TV2's assessment of the risk for those registered in credential stuffing attacks was incorrect

Date: 18-12-2020

Decision

Private companies

Serious criticism

Reported breach of personal data security

Treatment safety

Hacking and others

Risk assessment and impact analysis

On the basis of TV2's erroneous assessment of the risk to the data subjects during the processing and the lack of implemented security measures, the Danish Data Protection Authority expressed serious criticism that TV2 did not comply with the rules on processing security

Journal number: 2018-441-0645

Summary

The Danish Data Protection Authority has made a decision in a case where TV2 had reported a number of breaches of personal data security to the Danish Data Protection Authority.

TV2 had been exposed to high-frequency hacker attacks of the "credential stuffing" type aimed at registered customers' accounts.

Credential stuffing is a form of attack where login information, typically consisting of leaked lists of usernames and passwords, is used to gain access to e.g. personal data, through extensive automated login requests with an internet service. In other words, the hackers thus test whether usernames and the associated passwords on the lists also provide access to the Internet service in question.

High-frequency hacker attacks mean that the attack takes place from one IP address, as opposed to low-frequency attacks, where the attacks are spread over several IP addresses with few login attempts per user. address spread over a longer period of time, which makes it more difficult to detect the attack.

Before the attack, TV2 did not want to introduce security measures that made it too difficult for customers to log in.

It was TV2's view that the purpose of the attacks is typically to get passwords for TV2 PLAY user profiles verified, so that streaming access can subsequently be sold illegally, which is why the most serious consequence for users, according to TV2, was that the user profiles could be misused by others and that the user would have to change password.

However, it was the Danish Data Protection Authority's assessment that there are more – far more serious – consequences associated with credential stuffing attacks than those TV2 had identified. Eg. can a list of verified combinations of usernames and passwords be used with other services where there is access to significantly more personal data, including payment information. It is very common for users to use the same passwords for several services.

It was therefore the Danish Data Protection Authority's opinion that TV2's assessment of the threat and its likelihood was incorrect.

Based on the identified risks, a data controller must ensure an appropriate level of security and implement necessary technical and organizational measures.

The Norwegian Data Protection Authority found that TV2 had not implemented such necessary measures to ensure an adequate level of security.

The Danish Data Protection Authority emphasized in particular that TV2 should already have implemented automatic blocking of IP addresses before the breach on 7 September 2018 in case of many failed login attempts that came from one or a few IP addresses.

The Danish Data Protection Authority also emphasized that the manual monitoring was not sufficiently effective.

On the basis of TV2's erroneous assessment of the risk to the data subjects during the processing and the lack of implemented security measures, the Data Protection Authority expressed serious criticism that TV2 did not live up to the rules on processing security.

1. Decision

After a review of the case, the Danish Data Protection Authority finds that there are grounds for expressing serious criticism that TV2's processing of personal data has not taken place in accordance with the rules in Article 32 of the Data Protection Regulation[1].

Below follows a closer review of the case and a rationale for the Data Protection Authority's decision.

2. Case presentation

In the period from 10 September 2018 to 8 December 2018, the Norwegian Data Protection Authority has received a number of notifications of breaches of personal data security from TV2, where TV2 has been exposed to high-frequency hacker attacks of the type "credential stuffing" aimed at registered customers' accounts.

2.1. TV2's remarks

TV2 has stated that in the reports in question, a very large number of repeated login attempts were made on TV2's user profiles from one IP address. It was established that a large number of successful logins had been made to TV2's user profiles. It also appears from the reports that there were a large number of rejected login attempts from the same IP address in the same period.

Those affected by the attack have been notified of the attacks via e-mail.

TV2 has stated that to log in to a user profile you must use a username, which is typically an e-mail address and a password. When you are logged into a user profile, the following personal data will be available:

email address

first name

year of birth

sex

username (e.g. a pseudonym)

last name

mobile number

Zip code

streaming history

Furthermore, TV2 has stated that the many login attempts and successful logins indicate a so-called "credential stuffing" attack. A credential stuffing attack is a form of attack where login information, typically consisting of lists of usernames and/or e-mail addresses and the corresponding passwords, is used to gain unauthorized access to user profiles, through extensive automated login requests at an internet service. The lists with login information basically contain login information from other services. The lists usually originate from previous breaches of personal data security at other services.

