Australia: Optus data breach highlights widespread security vulnerabilities

Martin Scott
5 October 2022

Millions of Australians face an increased risk of identity theft after their personal data was exposed in a massive online security breach at Optus last month.

The so-far unidentified hacker obtained sensitive details, including passport, drivers' licence and medicare numbers, of around 10 million current and former customers of Australia's second-largest telecommunications provider.

While Optus insists that 7.7 million of the victims need not take action, this may only mean that the information of theirs that was compromised is impractical to change, such as their full name, home address and date of birth.

The company reports that of the 2.1 million customers who had at least one identifying document number stolen, 1.2 million had current, valid identification numbers exposed. In most cases this included drivers' licences, while around 150,000 passports and 37,000 Medicare cards were also compromised.

While an online forum poster using the name "Optusdata," thought to be the hacker, claims to have deleted the stolen data, there is no guarantee that this is true. As a result, almost 40 percent of the Australian population, along with international visitors who registered for Optus services since 2017, confront an enhanced likelihood of fraud.

At minimum, more than 10,000 Optus customers are at risk, as they were in included in a sample posted online by "Optusdata" to prove they had access to the data. This data has been reposted and remains readily accessible.

Stolen identity documents could be used to establish fraudulent bank and credit card accounts, allowing criminals to launder money or rack up huge debts against the names of the Optus breach victims.

Basic information like that stolen from customers, that Optus says should not be of concern, such as addresses, phone numbers, full names and dates of birth, could be used in social engineering attacks to gain access to existing accounts with other companies.

The Optus hack was reported in the media on September 22, the day after the company detected unusual data traffic on their networks.

While the company initially claimed it had been the victim of a "sophisticated" attack, the consensus among security experts, backed up by the claims of the purported hacker, is that it was anything but.

"Optusdata" told Information Security Media Group reporter Jeremy Kirk they had acquired the data through an unsecured Application Programming Interface (API), which allowed access to Optus's customer database from devices anywhere on the public internet.

The hacker was able to access the information of all of the company's customers by running an automated script that asked for database records one-by-one, simply increasing the "contactId" index number by one with each request.

"Optusdata" explained that no username, password or authentication token was required, writing to Kirk: "No authenticate needed. That is bad access control. All open to internet for any one to use."

APIs are used extensively to allow communication between different pieces of software, within a single device or across networks. When Optus customers view their account via a mobile app or the web, a similar API to the one that was breached is used to retrieve and display their own information. Properly implemented, this is only possible after logging in, and cannot be used to display the details of other customers.

Security experts have speculated that the exploited API was a new version that was being tested and was not intended to be accessible from the public internet. To protect security, such an API should have used test data rather than actual customer details.

Kirk's analysis of public Domain Name System (DNS) records—essentially the internet equivalent of a phone

book—suggests that the unsecured API may have been accessible for up to three months.

The massive breach points to the danger of placing sensitive data in the hands of vast corporations, whose only concern is profit. While the Optus data breach is notable for its vast scale, hacks accessing substantial amounts of personal data are increasingly common.

Last month, American Airlines revealed that personal data including drivers' licences, passport numbers and "certain medical information" of more than 1,700 employees and customers had been stolen in a phishing attack in July.

Last week, Uber's former security chief, Joe Sullivan, was found guilty of covering up the 2016 exfiltration of 50 million customers' and 7 million drivers' personal data. The court heard that Sullivan paid the hackers $US100,000 in Bitcoin in exchange for their silence on the breach, which was only revealed more than a year later when Sullivan was fired.

In 2020, Australian logistics giant Toll was hit by a ransomware attack that compromised workers' personal and financial details and prevented them from being paid correctly. The email addresses and full names of 139 million users of graphic design software company Canva were stolen in 2019.

One of the largest ever breaches of sensitive data was the 2017 exploitation of a "website application vulnerability" at credit reporting agency Equifax, in which the personal and credit information of 143 million was stolen over a period of more than two months. The company had failed to install a patch for a well-known bug in their Apache web server.

This is particularly notable because Optus is offering customers affected by last month's hack a 12-month subscription to Equifax's credit monitoring service.

In response to the Optus attack, federal Treasurer Jim Chalmers and Minister for Communications Michelle Rowland today announced changes to the Telecommunications Act to "facilitate targeted data sharing between telcos and financial institutions."

For "security reasons," Chalmers claimed, the identity of these financial institutions could not be disclosed. In other words, some 10 million Optus customers, whose personal information may already be being traded on the online black market, now face having it shared further between unidentified institutions.

The announcement marked a shift from Labor's earlier denunciations of the lax security at Optus. Now, the government's clear priority is to work closely with the multi billion-dollar company to salvage its reputation.

The latest regulatory change is in line with years of prior legislation, passed with bipartisan support, that imposes few responsibilities on corporations to protect user data, and minimal penalties for the failure to do so.

Legislation regarding the telecommunications industry has instead been focussed on increasing the scope of data that must be retained, in order to facilitate greater surveillance by the state. The very fact that Optus had passport and drivers' licence numbers recorded, and therefore vulnerable, is a result of such laws.

In addition to identity information, Australia's data retention laws require telecommunications providers to keep records of source and destination phone numbers, email addresses and IP addresses for all communication except web browsing, as well as the location of the user at the time of the transmission.

Amendments to the Security of Critical Infrastructure Act 2018 passed in 2021 allow the Australian Signals Directorate to take control of "critical infrastructure," the definition of which has been expanded to include supermarkets, banks, financial markets, education and transport, in the event of a "cyber security incident."

Law firm Corrs, Chambers and Westgarth noted last year: "The new government response powers go beyond the measures other members of the 'Five Eyes' alliance have implemented."

These regulatory changes have nothing to do with protecting ordinary Australian people from the growing threat of cyber attack. Despite the propaganda campaign employed to justify ever more draconian surveillance measures, digital attacks are mostly opportunistic exploitations of vulnerabilities that exist due to the profit-led priorities of business.

The only answer to this is to take the valuable personal data of individuals out of the hands of corporations by placing vital digital infrastructure, like telecommunications and cloud services, along with traditional utilities and the banks, under democratic workers' control and ownership.