Serious criticism of Sports Connection for lack of treatment safety

Date: 04-07-2022

Decision

Private companies

Serious criticism

Reported breach of personal data security

Notification of breach of personal data security

Password

Treatment safety

Hacking and others

Unauthorized access

The Danish Data Protection Authority expresses serious criticism of Sports Connection for not having implemented appropriate security measures in connection with a hacker attack in which unauthorized persons collected customers' payment information.

Journal number: 2021-441-10210

Summary

The Danish Data Protection Authority has made a decision in a case where Sports Connection ApS has reported a breach of personal data security.

Sports Connection was the victim of a hacker attack where unauthorized persons injected malicious program code into Sports Connection's webshop to collect their customers' payment information.

Prior to the incident, the company had not security patched the e-commerce software to the latest version.

On this basis, the Danish Data Protection Authority found grounds for issuing serious criticism of Sports Connection.

1. Decision

After a review of the case, the Danish Data Protection Authority finds that there are grounds for expressing serious criticism that Sports Connection ApS' processing of personal data has not taken place in accordance with the rules in the data protection regulation[1] article 32, subsection 1 and article 24, subsection 1, cf. article 32, subsection 1.

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

2. Case presentation

On 28 September 2021, the Danish Data Protection Authority received a notification from Sports Connection ApS that there had been unauthorized access to Sports Connection ApS' webshop, which had resulted in a breach of personal data security, whereby customers' payment information had been accessed. Sports Connection ApS became aware of the unauthorized access when the company discovered that a field had been added to the shopping cart on the webshop that had not previously been there.

It appears from the case that Sports Connection ApS' webshop is based on the Magento e-commerce program. On 26 September 2021, via a security hole in Magento, a malicious program code was injected that made it possible to upload a file to the webshop, which meant that the webshop's check-out page could be manipulated. The actual access from the outside lasted 17 seconds, when the external file was uploaded to the company's webshop.

It also appears from the case that the webshop was immediately shut down at the time the incident was discovered, after which Sports Connection ApS discovered the security flaw and closed it down. The company then determined the extent of the incident and contacted the affected customers the same day.

Sports Connection ApS has stated in connection with the processing of the case that Magento version 1.9.3.8 was discontinued on the website at the time of the breach. The company has stated that Magento could have been updated to a newer version, but that the newer version did not include additional security updates that could have prevented the attack.

It also appears from the case that the attack took place via a module in Magento, which was hacked. This happened via the separate module called "slider-filemanager", which works independently of Magento, with its own login. Sports Connection ApS were not aware of the separate module, including that the module could be accessed by outsiders.

Sports Connection ApS has informed the case that unauthorized persons gained access by learning about the login to the slider functionality in "Slider_filemanager", which made it possible to upload a file to the check-out page where credit card information could be entered. The unauthorized access to the module lasted for 17 seconds during which customers' credit card information was accessed. The security hole was subsequently closed and the module in question was removed from Magento.

Sports Connection ApS has finally stated that the company changed development partners in the first quarter of 2021. The company has stated in this connection that it has not been possible to obtain a log file of updates to Magento, as the log file

has either been deleted or as a result of that has been updated without the log file in a previous development collaboration.

3. Reason for the Data Protection Authority's decision

Based on the information provided by Sports Connection ApS, the Danish Data Protection Authority assumes that the company – at the time the webshop was hacked – was running Magento version 1.9.3.8. and that at this time a newer patched version 1.9.3.9 had been released. In addition, the Danish Data Protection Authority assumes that this patch – in the patch history – states to remove general vulnerabilities in the product.

3.1. Article 32 of the Data Protection Regulation

Article 32, subsection of the Data Protection Regulation. 1, states that the data controller, taking into account the current technical level, the implementation costs and the nature, scope, context and purpose of the processing in question as well as the risks of varying probability and seriousness to the rights and freedoms of natural persons, implements appropriate technical and organizational measures in order to ensure a level of security appropriate to these risks.

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.

In Article 32, subsection 1, as examples of security measures are specifically mentioned the ability to ensure ongoing confidentiality, integrity and robustness of processing systems and a procedure for regular testing, assessment and evaluation of the effectiveness of the technical and organizational measures to ensure processing security.

The Danish Data Protection Authority is of the opinion that the requirement cf. Article 32 for adequate security will normally imply that the data controller has a duty to ensure that the personal data processed by the data controller does not come to the knowledge of unauthorized parties. In the Data Protection Authority's view, this means, among other things, that the data controller must ensure that customers, when using the data controller's webshop, do not inadvertently pass on information to unauthorized parties, e.g. by ensuring that customers are not forwarded to a payment page where the customer's payment information is intercepted by unauthorized persons. The Danish Data Protection Authority generally believes that webshops and payment solutions that are made available via open accessible websites must have procedures and checks that ensure that administrative user accounts are kept separate from individual user accounts, that these must generally be secured by using multi-factor authentication. In addition, as far as possible, different usernames and keywords must be used for the modules and parts of the solution. It is a known risk scenario that the frequently used e-commerce platforms and their add-on

products are attempted to be compromised by built-in weaknesses, it is therefore essential that patches are made as soon as the supplier releases a security patch, both those that correct specific threats, but also those that simply state to fix general vulnerabilities.

In this connection, the Danish Data Protection Authority is of the opinion that the data controller, as part of the development and adaptation of IT solutions for the processing of personal data, must ensure that IT systems are continuously updated and checked with a view to identifying conditions that may lead to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data.

Based on the above, the Danish Data Protection Authority finds that Sports Connection ApS - by not having updated the e-commerce program Magento to the latest version at the time of the attack - has not taken appropriate organizational and technical measures to ensure a level of security that is suitable for the risks that is in the company's processing of personal data, cf. the data protection regulation, article 32, subsection 1.

3.2. Article 24 of the Data Protection Regulation

Sports Connection ApS has stated that it has not been possible to obtain a log file of patches for the e-commerce program Magento, as the log file has either been deleted, or as a result of the log file being updated in a previous development collaboration.

It follows from the data protection regulation article 24, subsection 1, that the data controller, taking into account the nature, scope, context and purpose of the processing in question as well as the risks of varying probability and seriousness to the rights and freedoms of natural persons, must implement appropriate technical and organizational measures to ensure and to be able to to demonstrate that processing is in accordance with this regulation.

Based on this, the Danish Data Protection Authority finds that Sports Connection ApS has generally not been able to demonstrate compliance with the regulation by not being able to document when the system has been patched, as it has not been possible to obtain a log file of ongoing updates in Magento. By not being able to do this, Sports Connection ApS has not met the requirement that the data controller must be able to demonstrate adequate security when processing personal data, cf. the data protection regulation, article 24, subsection 1, cf. Article 32, subsection 1.

3.3. Summary

Based on the above, the Danish Data Protection Authority finds that there are grounds for expressing serious criticism that

Sports Connection ApS's processing of personal data has not taken place in accordance with the rules in the data protection regulation, article 32, subsection 1 and article 24, subsection 1, cf. article 32, subsection 1.

When choosing a response, the Norwegian Data Protection Authority emphasized that it is a known risk scenario that frequently used e-commerce platforms are attempted to be compromised through built-in weaknesses. In addition, the Danish Data Protection Authority has emphasized that the customers' payment information is involved.

The Danish Data Protection Authority has also emphasized that Sports Connection ApS has not secured the necessary documentation, and thus has not been able to document that the Magento e-commerce program has been regularly updated sufficiently for security.

[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).