TV2 has stated that before the first attack on 7 September 2018, credential stuffing was not part of the usual threat picture for

TV2 Play. This depends, among other things, on together with the fact that, due to the language, the content of TV2 Play is really only interesting for a Danish audience. However, since the breach on September 7, 2018, there has been a sharply increasing number of attempts at credential stuffing, which is a trend that has been felt throughout the industry.

It is TV2's opinion that the purpose of the credential stuffing attempts that have been directed at TV 2 PLAY has only been to identify which usernames and passwords from the list used could give access to TV 2 PLAY, so that the streaming access could be resold illegally.

TV2 has assessed that the consequence for the data subject of a compromise is almost negligible. Many customers will probably not discover it if there is an unauthorized person using their account, just as a compromise will not entail any costs for the data subject.

In relation to which security measures can be implemented, TV2 has also stated that it is limited how elaborate security measures can be associated with login. If the security measures are too complicated or are experienced as disturbing for the use of a – in this case – relatively simple service, customers refrain from using the service. TV2 therefore carries out an ongoing assessment of, on the one hand, which personal data the service provides access to and the resulting risks, and on the other hand, the importance that various security measures will have for user-friendliness.

TV2's security level before the breach on 7 September 2018 was measured in relation to the assessment of the risk associated with a credential stuffing attempt. The following relevant security measures had been implemented before the breach:

[excluded from publication]

Regarding the system's handling of login attempts, TV2 has stated that:

[excluded from publication].

TV2 had the option and had tried to implement automatic blocking of login activity already before 7 September 2018. However, it turned out to be operationally problematic and almost ineffective, since the attacker simply changed the IP address in that case.

Regarding the manual monitoring, TV2 has described in detail that real-time monitoring of the login activities had been established. This means that TV2's employees kept an eye on specific operating parameters. The employees were notified of irregularities by an alarm or a warning email. Specifically regarding credential stuffing [excluded from publication].

In addition, periodic reviews of the activity log were carried out, which meant that the log was analyzed when abnormal activity

had been recorded. This analysis work could only be carried out backwards, which is why the purpose of this i.a. was to ensure notification of affected users.

TV2 has also stated that workshops have been held, among other things, with a view to uncovering which protection measures could be established in front of the login system.

Finally, TV2 has stated that in the period after 7 September 2018, TV2 has implemented new measures and that these measures have been adapted from incident to incident. The credential stuffing attempts are being developed all the time and the norm is now that the attacks consist of attempts distributed over many thousands of IP addresses with very few login attempts per address spread over many hours - so-called low-frequency hacker attacks. It means [excluded from publication].

3. Reason for the Data Protection Authority's decision

3.1. Of the data protection regulation, article 32, subsection 1, it appears that the data controller must implement technical and organizational measures that suit the risks of varying probability and seriousness to the rights of the data subjects.

The data controller thus has a duty to identify the risks that the data controller's processing poses to the data subjects and to ensure that appropriate security measures are introduced to protect the data subjects against these risks.

3.2. The Danish Data Protection Authority is of the opinion that TV2 had not sufficiently identified the risks, the likelihood thereof and the consequences for the data subjects.

When assessing risks, it must be done on the basis of an overall assessment of the consequence of and the probability of a threat being realised.

TV2 has stated that the purpose of the credential stuffing attacks is typically to get passwords for TV2 user profiles verified, which can then be sold illegally, which is why the most serious consequence for users is that their user profiles are misused by others and that the user has to change their password.

However, it is the Danish Data Protection Authority's assessment that there are more - far more serious - consequences associated with credential stuffing attacks than those identified by TV2, as the attacks are not only carried out with a view to being able to resell streaming access.

It is very common for users to use the same passwords for several services. A credential stuffing attack is therefore a way of verifying the combination of an e-mail address or other username and a password, after which a list of verified combinations will be worth significantly more and could be used with other services, where there is access to significantly more personal

data , including payment information, and where the resale of access may be more attractive.

The fact that users themselves should be aware of the risk of using a password for several services cannot lead to a data controller not having to implement appropriate security measures that prevent the closest possibilities of having such a verification made. The responsibility for security and that adequate security is ensured rests with the data controller and cannot be transferred to the data subjects.

