Breach of personal data security at Dantherm

Date: 13-10-2021

Decision

The Danish Data Protection Agency has criticized the fact that Dantherm did not have adequate security. Nor could the company demonstrate that the treatment had complied with the rules.

Journal number: 2020-441-6990

Summary

The Danish Data Protection Agency has made a decision in a case where Dantherm had reported a breach of personal data security to the Authority.

Dantherm had been subjected to a ransomware attack, in which hackers managed to gain access to Dantherm's IT environment, from which the hackers leaked information about current and former employees to the dark web.

The hackers probably gained access via the user "AV" who had administrator rights. The user account had previously been used by an external consultant who should not have access at the time of the attack. The hackers deleted most of the logs. Dantherm could therefore not answer whether the account "AV" had been active or deactivated.

The Danish Data Protection Agency stated that administrative rights must only provide access to relevant limited resources (computers, active devices, programs, services or the like), and logging of all use of the rights must be ensured. The log files must therefore be stored in such a way that users with the administrative rights can not shut down, delete or change the log.

The Danish Data Protection Agency found that Dantherm's processing of personal data had not been in accordance with the rules on appropriate security.

In the assessment, the Danish Data Protection Agency emphasized that Dantherm had not ensured that users with administrator rights could not delete or change the log files.

In addition, the Danish Data Protection Agency found that Dantherm had not complied with the requirement that the data controller must be able to demonstrate appropriate security in the processing of personal data. In this connection, the Danish Data Protection Agency emphasized that Dantherm could not document the periods during which the “AV” account was active.

Against this background, the Danish Data Protection Agency found grounds to criticize the fact that Dantherm's processing of personal data had not taken place in accordance with the data protection rules.

The case contained so-called cross-border processing of personal data, as employees in i.a. Germany, Poland and England were also affected by the breach. The Danish Data Protection Agency has therefore made a decision as the leading supervisory authority according to the "one-stop-shop mechanism".

Decision

After a review of the case, the Danish Data Protection Agency finds that there are grounds for expressing criticism that Dantherm's processing of personal data has not taken place in accordance with the rules in Article 32 (1) of the Data Protection Regulation [1]. 1 and Article 24, para. Article 32 (1) 1.

Below is a more detailed review of the case and a justification for the Danish Data Protection Agency's decision.

2. Case presentation

On 25 September 2020, Dantherm reported a breach of personal data security to the Danish Data Protection Agency.

It appears from the notification that on the evening of 26 August 2020, Dantherm observed abnormal behavior on a backup server. Further investigation showed that on 21 August 2020 there had been malicious activity on the network. The activities had reportedly primarily concerned an investigation of network structure and destruction of running backup. The technical investigations carried out by the IT security company Dubex A / S (hereinafter Dubex) did not give rise to any suspicion of a breach of personal data security at that time.

It further appears from the notification that the network connection was disconnected and the malicious activity was thus stopped. In collaboration with the hosting partners and Dubex, the network was opened in a sound manner, and further investigation of the hackers' behavior on the network was initiated.

In this connection, it was on 22 September 2020 at. 21.00 found that personal data from Dantherm had been filtered out, which had been posted online on a third-party hosting site. The data was confirmed removed on September 23, 2020 at. 14.45.

In addition, the notification states that the personal data concerned concerned:

bank information in the form of account information for use in salary payment of approx. 100-450 employees in Germany, Poland and England,

Religious matters solely for the purpose of tax considerations of approx. 50 employees in Germany,

Health information including in Denmark minutes of 87 health interviews and in Poland and England information of relevance to the employment relationship,

and social security numbers of approx. 1,525 citizens in Denmark.

On 15 June 2021, DAHL Advokatpartnerselskab issued a statement in the case on behalf of Dantherm. DAHL Advokatpartnerselskab has i.a. stated that based on the activity that could be ascertained, it was concluded by Dantherm in collaboration with Dubex that a ransomware attack had been launched against Dantherm, where hackers had managed to gain access to parts of the IT environment, but where the attack has not yet was effected. At this point, the hacker and ransomware attack was averted.

The initial investigations showed no indication that there was a breach of personal data security, including that data had been definitively deleted, that data had been copied or distributed from Dantherm's IT environment, or that there was unauthorized access to personal data. This was only subsequently ascertained.

The further investigations led to the discovery on 22 September 2020 that personal data from Dantherm's IT environment had been filtered out in the form of a single data file, and that this data had been accessible from a server via a reference in a forum on the dark web. The file contained information about current and former employees.

On September 23, 2020 at At 14.45 it was confirmed that the file had been removed online from the server where it was found. The investigations conducted by Dubex indicated that the file was transmitted directly from Dantherm's IT environment to the hosting site in question. DAHL Advokatpartnerselskab has stated in this connection that it has not been possible to investigate who - if anyone - may have acquired the data while they have been online.

DAHL Advokatpartnerselskab has stated that Dantherm had implemented a large number of security systems and that these were activated until the hackers partially deactivated some of them in connection with the attack. It further appears from the statement from DAHL Advokatpartnerselskab that Dantherm continuously rolls out updates on servers in various rings via SCCM. There are various reasons why, in practice, updates to the latest versions of operating systems are not always updated as soon as they are released. This is not generally considered to be in conflict with best practice in the field, including that updates are not necessarily of a security nature.

DAHL Advokatpartnerselskab has also stated that data has not been deleted by Dantherm and that Dantherm has not been denied access to data. The hackers have also not made any demands to refrain from publishing the data.

It appears from the case that the data subjects concerned have been notified by letter sent on 29 and 30 September 2020.

