Repeat hacks highlight Australia's cyber flaws

November 11 2022

Credit: Unsplash/CC0 Public Domain

Inadequate privacy safeguards and the stockpiling of sensitive customer information have made Australia a lucrative target in the eyes of foreign hackers, cybersecurity experts told AFP following a series of major data

breaches.

Medibank, Australia's largest private health insurer, recently confirmed that hackers had accessed the data of 9.7 million current and former customers, including medical records related to drug abuse and pregnancy terminations.

Telecom company Optus fell prey to a data breach of similar scale in late September, during which the personal details of up to 9.8 million people were accessed.

Both incidents sit comfortably among the largest data breaches in Australian history.

Australian National University cybersecurity expert Thomas Haines said many companies had been hoarding personal data that they should not have been hanging on to.

"There was a famous line for a while: Data is the new oil," he told AFP.

"If data is the new oil, then we're living the era of the weekly oil spill."

Haines contrasted Australia's approach with that of the European Union, which in 2018 adopted sweeping privacy reforms limiting how organisations collect, use and store personal data.

"There have got to be incentives in place to stop companies hoarding data they don't need, or to penalise those companies for big leaks. Europe has done this," he said.

"At the moment the business incentives are basically along the lines of: Let's just keep a whole bunch of data."

Haines said Medibank appeared to be an exception, in that most of the sensitive information within its databases had been stored for good reason.

Hacking 'for profit'

Australia's comparatively weak safeguards against identity theft meant it was also easier to exploit stolen personal information, Haines said.

"All they need to know is your passport, your driver's licence and some other things—and then I can start taking out loans in your name."

Haines said European countries such as Norway had much more stringent requirements involving face-to-face contact.

Dennis Desmond, a former FBI agent and US Defense Intelligence Agency officer, said most hackers were searching for particular types of data.

"For-profit hackers are going after healthcare data, they're going after identity data and credentials to access systems," he told AFP.

"There is a profit motivation there, otherwise they wouldn't be risking jail and prosecution."

The Medibank hackers this week started leaking stolen data to a dark web forum, after the company refused to pay a US$9.7 million (Aus$15 million) ransom.

The Optus breach led to the theft of customers' names, birth dates, and passport numbers.

Russia blamed

Australian Federal Police Commissioner Reece Kershaw on Friday blamed the Medibank cyberattack on a team of hackers based in Russia.

"We believe those responsible for the breach are in Russia," he told reporters.

"Our intelligence points to a group of loosely affiliated cyber criminals who are likely responsible for past significant breaches in countries across the world."

Medibank data leaked to the dark web so far has included hundreds of potentially-compromising medical records related to drug addiction, alcohol abuse and sexually-transmitted infections.

Home Affairs Minister Clare O'Neil conceded on Friday the country's cyber defences had not always been up to scratch.

University of Sydney data researcher Jane Andrew said one major flaw was that Australian companies were not always obliged to report data breaches.

"There are heaps of data breaches happening all the time that we don't hear anything about," she told AFP.

"Companies have been gathering data because it's seen to be valuable, without fully understanding the potential risks."

© 2022 AFP

Citation: Repeat hacks highlight Australia's cyber flaws (2022, November 11) retrieved 13 March 2024 from

https://techxplore.com/news/2022-11-hacks-highlight-australia-cyber-flaws.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.