Bryce Jensen
CS-405-10914
5-1 Case Study: Triple-A and Defense in Depth
10-2-24

Introduction

- Name of case and link: LinkedIn Data Breach
- Date of case: June 22, 2021
- Why did this case make the news?
    - The LinkedIn data breach made the news because it exposed data from 700 million users, which, at the time, was over 92% of LinkedIn's user base. The breach involved sensitive information such as email addresses, phone numbers, and even geolocation data. This, understandably, raised concerns about user privacy and data security.

Describe the breach

- Type of security or data breach or combination
    - The breach involved the unauthorized access of LinkedIn's user data using the LinkedIn API. The compromised data included email addresses, full names, phone numbers, physical addresses, geolocation records, LinkedIn usernames, profile URLs, salaries, and other personal and professional information
- Why was this company a target?
    - LinkedIn was targeted because it has an extensive database of valuable professional and personal information. As a leading professional networking platform, criminals highly seek after their data. They can use this for identity theft, phishing, and other malicious activities.

Identify the threat(s)

- Immediate threat(s): The immediate threats were unauthorized access to personal information, identity theft, and targeted phishing attacks using the exposed data.
- Potential threat(s) if the vulnerability goes unresolved: ongoing identity theft, other exploitation of personal data, and potential financial fraud using the user's personal information.

What could a developer have done to prevent this breach?

- Which policy or policies will help prevent this type of attack?
    - Developers could have done several things, including, more strict API access, rate limiting (where there is a controlled number of requests allowed within a specific time frame), and more monitoring to detect and prevent unauthorized API use.

Summarize the case by explaining the role of best practices, Triple-A, and defense in depth in preventing future attacks.

- Authentication: Implementing MFA (multi-factor authentication) would add an extra layer of security to a user's data even if a bad actor did get access to user credentials.
- Authorization: Ensuring access controls are set correctly and regularly checked can prevent unauthorized access to sensitive data and systems.
- Accounting: Maintaining detailed logs of user activities and reviewing these logs can help detect suspicious activity.
- Defense in depth: Using a multi-layered security approach such as using firewalls, intrusion detection, and regular security updates, can provide holistic protection against all kinds of cyber threats.