It appears from Dubex's report with conclusions about the cause of the breach that it was especially one of the [servers] that

stood out, as this had many services exposed to the Internet, including Microsoft Remote Deskop (RDP). From this server it was subsequently possible to access other systems in the entire network to all internal systems. The attackers then turned off antivirus / malware, disabling event logging on all machines involved in the attack to avoid being detected.

In addition, the report from Dubex states that the attackers managed to log in to [the server] via the AD user account "AV", which had previously been used by an external consultant in the spring of 2020 from an external company that had assisted Dantherm. Dubex has stated that "AV" was no longer with the external consulting company, and there was therefore no reason for this account to log in to some of Dantherm's systems. The account was a member of the domain administrator group and therefore had full access to all machines in the AD. According to Dubex, the attackers may have gained access to the account by guessing the password.

DAHL Advokatpartnerselskab subsequently claimed on 20 July 2021 that Dubex stated to Dantherm in connection with the reporting of the hacker attack that the first account with administrator rights that the hackers gained access to was probably the user "AV".

According to what was reported to Dantherm, it could not be demonstrated that the user "AV" had ever been logged on to [the server]. In this connection, DAHL Advokatpartnerselskab has stated that the conclusions are an indication of what is most likely to be found, and not an indication of what can be definitively used as established fact.

Furthermore, DAHL Advokatpartnerselskab has stated that Dantherm's IT manager finds it just as likely that the hackers gained access to another domain administrator rights account as the first, and only subsequently used the account "AV", possibly because the hackers thought it was a service account to Dantherm's antivirus system.

Finally, DAHL Advokatpartnerselskab has stated that no real answer can be given as to why the user account "AV" could still be used to log in to Dantherm's systems, as the hackers deleted most of the log files in the IT environment. The only thing that can be stated is that the user account "AV" was not deleted. Whether the account was active or disabled cannot be determined by Dantherm.

Dantherm's normal procedure is that external consultants only have access to the company's IT systems during the period when the individual consultant has a real need for this. When the individual consultant no longer has a specific need for access to Dantherm's IT systems, the account is either deactivated or expired after a given date, and then deleted. When there is a presumption that a consultant, after completing a specific task, must perform tasks for Dantherm again at a later date, which

requires access to the company's IT systems, Dantherm typically does not delete the consultant's account, but sets the account "disabled". During this status, the consultant can not use the account to log in and access Dantherm's IT systems.
In this connection, Dantherm's IT manager has stated that it is the presumption that this normal procedure has also been complied with in relation to the account "AV", and that there are no indications that this should be the case. As the relevant logs were deleted by the hackers during the attack, Dantherm does not have the opportunity to provide documentation of the conditions around when the account "AV" has been active and during which periods the account has been deactivated. DAHL Advokatpartnerselskab has stated in this connection that it can therefore not be concluded that the account was active at the time of the hacker attack.
In 2020, when the hacker attack took place, Dantherm's IT department consisted of four employees with administrator rights. All four employees sat in the same physical office. Guidelines were therefore set and administered verbally in plenary among these staff. Since the hacker attack, more employees have been added, and the current procedures are therefore also written down.
Justification for the Danish Data Protection Agency's decision
Based on the information in the case, the Danish Data Protection Agency assumes that Dantherm has been subjected to a hacker attack, which resulted in files containing information about employees being published on the dark web.
On this basis, the Danish Data Protection Agency assumes that there has been unauthorized access to personal data, which is why the Authority finds that there has been a breach of personal data security, cf. Article 4, no. 12 of the Data Protection Regulation.
It follows from Article 24 (1) of the Data Protection Regulation 1, that a data controller must implement appropriate technical and organizational measures to ensure and to be able to demonstrate that the processing is in accordance with the Regulation.
Article 32 (1) of the Data Protection Regulation Paragraph 1 states that the data controller must take appropriate technical and organizational measures to ensure a level of security appropriate to the risks involved in the data controller's processing of personal data.
Thus, the data controller 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 put in place to protect the data subjects against these risks.

In the opinion of the Danish Data Protection Agency, the requirement for adequate security means that in system landscapes where access to confidential personal data or special categories of personal data can be created across different resources in the domain structure, there must normally be a restriction on administrative privileges. It will therefore normally be an expression of appropriate security that the administrator's right is granted only to the relevant limited resources and for a limited period of time.

This could be done by not using broad administrative privileges and accesses, and by not granting these permanently, but only by elevating the rights ad hoc.

Allocation of administrator rights should be organized in such a way that only relevant resources are accessed and in all cases mechanical registration (logging) of all uses of the rights is carried out. The log files must also be stored in such a way that users with the administrative rights cannot delete or change them.

Based on the above, the Danish Data Protection Agency finds that Dantherm - by not ensuring that users with administrator rights could not delete or change the logs - has not taken appropriate technical measures to ensure a level of security that suits the risks involved in Dantherm's processing of personal data. , in accordance with Article 32 (2) of the Data Protection Regulation. 1.

The Danish Data Protection Agency also finds that Dantherm - by not being able to demonstrate in which periods the "AV" account was active, or by - in other ways - has been able to create clarity about how the breach of personal data security could occur - has not complied with the requirement that the data controller must be able to demonstrate appropriate security in the processing of personal data, in accordance with Article 24 (1) of the Data Protection Regulation. Article 32 (1) 1.

The Danish Data Protection Agency has emphasized that Dantherm has not sufficiently secured the necessary documentation that in the specific case could shed light on whether the regulation was complied with.

After an examination of the case, the Danish Data Protection Agency finds that, overall, there is a basis for expressing criticism that Dantherm's processing of personal data has not taken place in accordance with the rules in Article 32 (1) of the Data Protection Regulation. 1 and Article 24, para. Article 32 (1) 1.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (General data protection regulation).