Path: Home page > Main menu > Supervisory and decision-making activity Checking the security of personal data when operating an online game (natural person doing business)

Based on the notification of a breach of personal data security and a complaint, the Office carried out an inspection, the subject of which was mainly the security of personal data processed in connection with the operation of an online game. The inspected person was the operator of this online game. The inspectors discovered that DDoS attacks were carried out against the game servers. The first attacks were successful and knocked the servers out of service. The game operator has therefore taken measures to improve security, but other attacks have also been successful. The attacker then offered the operator to stop the attacks and help secure the servers after paying a certain amount. The operator agreed and paid the required amount. The attacker therefore provided him with a firewall, which the operator uploaded to the source code of his game server after verification. The source code modified in this way was more resistant to DDoS attacks, but the operator did not reveal the so-called backdoor into the system, specifically the script that was hidden in the image file. Using this script, the attacker was able to obtain the player database of the online game in question. The attacker then published the database and redirected the game website to his website. The subject database consisted of more than four and a half thousand accounts and was available on the Internet for about one and a half hours. The database mainly contained the following types of personal data: username, password in encrypted form, phone number, e-mail address, IP address and information listed in the database for payments (current payment status, number of purchased virtual currency, name of the account from which the payment was made , time and method of payment).The operator immediately interrupted the operation of the game and database server and subsequently reported the matter to the Office, reported it to the affected data subjects and filed a criminal complaint. Following the above, the inspectors came to the conclusion that the inspected person did not ensure the resilience of the system and services by , that it adopted a protective solution (firewall) from the originator of DDoS attacks, in which a so-called backdoor was incorporated, through which the attacker got to the player database. This database was subsequently published on the Internet. The controlled person thus did not take sufficient technical and organizational measures to secure the personal data of its users. The inspectors also found that the inspected person used two processors of personal data, namely a hosting provider in the form of a cloud storage and a project technician, without concluding the relevant processing contract with them in the sense of Article 28, paragraph 3 of Regulation (EU) 2016/679. The Office found that the inspected person violated the obligations set out in Article 5 paragraph 1 letter f) (integrity and confidentiality), Article 5 paragraph 2 (principle of responsibility), Article 28 paragraph 3 (processing contract) and Article 32 (security of personal data) of Regulation (EU) 2016/679. Given that, that the inspected person does not currently operate the online game in question, the Office did not impose measures to eliminate the identified deficiencies. For this action, the Office imposed a fine of CZK 25,000 on the inspected person. The inspection was conducted by inspector Ing. Josef Vacula. Recommendation: In the event that your computer system or program becomes the subject of an attack, report the matter to the Police of the Czech Republic and, in the event that personal data is affected, evaluate whether you are obliged to comply with Articles 33 and 34 of Regulation (EU) 2016 /679 (obligations in case of breach of personal data security). In no case, however, do not allow an attacker or other unknown originator to participate in increasing the security of your system by using a program or file that he supplies.

ContextLocation: Document folders > Site map > Main menu > Supervisory and decision-making activities > Completed inspections > Inspections for 2019 > Inspection activities in the field of personal data protection - 1st semester > IT technology > Inspection of personal data security when operating an online game (natural person entrepreneur)View current documents | document archive | documents including the archive