MOROĞLU ARSEVEN

The Personal Data Protection Board Issued a Decision Regarding the Data Breach Notification made by Yemek Sepeti

15 Apr 2022

Following the data breach notification made by Yemek Sepeti that the web servers were accessed, the Personal Data Protection Authority ruled the second highest administrative fine it had ever imposed.

- The following statements are included in the data breach notification submitted to the Personal Data Protection Auhority ("**Authority**") by the data controller, Yemek Sepeti Elektronik ?leti?im Perakende G?da Lojistik A.?. ("**Yemeksepeti**");
    - A web application server belonging to the data controller was accessed by an unidentified person/persons on 18 March 2021,
    - Under normal circumstances, there is a problem record on the vehicle that gives a warning when there is an unauthorized access, but due to a malfunction, the unauthorized access could not be noticed at that moment,
    - When the alarms received on 25 March 2021 are examined, it is determined that there is a suspicious behavior,
    - In the examination made on the same date, the application was installed by taking advantage of the vulnerability on a web application server belonging to Yemeksepeti and the server was accessed by running a command,
    - It has also been determined that the violator(s) tried to collect data through different tools by creating a user on the server they accessed and that they sent traffic to remote servers,
    - 21,504,083 Yemeksepeti users were affected by the violation,The attackers transmit the data to an IP address/server in France and this transmitted traffic has traces on the firewall,
    - The personal data affected by the breach are user name, address, phone number, e-mail address, user password and IP information.
- As a result of examining the data breach notification within the framework of the Authority's authority and duty; It has been determined that the server was accessed by installing an application and running a command due to a vulnerability on a web application server belonging to the data controller, and 21,504,083 users were affected by the breach.
- Considering that the affected personal data are user name, address, phone number, e-mail address, password and IP information and the number of people affected by the breach is very large and almost the entire customer database is leaked, it is stated that the breach is very large. Considering the extent of the breach, the size of the leaked data and the nature of the leaked personal data as a result of the investigation, it was added that the breach would pose significant risks such as loss of control over the personal data for the persons concerned.
- According to the Data Protection Board's ("**Board**") decision, the person or persons who entered the system, after logging into the system with malicious software and tools, other systems were accessed and information was collected, and the installation and operation of malicious software on the system could not be noticed by the data controller for 8 days. Therefore, the data controller was found to be defective in checking which software and services are running in the information networks and in determining whether there is a leak or an action that should not be in the information networks.
- It is stated that alarms have occurred in security software since 8 March 2021, and that these alarms were turned off without notifying the Yemek Sepeti Security Teams of the products monitored by third party companies and without taking the necessary actions. Considering this, it has been decided that this situation

is an indication that there is no effective control mechanism on the third-party companies that the data controller receives service from and that there are deficiencies in the follow-up of security software and the use of security procedures.

- Considering that the attackers transmit the data obtained from the data controller to an IP address/server location in France, 28.2 GB of data coming out of the system/outgoing traffic cannot be noticed by the data controller and this data traffic has traces on the firewall; Although there are traces on the firewall, the fact that such data leaks cannot be noticed shows that security controls and data security monitoring are not done properly by the data controller.
- Considering that it was stated that the server with the vulnerability was a server that passed the penetration test, this situation shows that the penetration tests were not / were not carried out effectively by the data controller, and the fact that the data controller who processes large amounts of personal data experienced such a breach and was late in the intervention does not determine the existing risks and threats well. Considering the points that it is indicative of, the Board has decided to impose an administrative fine of 1,900,000 TL, taking into account the fault and economic situation of the data controller regarding the data controller who does not take the necessary technical and administrative measures to ensure data security within the framework of paragraph (1) of article 12 of Personal Data Protection Law numbered 6698, the extent of the violation, and the unfairness of the offense.

You can access the full text of the decision summary via this link. (Only available in Turkish)

Related Practices

- Privacy and Data Protection

Related Attorneys

- BURCU TUZCU ERS?N, LL.M.
- CEYLAN NEC?PO?LU, Ph.D, LL.M.