

WŁADZE SINGAPURU: ZA CYBERATAKIEM NA KLINKI ZDROWIA MOŻE STAĆ OBCE PAŃSTWO

Minister łączności i informacji oraz handlu i przemysłu Singapuru S. Iswaran poinformował w poniedziałek, że za cyberatakami na kliniki zdrowia grupy SingHealth, który ujawniono w lipcu, może stać obce państwo. W wyniku ataku wyciekły dane 1,5 mln osób.

Zdaniem ministra S. Iswarana, wyniki przeprowadzonej przez rząd Singapuru szczegółowej analizy wskazują na działalność bardzo wykształconych hakerów, którzy pracują w zorganizowanej grupie, potencjalnie opłacanej przez wroga państwa.

Jak podkreślił Iswaran, "grupy tego rodzaju znane są z wyszukanych i zaawansowanych cyberataków i złożonych cyberoperacji, które są z reguły szczegółowo zaplanowane celem np. wykradania poufnych informacji".

Hakerzy stojący za atakiem na kliniki zdrowia z grupy SingHealth według singapurskiego ministra korzystali z "zaawansowanych narzędzi", w tym "specjalnie przygotowanego złośliwego oprogramowania, które było zdolne do ominięcia programów antywirusowych działających w strukturach SingHealth i aktywnych tam narzędzi bezpieczeństwa".

Powołując się na względy bezpieczeństwa państwowego, Iswaran zaznaczył, że nie chce wskazywać konkretnego państwa, które jest podejrzewane o wrogi działanie.

W wyniku cyberataku, który miał miejsce pomiędzy 27 czerwca a 4 lipca tego roku, przestępcy skopiowali dane personalne osób, które odwiedzały kliniki należące do grupy SingHealth od lipca 2015 roku, w tym ich imiona i nazwiska, adresy i numery dokumentów.

Wykradzono również informacje na temat leków przepisanych 160 tys. pacjentów, w tym premierowi kraju Lee Hsien Loongowi. "Sprawcy konkretnie i wielokrotnie celowali w dane personalne i informacje o lekach przepisanych premierowi Lee" - napisano w państwowym komunikacie, który ukazał się 20 lipca.

Nie wykradzono natomiast innych informacji dotyczących stanu zdrowia pacjentów, ich historii medycznej, diagnoz lekarskich czy wyników badań - podano w lipcowym komunikacie. Hakerzy nie skasowali ani nie zmienili żadnych informacji w bazie danych; nie ma dowodów, aby do podobnych ataków doszło w systemach innych firm świadczących usługi medyczne - zapewniono.

Atak ten pokazuje jak ważne jest cyberbezpieczeństwo systemów i sieci teleinformatycznych w placówkach medycznych. Polska wdrażając elektroniczne systemy w służbie zdrowia powinna pamiętać o ochronie tych danych.