Abuse of access to user information by employees of social media / digital service companies

Reference: Memo [190604-1] Date: 04/06/2019 - Version: 1.0
Keywords: social media, cloud, Snapchat, Facebook, Twitter, Instagram, LinkedIn, G Suite, access abuse, personal data
Sources: publicly available information

Key Points

- Snapchat personnel abused their level of access to user data some years ago.
- Corporate Gmail accounts had their passwords stored in plain text.
- These are the most recent cases of social media platforms exposing user data to insider's abuse.

Summary

On May 29, ex-employees of the social media company Snap (parent organisation of the Snapchat platform) revealed that in several instances administrators abused their privileges to access user information. The events have taken place in previous years, without the report specifying exactly when.

Specifically, company administrators have used an internal tool called SnapLion, normally used for fulfilling law enforcement requests for information. According to the report, several groups of company operators had access permissions to this tool that provides a complete image of user data. Although such tools, due to their potential for abuse, are supposed to log their usage, it is almost certain that their logging capability was less than optimal, something that the company claims to have remedied in recent years.

In a similar incident, on May 22, Google revealed that for corporate Gmail accounts (G Suite enterprise accounts) it was keeping passwords in plain text. The norm for secure password storage is to encode them using a non-reversible hash function to a standard length string. The hash string, even if leaked cannot be reversed to reveal the original password, although a simple enough password can be discovered by brute-force trials of potential passwords until the hash function produces the same string. If however the password is of sufficient length (and a so-called "salt" is used to increase the complexity) the brute-force method becomes prohibitive due to the time and computing resources it requires. In the case of Google G suite, the accounts concerned should normally be protected from external leakage, however they would still be at risk from malicious insiders. The event constitutes a serious oversight that should have been remedied by security policies. According to the company, the problem goes back to 2005, although there are no indications of the passwords being stolen or abused.

Comments

Users might not be aware of the potential for misuse of their personal data by social media employees. Indeed, individuals inside these companies may be prone to misuse of their work-related privileges even if the organisation itself adheres to relevant rules and regulations.

Some very recent cases highlighting the risks to personal data due to mishandling by social media platforms include:

- May 22: public reports indicated that contact data, as well as other pieces of personal data, in the form of a database originating from the social media platform *Instagram*, were leaked online. Contrary to the *Snapchat* case, the information appeared to be nominally collected ("scrapped") but contained important private details. The scale of the disclosure (containing, according to the scrapping company about 350 000 entries, but highly likely more than 49 million records) and the fact that it was referring to the most important individuals in the *Instagram* platform ("influencers" and celebrities) has made this a major privacy intrusion event.
- May 15: *Twitter* confirmed that it had been collecting user location information (via its iOS app) and sharing it with a third party.
- April 18: *Facebook* admitted uploading 'unintentionally' the email contacts of 1,5 million of its users since May 2016. The news prompted a legal investigation by the New York state authorities on April 25.
- April 3: security researchers reported they had found 540 Million *Facebook* user records on unprotected *Amazon* S3 buckets. The data had been collected and stored (improperly) by third-party Facebook app developers, to whom the company had provided access.
- March 21: the security researcher Brian Krebs reported that hundreds of millions of *Facebook* users had their account passwords stored in plain text and searchable by thousands of *Facebook* employees since at least 2012.
- January 30: a criminal actor offer for sale information of 159 million *LinkedIn* clients. As proof of his access to these records, he released the personal information of 100 individuals, including that of some big-company CEOs.

Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.