HealthManagement
Promoting Management and Leadership

Foreign Government Behind Anthem's 2014 Hack?

According to investigators, the cyberattackers who broke into national insurer Anthem's IT system – exposing 78.8 million patient records as a result – were likely working on behalf of a foreign government. They also said that Anthem agreed to invest $260 million in improving its information security systems.

See Also: Locky Ramps Up Attack Methods via Facebook

However, a report released in early January detailing the investigation's findings did not identify the hackers or the foreign government for which they worked. The investigation was conducted jointly by the California Department of Insurance and six other state insurance departments. A spokeswoman for the California Insurance Department said federal officials requested the department not divulge any information regarding what government was behind the breach because of an ongoing federal probe.

Some cybersecurity firms have previously said that they were able to peg the breach to China because the malware was so unique.

“In this case, our examination team concluded with a significant degree of confidence that the cyberattacker was acting on behalf of a foreign government,” California Insurance Commissioner Dave Jones said in a statement announcing the findings. “Insurers and regulators alone cannot stop foreign government-assisted cyberattacks."

The U.S. government needs to take steps to prevent and hold foreign governments and other foreign actors accountable for cyberattacks on insurers, much as the president did in response to Russian government-sponsored cyberhacking in our recent presidential election, Jones explained. President Obama has said the U.S. will retaliate against Russia's alleged hacking and interference in the last election.

In 2014, hackers infiltrated Anthem's information technology system, gaining access to members' names, birth dates, Social Security numbers, home addresses and other personal information. The hackers gained access to Anthem's data warehouse and other Anthem computer systems when a user at one of Anthem's subsidiaries opened a phishing email containing malware, according to the California Insurance Department's report.

An Anthem spokeswoman said the insurer is working with the FBI and has found no evidence that the hackers shared or sold members' data, or evidence that fraud has occurred against individuals as a result of the breach.

Source: Modern Healthcare
Image Credit: Wikimedia Commons

Published on : Tue, 17 Jan 2017