Bonn/Berlin, March 21, 2019

Press release 13/2019

Facebook again reveals significant data protection deficits

The current scandal proves that Facebook still neglects the issue of data protection. Precisely because the Facebook access data can also be used for many other services as an authentication option, users of the social network should definitely change their passwords.

For Ulrich Kelber, the Federal Commissioner for Data Protection and Freedom of Information, the renewed scandal caused a shake of the head: It is sad, but a data protection incident on Facebook is unfortunately no longer a big surprise. What is scandalous, however, is that one of the world's largest IT companies obviously does not know how customer passwords have to be saved. Facebook is thus exposing its customers to an unnecessary risk. It's a bit like when passengers in a taxi can't buckle up because the driver doesn't know how a seat belt works.

Since companies only have to check whether the access ID and password match during the registration process, it is state of the art to regularly store passwords only in encrypted form, for example as a hash value. In a similar case, the state data protection officer in Baden-Württemberg fined a German company a few months ago for this reason.

The BfDI is therefore certain that the present case will also be meticulously investigated by the data protection supervisory authorities: On the one hand, it must be clarified whether Facebook has violated the reporting regulations under the General Data Protection Regulation. The problem seems to have been known since January. Irrespective of this, the Irish data protection officer responsible in Europe will certainly examine the initiation of fine proceedings. Finally, we will also discuss the case in the European Data Protection Board.

Facebook announced today that the passwords of hundreds of millions of customers had been stored unencrypted on internal servers for years and were therefore accessible to more than 20,000 employees. The case is particularly critical because this data can be used not only for access to the social network itself, but also as a so-called single sign-on. Many other apps or online services make it possible to log in to them using the Facebook access data. The data potentially also grants access to other data that may be very sensitive, for example from health apps. Facebook users should therefore urgently change their password. Tips for secure passwords can be found, for example, on the website of the Federal Office for Information Security.

Update from 03/22/2019, 1:15 p.m.:

After the publication of the press release, we learned that Facebook is storing customer passwords in encrypted form in its password database. Instead, the passwords in question were apparently stored in plain text in log files. The Federal Commissioner for Data Protection and Freedom of Information, Ulrich Kelber, explains: The new findings do not change the basic assessment of the incident. If anything, it makes the whole thing worse, since passwords—whether encrypted or plain text—generally have no place in log files.

contact finder

Here you can find out in just a few clicks who is responsible for your inquiry or complaint about data protection.

public bodies

The term public body not only includes the traditional administrative authorities, but also courts, parliaments and public foundations. This also includes social insurance, such as health insurance.

company

Private companies are mostly supervised by state authorities, but there are some exceptions. Private organizations such as clubs and associations also fall into this category.

Press, radio, church

Special responsibilities apply in these areas. Churches and public broadcasters have e.g. B. via their own data protection officers. The federal and state supervisory authorities are not responsible for other organizations either.