Beat: Technology

Personal data of 4.5 million U.S. patients stolen in cyber attack

-, 18.08.2014, 18:30 Time

USPA News - Hackers from China have stolen personal data, including names and social security numbers, belonging to about 4.5 million Americans who visited hospitals operated by Community Health Systems, Inc. over the past five years, the firm disclosed Monday. The Tennessee-based company, which owns or operates 206 hospitals across 29 states, said it became aware last month that its computer network had been the target of external cyber attacks in April and June.

It was not clear why it took so long for CHS to disclose the information, which it did in a regulatory filing with the U.S. Securities and Exchange Commission (SEC). "The Company and its forensic expert believe the attacker was an `Advanced Persistent Threat` group originating from China who used highly sophisticated malware and technology to attack the Company`s systems," the company said in its filing. "The attacker was able to bypass the Company`s security measures and successfully copy and transfer certain data outside the Company." Community Health Systems said it had completed the eradication of the malware from its systems shortly before Monday`s filing, and added that it had also finalized the implementation of other remediation efforts which are designed to protect against future intrusions of the same type. The type of attacker identified in the CHS cyber attack would normally seek valuable intellectual property, such as medical device and equipment development data, the company said. In this instance, however, the attackers went after non-medical patient identification data relating to the company`s physician practice. It is believed that information was stolen which belonged to approximately 4.5 million individuals who visited CHS hospitals in the last five years or received services from physicians affiliated with the company. This data includes patient names, addresses, birthdates, telephone numbers, and social security numbers. Credit card details, medical information and clinical information were not affected. "The Company is providing appropriate notification to affected patients and regulatory agencies as required by federal and state law. The Company will also be offering identity theft protection services to individuals affected by this attack," the hospital operator said, adding that its cyber/privacy liability insurance was expected to mitigate any financial losses. Community Health Systems spokeswoman Tomi Galin did not respond to a request for comment. Monday`s news came less than two weeks after US Investigations Services, LLC (USIS), which has its headquarters in Virginia and is the largest commercial provider of background investigations to the federal government, also reported a breach of its computer network. It said the cyber attack had "all the markings of a state-sponsored attack." There was no indication the events were related.

Article online:
https://www.uspa24.com/bericht-2589/personal-data-of-45-million-us-patients-stolen-in-cyber-attack.html

Editorial office and responsibility:
V.i.S.d.P. & Sect. 6 MDStV (German Interstate Media Services Agreement):

Editorial program service of General News Agency:
UPA United Press Agency LTD
483 Green Lanes
UK, London N13NV 4BS
contact (at) unitedpressagency.com

Official Federal Reg. No. 7442619