TechXplore

Australia mulls tougher cybersecurity laws after data breach

September 26 2022, by ROD McGUIRK

A customer waits for service at a Optus phone store in Sydney, Australia, Thursday, Oct. 7, 2021. The Australian government said on Monday, Sept. 26, 2022, it was considering tougher cybersecurity rules for telecommunications companies after Optus, the nation’s second-largest wireless carrier, reported personal data of 9.8 million customers had been breached. Credit: AP Photo/Mark Baker, File

The Australian government said on Monday it is considering tougher cybersecurity rules for telecommunications companies and blamed Optus, the nation's second-largest wireless carrier, for an unprecedented breach of personal data from 9.8 million customers.

Optus said last Thursday it had become aware the day before of the cyberattack which obtained the details of 9.8 million people—of Australia's population of 26 million.

Cybersecurity Minister Clare O'Neil told Australian Broadcasting Corp. the hack was an "unprecedented theft of consumer information in Australian history."

For 2.8 million current and former Optus customers, the breach involved "significant amounts of personal data," including driver's licenses and passport numbers, O'Neil said.

Those 2.8 million people are at significant risk of identity left and fraud, she said.

"The breach is of a nature that we should not expect to see in a large telecommunications provider in this country," O'Neil told Parliament.

In some countries, such a breach would result in fines "amounting to hundreds of millions of dollars," O'Neil said.

Australian law doesn't currently allow for Optus to be fined for the breach.

"A very substantial reform task is going to emerge from a breach of this scale and size," O'Neil said.

"One significant question is whether the cybersecurity requirements that we place on large telecommunications providers in this country are fit for purpose," she added.

Australian Federal Police said in a statement that reports the stolen data had already been sold were under investigation.

Australian investigators are working with overseas law enforcement agencies to determine who was behind the attack and to help shield the public from identity fraud, the statement said.

"To protect the integrity of the criminal investigation, the AFP will not divulge what information it has obtained in the first few days" of the investigation, police said.

Jeremy Kirk, a Sydney-based cybersecurity writer, said he used an online forum for criminals who trade in stolen data to ask someone who claimed to have downloaded the Optus information how it was accessed.

Optus appeared to have left an application programming interface, a piece of software known as an API that allows other systems to communicate and exchange data, open to the public, she said.

"It looks like it was a failure to secure the software system, so anybody on the internet could find it," Kirk told Ten Network television.

O'Neil didn't detail how the breach occurred, but described it as a "quite a basic hack."

Optus had "effectively left the window open for data of this nature to be stolen," she said.

O'Neil called on Optus to offer compromised customers free credit monitoring to protect them from identity theft, a request that the Sydney-based company complied with later on Monday.

Optus announced it was offering its "most affected" customers free 12-month subscriptions to Equifax Protect, a credit monitoring and identify protection service.

Optus said the information that had been accessed by an unidentified third party included customers' names, dates of birth, phone numbers and email addresses.

Police and other government security agencies worked through the weekend to protect affected customers, O'Neil said.

Government agencies were also working with the banking sector to protect customers.

"This is complex. It's legally and technically complex, but we are working on a solution," O'Neil said.

Prime Minister Anthony Albanese described the breach as a "huge wake-up call for the corporate sector."

Albany foreshadowed potential changes to privacy provisions so that banks can move more quickly to protect their own customers after such a breach.

"We know that in today's world there are actors—some state actors, but also some criminal organizations—who want to get access to people's data," Albanese said.

Optus chief executive Kelly Bayer Rosmarin said in a statement last week that, "We are devastated to discover that we have been subject to a cyberattack that has resulted in the disclosure of our customers' personal information to someone who shouldn't see it."

Citation: Australia mulls tougher cybersecurity laws after data breach (2022, September 26) retrieved 4 May 2024 from https://techxplore.com/news/2022-09-australia-mulls-tougher-cybersecurity-laws.html