5-1 Case Study

* Introduction
  + Name of case and link
    - Yahoo Data Breach
    - https://lifelock.norton.com/learn/data-breaches/company-data-breach
  + Date of case
    - September 2016
  + Why did this case make the news?
    - At least 500 million users accounts were exposed.
* Describe the breach
  + Type of security or data breach or combination
    - Cookie-Based attack where users could be authenticated without a password.
  + Why was this company a target?
    - A Canadian hacker who was associated with a Russian FSB spy did it to access personal messages.
* Identify the threat(s)
  + Immediate threat(s)
    - The way that the hackers were able to get into the data was by a mistaken click. That is all it took for someone to access 1.5 billion accounts and data.
  + Potential threat(s) if the vulnerability goes unresolved
    - Without the fix, Yahoo could have been completely compromised and this type of issue could have fully condemned Yahoo. If there was a smaller threat, it could’ve potentially gone unnoticed, but one this size was impossible to miss.
* What could a developer have done to prevent this breach?
  + Which policy or policies will help prevent this type of attack?
    - I believe that better testing could’ve been done to prevent this data breach. IF all it took was a simple click from the hackers, I believe there wasn’t sufficient testing to ensure that Yahoo’s software was safe.
* Summarize the case by explaining the role of best practices, Triple A and defense in depth in preventing future attacks.
  + Authentication
    - Authentication is extremely important, but in this case, the authentication that was put in place wasn’t enough. I believe that the use of two factor authentication could have really helped.
  + Authorization
    - Authorizing the user wasn’t done. The hacker was able to skip that step of the login process and access a multitude of accounts.
  + Accounting
    - Using a cyber security software accounting tool will minimize issues like this in the future.
  + Defense in Depth (DiD)
    - Using the DiD system will allow the software to have multiple tools in place to pre

Sources

*Yahoo announces 500 million users impacted by Data Breach*. LifeLock Official Site. (n.d.). Retrieved March 29, 2023, from https://lifelock.norton.com/learn/data-breaches/company-data-breach#

* + - vent security breaches in the future.