In addition, the Danish Data Protection Authority finds that there are significantly more serious consequences for those registered with the verification of the combination of an e-mail address and a password. In part, it gives the attacker the opportunity to try blackmailing a large number of users. Since it is a leaked email address, an email can be sent directly to the user, and since the attacker can provide a password that the user uses, the user will be more likely to believe what is written in the email the email. This may result in the user allowing themselves to be blackmailed for larger or smaller sums of money. In addition, verification of the access criteria provides a more credible platform for phishing and other types of attacks that aim to give the attacker access to other accounts, resources or assets.

It is therefore the Danish Data Protection Authority's opinion that there are serious consequences associated with loss of confidentiality – and thus with credential stuffing attacks – regarding the information that TV2 processes, and that the form of the attack creates the possibility of potential loss of rights for the data subjects, which lie beyond the concrete abuse of their access to the services TV2 provides.

The Danish Data Protection Authority is of the opinion that TV2's assessment of the threat and its likelihood was incorrect. TV2 has stated that credential stuffing attacks were not part of the usual threat landscape for TV2 prior to September 7, 2018. However, credential stuffing was known among streaming services prior to September 7, 2018[2]. TV2 should thus have been aware of the phenomenon and have included this in the assessment of risks and which technical and organizational measures were necessary to ensure an appropriate level of security.

3.3. Based on the identified risks, a data controller must ensure an appropriate level of security and implement necessary technical and organizational measures.

The Norwegian Data Protection Authority finds that TV2 had not implemented such necessary measures to ensure an appropriate level of security.

The Danish Data Protection Authority has particularly emphasized that TV2 should already have implemented automatic

blocking of IP addresses before the breach on 7 September 2018 in the event of many failed login attempts originating from one or a few IP addresses.

TV2 has stated that they had tried to implement automatic blocking, but that this turned out to be operationally problematic, and that it was almost ineffective, as the attacker changed the IP address in that case.

In this connection, the Danish Data Protection Authority must note that the fact that an attacker – after meeting resistance with a security measure – finds other methods cannot justify that the security measure is not implemented. If the security measure can have an effect against just one type of attack, this should be implemented, regardless of whether it does not also work against other types of attacks that the attacker resorts to after encountering the security measure.

The Danish Data Protection Authority has also emphasized that the manual monitoring was not sufficiently effective.

TV2 has stated that manual monitoring was carried out by keeping an eye on the proportion of rejected login attempts that exceed the normal level on screens etc. and that an alarm or warning email notified of irregularities. However, the Danish Data Protection Authority is of the opinion that the manual monitoring should have led to the detection of the attack at an earlier stage so that it could have been stopped.

The Danish Data Protection Authority is of the opinion that the provision on adequate security means that data controllers, especially when offering services aimed at public use and with many registered users, must protect themselves against the most obvious misuse scenarios, including those used in credential stuffing. Many access attempts against several accounts from one or a few IP addresses, from IP addresses that geographically fall outside normal usage scenarios and access attempts that are not supported by a subsequent normal usage pattern must all give rise to a reaction,

If an organizational measure is chosen on the basis of set threshold values, this must be just as effective in repelling the attacks in question as a technical solution, also in terms of time.

3.4. Based on both TV2's erroneous assessment of the risk to the data subjects during the processing and the lack of implemented security measures, the Danish Data Protection Authority finds reason to issue serious criticism that TV2 did not meet the requirement to implement appropriate security measures according to Article 32 of the Data Protection Regulation.

The Danish Data Protection Authority has noted that TV2 has subsequently implemented new measures and is thus trying to meet the real threat to the rights of the data subjects that credential stuffing poses.

The Danish Data Protection Authority has also noted that TV2 has continuously informed the affected users via e-mail and

encouraged them to change their password, just as TV2 has blocked user profiles that have not changed their password. The Danish Data Protection Authority notes in this connection that regardless of whether the data controller is obliged to notify the data subject as a result of a high risk, cf. the data protection regulation's article 34, it is appropriate in the event of abuse to inform the affected data subjects when there has been a breach of personal data security . However, the supervision must make sure that the information provided to the data subjects actually describes the rights threats that exist, not just the data controller's business risk.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons in connection with the processing of personal data and on the free exchange of such data and on the repeal of Directive 95/46/EC (general regulation on data protection).

[2] See appendix 1 to Bruun & Hjejle's statement on behalf of TV2 of 21 June 2019