SNHU CS-405 Case Study

Tanner Holbrook

Southern New Hampshire University

* Introduction
  + This data breach happened in 2019 and made the news due to the sheer scale of the exposed sensitive data, including account names, user IDS, and even comments stored on an unprotected Amazon S3 server. However, the exposed data happened with third-party apps integrated with Facebook at the time.
  + This data breach occurred because third-party apps stored sensitive customer data on an unsecured Amazon S3 server, which was vulnerable to attacks. Furthermore, the information was not properly secured, leading to unauthorized access to the sensitive user information.
* Describe the breach
  + The type of security was a data breach exposing sensitive personal information.
  + Facebook was a prime target because it contained a huge amount of unsecured personal data, making it a prime target for cybercriminals.
* Identify the threat(s)
  + The threat was unauthorized access, use, and exposure of personal data.
  + The immediate threats involved the potential for the exposed information to be used for identity theft, phishing, and scams in the form of a ransom.
  + If the vulnerability went unresolved and was never corrected, there was a severe risk of continual unauthorized access to the data and the potential for the data to be misused.
* What could a developer have done to prevent this breach?
  + The developers could have prevented this reach by ensuring the proper implementation of best practices regarding security. For instance, authentication, authorization, encryption of data at rest, proper access controls, and ensuring the buckets were correctly secured.
  + The policies that would have prevented this attack include data protection, encryption, and any other procedure for secure storage and handling of the data.
* Summarize the case by explaining the role of best practices, Triple A and defense in depth in preventing future attacks.
  + This breach shows the need for robust security practices, especially regarding the secure protection of data and limiting data access. Developers must prioritize implementing stringent authentication controls and ensure only authorized and authenticated users can access personal data. In addition, developers will enforce access controls for any application interacting with the data, hopefully minimizing access to sensitive information. Also, regular audits will be performed on any stored data to catch any unauthorized use or unusual activity. Furthermore, implementing multiple security layers like encryption and access controls while conducting routine audits will help embody the role of defense in depth. In conclusion, this case study aimed to show the importance of strict and adequate security measures to minimize or eliminate potential attacks from cybercriminals.

**References**

Kovacs, E. (2019, April 4). *AWS S3 buckets exposed millions of Facebook records*. SecurityWeek. https://www.securityweek.com/aws-s3-buckets-exposed-millions-facebook-records/