**Module Five – LinkedIn (2021) Case Study**

**Justin Hancock**

**CS-405 Secure Coding**

**09.30.2024**

* **Introduction**
  + LinkedIn Data Breach
  + June 2021
  + This breach made headlines because it exposed data from around 760 million LinkedIn users, representing over 92% of its total user base. Although sensitive financial data wasn’t included, the sheer size of the breach and potential misuse of personal information sparked significant concerns.
* **Describe the breach**
  + Hackers exploited LinkedIn’s security to scrape user data which included names, email addresses, phone numbers, and other personal details. Data scraping is a type of data breach where publicly accessible data is collected on a massive scale. Although this was not a direct hacking event, the massive amount of personal data exposed made it a serious incident.
  + LinkedIn is a popular professional networking platform. This made it a prime target for attackers seeking valuable data for social engineering, phishing, and identity theft.
* **Identify the threat(s)**
  + Immediate threats are the misuse of personal information for phishing scams or identity theft.
  + Potential threats, if left unresolved, is that the leaked data could be used for long-term social engineering attacks or even sold on the dark web markets.
* **What could a developer have done to prevent this breach?**
  + Developers could have implemented stricter rate-limiting mechanisms, used CAPTCHA challenges, and monitored for unusual data scraping activity to prevent such a large-scale scraping incident.
  + Implementing data privacy policies that enforce stronger security measures on publicly accessible data and regularly reviewing security configurations would help prevent this type of attack.
* **Summarize the case by explaining the role of best practices, Triple A and defense in depth in preventing future attacks.**
  + Best practices like Authentication, Authorization, and Accounting along with a defense-in-depth strategy are crucial to preventing these breaches.
  + Authentication involves verifying the user’s identity.
  + Authorization controls access to resources.
  + Accounting tracks the user’s activities.
  + Defense in depth means layering security measures, so even if one fails, others are in place to protect sensitive data.

**Citations**

Leyden, M. H. D. S. a. J. (2024, September 12). *The 18 biggest data breaches of the 21st century*. CSO Online. <https://www.csoonline.com/article/534628/the-biggest-data-breaches-of-the-21st-century.html>

*Reported LinkedIn data breach: 700 million users data exposed - Cybersecurity - Nixon Peabody Blog | Nixon Peabody LLP*. (2021, June 30). Nixon Peabody LLP. <https://www.nixonpeabody.com/insights/articles/2021/06/30/reported-linkedin-data-breach-700-million-users-data-exposed>