Incidence Response Playbook

Overview of 23andMe Data Breach

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).

Incident Response Playbook

Incident Detection and Analysis:

1. Preparation
    a. **Team Structure:**
        i. **IR Manager**: oversees the entire incident response to unauthorized access into the company's systems.
        ii. **Technical Lead**: Performs in-depth technical analysis of the incident, identifies root cause, and recommends remediation steps.
        iii. **IT Security Analysts**: Analyze logs, such as the authentication logs that led to the breach.
        iv. **Recovery Specialist**: Develops and implements recovery plans to restore affected systems and data to operational status.
        v. **Legal Counsel:** Provides legal advice and guidance regarding data privacy, incident reporting, and liaises with law enforcement.
        vi. **Public Relations Team**: Responsible for communicating with customers about the situation and updates regarding the incident.
    b. **Communication Plan**:
        i. Establish clear channels of communication for reporting suspected authorized access.
        ii. Develop out-of-band communication systems in case primary communication tools have been compromised.
    c. **Tools and Resources:**
        i. Access to authentication logs captured by SIEM tool.
        ii. Forensic tools for network analysis.
        iii. Secure communication platforms.
2. Identification
    a. **Incident Detection and Analysis:**
        i. The breach would be detected from an automated SIEM alert notifying IT Security Analyst of login attempts made from unauthorized location in addition to repetitive failed attempts.

ii. Data Loss Prevention (DLP) system detects and alerts on suspicious data transfers.

b. **Initial Assessment:**
    i. Confirm whether the alerts are in fact, malicious activity.
    ii. Assess the scope and method of the unauthorized access (credential stuffing attack, brute-force attack, malware injection, etc.).
c. **Notification:**
    i. Immediately notify the IR Manager and initiate the IR protocol.

3. Containment
    a. **Immediate Actions:**
        i. Contact the IT Security Analyst to lock the accounts of the persons who have made attempts to log into 23andMe web server.
        ii. Communicate to Team Lead to isolate compromised systems to prevent further data exfiltration processes.
4. Eradication
    a. **Investigation:**
        i. Determine how the unauthorized access was perpetrated (e.g., phishing, account hijacking, etc.).
    b. **Eradication actions:**
        i. Contact Technical Lead to revoke permissions granted to the compromised user account.
5. Recovery
    a. **System and Process Restoration:**
        i. IR Manager communicates to IT security Analyst to assess the user permissions with the database management system to see if the user account no longer has access privileges.
        ii. After unauthorized access has been revoked, IR Manager requests and receival approval from CISO to implement MFA for all users to prevent future intrusions.
    b. After eradication efforts have been taken, the PR team contacts regulatory bodies and customers to inform them of the breach.
    c. PR team crafts an email/letter communicating to stakeholders the need for all existing and new users to utilize MFA.
6. Lessons Learned
    a. **Post-Incident Review:**
        i. Schedule meeting with all members of the IRT including the CISO and relevant stakeholders to debrief: Discuss what was done effectively and identify areas for improvement.
        ii. The Technical Lead analyze the incident to identify failures in authentication security measures.
        iii. IR Manager documents the incident, response effectiveness, and areas for improvement. Updates IR playbook to incorporate lessons learned and other security policies.
        iv. IR requests to CISO to create Authentication policy requiring all users to utilize MFA.
7. Integrate Continuous Monitoring

a. Tools such as SIEM and EDR will be beneficial in our response plan as it would have alerted the IT security analyst/team of suspicious authentication behavior to subsequently lock the account. These would also be helpful with detecting any further suspicious behaviors during the containment effort to ensure there is no lateral movement. Additionally, these tools are helpful This tool would be helpful in having a centralized resource for handling access management when alerts have been sent to the system.

References

- Cellcrypt. (2023). Secure out-of-band communications in cybersecurity incident response. Retrieved from https://www.cellcrypt.com/post/secure-out-of-band-communications-in-cybersecurity-incident-response
- Fortinet. (n.d.). Data exfiltration. Retrieved from https://www.fortinet.com/resources/cyberglossary/data-exfiltration
- Wiz.io. (n.d.). Incident response team. Retrieved from https://www.wiz.io/academy/incident-response-team