Security failure at Facebook—what we know

October 3 2018

The Facebook breach affecting some 50 million users and disclosed late last month is now under investigation by Ireland's data protection authority

The security breach revealed on September 28 by Facebook affected tens of millions of accounts at the social network, which boasts more than 2.2 billion monthly users.

On Wednesday, the Irish data authority said it was opening up a formal investigation into whether the world's biggest social network complied with tough new EU privacy regulations.

- What happened?

Hackers took advantage of a "complex interaction" between three software bugs, which required a degree of sophistication.

The vulnerability was created by a change to a video uploading feature in July of 2017.

It involved a flaw in a "See As" feature that showed Facebook what their profiles look like to other people at the social network.

Using the feature generated digital keys, called "access tokens," which let users stay connected to their accounts without having to enter passwords anew.

Hackers were able to steal copies of the digital keys, giving them the same access and control of accounts as their legitimate owners.

On September 16, Facebook noticed a spike in activity that prompted it to investigate.

On September 25, Facebook engineers determined hackers had launched a sophisticated attack exploiting the vulnerability. A fix was in place two days later and stolen tokens rendered useless.

Facebook did not disclose when hackers first took advantage of the flaw, saying the investigation was early.

- What data was leaked?

Information hackers appeared interested in included names, genders, and home towns, but it was not clear for what purposes, the executives said in a telephone briefing.

Facebook said it was still trying to figure out what, if anything, hackers did in violated accounts. It did not seem at the outset that messages or posts were tampered with, and there was no access to banking or password information, according to the social network.

Given that digital keys opened Facebook doors wide to hackers, they would have had the ability to reach into third party applications linked to social network accounts.

They would have been able to get into linked accounts including Messenger or Instagram, both owned by Facebook, but not into the social network's WhatsApp service.

An analysis of logs of third-party applications turned up no sign they were meddled with by the hackers, Facebook said on October 2.

- Who should worry?

Facebook said that "up to 50 million accounts" were directly affected, meaning hackers swiped digital keys.

According to the Data Protection Commission in Ireland, five million or fewer European users were among those affected.

An additional 40 million accounts that used the "View As" feature had tokens reset although it didn't appear they were targeted by hackers.

- Measures taken by Facebook?

Facebook said it sealed the breach late on September 27 in California, where it has its headquarters, and alerted US law enforcement authorities as well as regulators in Ireland.

Facebook invalidated "access tokens" at issue in the breach, requiring people to log in anew with passwords. The social network informed those involved by posting messages atop news feeds.

- What is the risk to Facebook?

The risks for Facebook depend on how it complied with various laws and regulations, including the new General Data Protection Regulation in Europe.

Questions likely to be asked will include whether Facebook was fast enough notifying users of the breach and how well it protected accounts.

Protection of people's data falls under the purview of the Federal Trade Commission in the United States, but states could also be interested in making sure local privacy or data protection laws were not violated.

In Europe, the Facebook breach and how it was handled would be examined through the lens of the GDPR, which strengthened protection for personal data.

Companies can now be fined a percentage of annual revenue if they break GDPR rules. Facebook appeared to have complied with a 72-hour deadline regarding publicly disclosing a hack, which could spare it a fine of more than a billion dollars.

from https://phys.org/news/2018-10-failure-facebookwhat.html