Lack of security around a development server

Date: 13-02-2020

Decision

Private companies

The Danish Data Protection Agency criticizes the fact that KMD had not implemented appropriate security measures in connection with the takeover of a development and test environment from another supplier.

Journal number: 2019-431-0036

Summary

In a specific case, the Danish Data Protection Agency has expressed criticism that a data processor in connection with the takeover of a development and test environment from another supplier (before the regulation applied) had not implemented appropriate security measures.

When the data processor acquired the IT solution (in connection with a company acquisition), it was not observed to what extent a test and development server contained information about natural persons. The server was for development tasks connected to networks outside the data processor's control (the Internet) and it was several years after the takeover compromised and used illegally to "extract" the cryptocurrency Bitcoin. Due to the original classification - as an internal development server, without personal data - was not subject to the data processor's ordinary operational security setup (patch and security policy).

When the improper use was found, it was simultaneously determined that the server - nevertheless - contained personally identifiable information from several data controllers.

The Danish Data Protection Agency found that the breach could have been avoided if ordinary technical security measures had been introduced (including firewall rules) and that the established security measures could therefore not be considered appropriate. The reason for this was primarily that the risk assessment was based solely on the original description of the server as an “internal server” (without personal data).

General information about test environments and production data

In general, the Danish Data Protection Agency must emphasize that the necessary attention is also paid in connection with development and testing if information about natural persons is processed. Several cases have been found where developers

either on their own, in collaboration with the business or as an agreed part of the development use production data to ensure the quality of the solution. There is nothing - necessarily - wrong with this, as long as there is an assessment of the risk to the data subjects' rights, and in accordance with this, appropriate security has been established before the processing begins, and that in all cases where the risk of the registered may be high, an impact assessment has been carried out.

Slightly squarely said, if you want to use production data, there must in principle be the same security on your development and test environment as what is considered appropriate in the operational setup.

Decision

The Danish Data Protection Agency hereby returns to the case where KMD A / S (hereinafter "KMD") in April 2019 experienced a breach of personal data security in that a server - on which personal data was stored - was compromised.

Decision

Following an examination of the case, the Danish Data Protection Agency finds that there are grounds for expressing criticism that KMD's processing of personal data has not taken place in accordance with the rules in Article 32 of the Data Protection Regulation [1].

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

2. Case presentation

It appears from the case that the server, which was compromised on 10 April 2019, was acquired through the company Avaleo, which KMD entered into a purchase agreement for in 2015 and which merged with KMD in 2017.

KMD has informed the Danish Data Protection Agency that in connection with the merger with Avaleo, there were several servers that were to be subject to KMD's responsibility, and in this process, investigation and securing of servers that had no direct significance for production and did not contain production data was discontinued. to later or considered superfluous. Therefore, the compromised server was not investigated further on April 10, 2019, and the security of the server was also not arranged according to the fact that the server contained personal information.

It appears from the case as presented by KMD that the compromised server contained a backup copy of data from a prioritization tool in which development tasks are recorded and prioritized. This backup contained error descriptions as part of the description of development tasks. After compromising the server was detected, a review of part of the backup was made. It was concluded that the copy contained social security numbers, often without further information, but it could also be with

name and possibly indication of substance abuse problems. The backup also contained login information for SMDB - a central database to which abuse treatments are reported.

From some of the affected data controllers, the Danish Data Protection Agency has received information indicating that other types of access may also be potentially affected, including access to information about the data controller's name, social security number, etc. or access to the Nexus system. The latter was a test user password, which, however, has not been used in 2019.

It appears from the case that it can not be ruled out that there was unauthorized access to the backup, which contained the personal information and login information, but it is KMD's assessment that it was not likely, due to the circumstances of the attack on the server.

It appears from the report on the course of events that it has been necessary for KMD to carry out a manual review of data, including content in free text fields, in order to determine which data controllers and which data subjects were affected. The fact that some data controllers were only informed of the breach a few weeks after it took place is justified, among other things, by the extent of data that had to be reviewed manually (a closer review of approximately 3,000 out of approximately 65,000 cases).

As part of handling the breach, KMD has deleted old registrations that were affected by the breach. KMD could therefore not state exactly how old the data was in relation to a specific municipality (data controller), but KMD could not deny that information dates from 2011 and 2012. Due to the deletion, KMD could not state with certainty what types of personal data were affected, where this specific municipality was data responsible for the processing.

68 data controllers - primarily municipalities - are affected by the breach.

The server is described as an "internal server" that was established for the development of the Avaleo solution, and KMD became aware of the breach, due to a sharp deterioration in the server's performance, which was due to the termination of a program for 'Bitcoin mining'.

Measures implemented by KMD on the basis of the breach included deletion of older data, restriction of access by the server can only be accessed from KMD's IP addresses, deactivation of the software that was used to gain unauthorized access, and relocation of login information (usernames and passwords) for a dedicated key management system.

In addition, measures have been implemented to minimize the processing of personal data on the server in the future.

Justification for the Danish Data Protection Agency's decision

The Danish Data Protection Agency assumes that KMD is the data processor in the processing of personal data that is affected by the breach.

When the data controller must report breaches to the Danish Data Protection Agency, the notification must, if possible, describe the categories of personal data that are affected, cf. Article 33 (1) of the Data Protection Regulation. 3, letter a. In a specific case, which was further investigated by the Danish Data Protection Agency, this does not seem to be possible, due to KMD's deletion of the information. Although the deletion may have been a sensible step in dealing with the breach, the data controller must also ensure that he can provide the information to the data controller enabling the latter to comply with Article 33. This should be possible without retaining the fatal personal data. , which was affected by the breach.

KMD has explained why some data controllers were only informed of the breach, a few weeks after it had happened. The Danish Data Protection Agency does not find reason to override KMD's explanation.

The Danish Data Protection Agency finds that KMD has violated Article 32 of the Data Protection Regulation by processing personal data as a data processor without having implemented appropriate technical and organizational measures to safeguard against the illegal processing of personal data.

The Danish Data Protection Agency has hereby emphasized that:

KMD acknowledges insufficient security for the processing that was affected by the breach of personal data security.

In describing the purpose of the server and the measures introduced in the light of the breach of personal data security, the case appears that KMD could have avoided this breach, by ordinary technical security measures that would not have prevented the intended use of the server.

[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).