputation which caused the company to face criticism for failing to properly protect customer data, as well as losing trust among users and the public (Patel, 2023). Adobe also faced legal challenges: lawsuits were filed against the company for the compromise of sensitive customer information. Furthermore, the stolen source code posed a substantial threat to the company's products and users. The hackers could analyze the stolen source code to find and exploit vulnerabilities or to create false versions of Adobe's products to harm devices or data (Patel, 2023).

Overall, several cybersecurity measures could have been taken to mitigate the consequences or prevent the incident. For starters, Adobe could have implemented better password protection measures and secure hashing methods. The company could have also regularly performed security assessments and penetration testing to scan for system vulnerabilities. Although they have started implementing this now, Adobe could have implemented two-factor authentication and enhanced encryption techniques used to store passwords (Oropesa, 2023).

References:

Bell, T. (2018). Adobe's CSO talks security, the 2013 breach, and how he sets priorities. *CSO Online*. https://www.csoonline.com/article/565054/adobe-s-cso-talks-security-the-2013-breach-and-how-he-sets-priorities.html

Dubey, G. (2014). Adobe security breach. *Slideshare*. https://www.slideshare.net/GauravFouzdar/adobe-security-breach-30650671

Kawushika, B. (2023). Adobe cyberattack 2013 case study. *LinkedIn.* https://www.linkedin.com/pulse/adobe-cyberattack-2013-case-study-bulitha-kawushika-hlrxc/

Oropesa, X.S. (2023). Case study about Adobe breach. *Scribd.* https://www.scribd.com/document/652388915/Case-Study-about-Adobe-Breach

Patel, M. (2023). The Adobe attack of 2013: A cautionary tale of cybersecurity failure. *Medium.* https://medium.com/@maazptl240602/the-adobe-attack-of-2013-a-cautionary-tale-of-cybersecurity-failure-1ef4ec74eb64#:~:text=In%202013%2C%20Adobe%20suffered%20a,network%20and%20steal%20valuable%20data