Służby nie chcą utrudniać sobie szpiegowania

25 maja 2015

Służby państw Sojuszu Pięciorga Oczu wiedziały jak szpiegować smartfony z wykorzystaniem linków do sklepów z aplikacjami Google i Samsunga. Szpiedzy zachowali tę wiedzę dla siebie, ale czy nie powinni jej ujawnić, aby zapobiegać zagrożeniom?

Gazety znów publikują informacje pochodzące z archiwum dokumentów Snowdena. Tym razem dokument z 2012 roku został opublikowany i opisany przez CBC News w tekście pt. „Spy agencies target mobile phones, app stores to implant spyware".

Ujawniony dokument mówi o wysiłkach podejmowanych przez służby specjalne tzw. Sojuszu Pięciorga Oczu (USA, Kanady, UK, Australii i Nowej Zelandii). Pracowały one nad możliwością instalowania oprogramowania szpiegowskiego na smartfonach w momencie, gdy użytkownik chciał się połączyć ze sklepem z aplikacjami od Google lub Samsunga.

Jak zauważa CBC, służby w zasadzie unikały szpiegowania obywateli swoich sojuszników. Skupiły się na serwerach, z którymi smartfony się łączą w czasie pobierania lub aktualizowania aplikacji. Na celownik trafiły serwery z Francji, Szwajcarii, Kuby, Rosji i innych krajów.

Następnie agenci odkryli luki w popularnej przeglądarce UC Browser, mającej szczególnie dużo użytkowników w Chinach. Te luki umożliwiały pozyskanie informacji m.in. o numerach telefonów użytkowników. Informacja o lokalizacji była szyfrowana, ale według ekspertów przepytanych przez CBC możliwe było stosunkowo łatwe złamanie tego zabezpieczenia.

Służby mogły dzięki wspomnianej luce śledzić przemieszczanie się danej osoby i badać jej powiązania z innymi osobami. Pytanie tylko, czy służby nie powinny powiadomić dostawcy

oprogramowania o odkrytej luce? Nie tylko służby specjalne mogły wykorzystać słabości aplikacji. UC Browser to oprogramowanie rozwijane przez firmę UCWeb przejętą przez Alibaba Group. Źródła CBC twierdzą, że dostawca oprogramowania nie otrzymał żadnego ostrzeżenia od służb.

Jeszcze raz powtórzmy pytanie – czy służby specjalne, nawet te najbardziej tajne, nie powinny powiadamiać o wykrytych lukach? Może się wydawać, że służby specjalne mają prawo wykorzystywać pewne „szczególne" środki. Spróbujmy jednak zadać pytanie pomocnicze. Po co stworzono służby specjalne? Żeby szpiegować? Wcale nie. Służby specjalne są po to, aby zapewnić ludziom bezpieczeństwo, natomiast szpiegowanie powinno być tylko wyjątkowym narzędziem tych służb, a nie celem ich istnienia.

Jeśli zatem służby specjalne wiedzą o luce bezpieczeństwa i ukrywają tę wiedzę, w rzeczywistości narażają obywateli na ryzyko. W tym wypadku trudno mówić o właściwym wypełnianiu zadań.

Nie wiadomo czy służby Sojuszu Pięciorga Oczu wykorzystały opisane możliwości. Najwyraźniej dobrze je przetestowały i potwierdziły, że metoda w praktyce zadziała.

To nie pierwszy wyciek mówiący o tym, że służby specjalne nie tylko nie usuwają zagrożeń, ale wręcz je pielęgnują. Zastanówmy się teraz, czy jeśli Snowden wyniósł z NSA wiedzę o tych lukach, to nie wyniósł jej wcześniej ktoś inny? Skąd mamy wiedzieć, że ta inna osoba zrobiła z tego dobry użytek? Jeśli jakaś organizacja pielęgnuję tajną wiedzę o zagrożeniach zamiast te zagrożenia usuwać, to nie wiemy jakie będą tego ostateczne konsekwencje.

Nie po raz pierwszy słyszeliśmy o tym, że służby specjalne mogą przyczyniać się do obniżenia standardów bezpieczeństwa informatycznego. Pod koniec roku 2013 pojawiły się doniesienia o tym, że pewna firma mogła wziąć łapówkę w zamian za zastosowanie technologii, która pozwoli służbom łatwiej ominąć

zabezpieczenia. Dużo się mówi o tym, że służby specjalne chcą „tylnych furtek” do popularnych technologii. Tylko czy służby przejmują się tym, że ktoś inny będzie korzystał z tej furtki?

Autorstwo: Marcin Maj
Źródło: DI.com.pl