23andMe Data Breach

Identify a Recent Cybersecurity Incident or Data Breach:

Overview of the Company

23andMe is a personal genomics and biotechnology company. that provides DNA kits, health reports, and research. The mission of the company is to help people understand and benefit from their DNA. The variety of services the company offered was genetic health reports, research, and therapeutics which uses data from its research to develop new treatments for patients with serious illnesses.

Overview of the Incident

On October 1, 2023, 23andMe disclosed a data breach that affected approximately 7 million customers. The threat actor initially targeted a relatively small number of accounts but since 23andMe's uses an interconnected data-sharing system, it allowed the attacker to access a broader user base. The data that was compromised contained users' ancestry information and some health-related details. The data breach resulted specifically from a credential stuffing attack where the threat actor used lists of previously compromised user credentials from other compromised websites to gain access to 23andMe systems. This type of attack often exploits sites that lack two-factor authentication (2FA).

Impact of the Breach

Following the breach, several class action lawsuits were filed against 23andMe alleging negligence and privacy law violations. 23andMe ended up losing the lawsuit and agreed to a $30 million settlement to compensate affected users, with the potential for individuals to receive up to $10,000 depending on the severity of their claims.

Analyze the Incident Using the IDPRR Cycle:

Identify: After 23andMe became aware of the incident and the method in which the attack was launched, the company required all new and existing customers to reset their passwords and to implement a two-step verification login method.

Protect: 23andMe employed standard password-based authentication with encryption protocols, and other access controls. The standard password-based authentication was not effective as the threat actor used credential stuffing to gain access to the system without much difficulty.

Detect: Although 23andMe has not explicitly stated whether they used a SIEM solution, they must have used it given the sensitive nature of their genetic data. It wasn't effective since a job of SIEM is to collect authentication logs which would have shown the sharp increase in login attempts which could have alerted security personnel to further investigate.

Respond: When 23andMe became aware of the incident, they immediately began working with third-party security experts to investigate the incident and contacted federal law enforcement. 9 days after the incident was detected, they immediately required all their customers to reset their password and informed their customers that they paused certain functionality within the platform as they continued the investigation. The company was also working to remove customer information from sites the threat actor reposted the stolen information.

Recover: The company made changes to their password policy by requiring all new and existing customers to login using two-step verification.

Discuss the Role of NIST RMF or CSF:

NIST CSF could have been utilized to prevent this incident as it would have enabled 23andMe to proactively identify and mitigate cybersecurity risks rather than reacting to the incident. Additionally, if the company had performed vulnerability scans more regularly it would have recognized problematic use of single factor authentication to protect very sensitive data. The company could have opted to use 2FA or even better, MFA, since it ended up implementing this after the incident occurred. Lastly, implementing a password policy that informed its customers to craft a strong and unique password or require passwords to be changed regularly could have helped with the credential stuffing attack. There are no lessons learned from the incident that align with NIST's best practices as even requiring 2FA is below the best practice of using MFA.

References

California Attorney General. (n.d.). *California data breach notification letters*. Retrieved from https://oag.ca.gov/system/files/CA%20AG%20-%20CA%20Notification%20Letters.pdf

Kindelan, K. (2023, October 10). *What to know about 23andMe's recent data security breach*. ABC News. Retrieved from https://abcnews.go.com/GMA/Wellness/23andme-dna-data-security/story?id=115818849

Risk Strategies. (2023, October 17). *Understanding the 23andMe data breach and ensuring cybersecurity*. Retrieved from https://www.risk-strategies.com/blog/understanding-the-23andme-data-breach-and-ensuring-cybersecurity