NSA zagląda wszędzie

6 grudnia 2014

Z opublikowanego wczoraj raportu dowiadujemy się, że NSA szpiegowała setki firm i organizacji. Pracownicy tej agencji są bowiem w stanie włamać się do sieci komórkowych na całym świecie. Dzięki znajomości szczegółowych danych na temat obecnych sieci oraz planów ich rozbudowy mogą penetrować infrastrukturę oraz wprowadzać do niej słabe punkty. Eksperci ostrzegają, że tego typu działania – polegające na wprowadzaniu luk lub dezaktywacji łat zastosowanych przez operatora sieci – to obosieczny miecz. Dziury takie mogą wykorzystać inne rządy oraz grupy cyberprzestępców. „Nawet jeśli popierasz działania NSA i twierdzisz, że nie masz nic do ukrycia, powinieneś być przeciwko działaniom, których celem jest wprowadzanie dziur. Bo gdy NSA spowoduje, że gdzieś pojawi się luka, to nie tylko NSA będzie mogła z niej skorzystać" – mówi Karsten Nohl, ekspert ds. bezpieczeństwa.

Nie po raz pierwszy NSA wprowadza luki do powszechnie używanego oprogramowania. Wiadomo, że agencja osłabiła oprogramowanie BSAFE firmy RSA, w związku z czym ta ostatnia wydała rekomendację, by zaprzestać używania programu w jego domyślnej konfiguracji.

Teraz dowiadujemy się, że w ramach programu AURORAGOLD NSA monitorowała ponad 1200 kont pocztowych należących do operatorów telefonii komórkowej. Jednym ze śledzonych celów jest GSM Association (GSMA). To brytyjska organizacja, która współpracuje z Microsoftem, Facebookiem, AT&T, Cisco i wieloma innymi firmami, a jej celem jest zapewnienie kompatybilności pomiędzy sprzętem i oprogramowaniem sieci komórkowych, a produktami wspomnianych firm. GSMA koordynuje m.in. prace operatorów sieci komórkowych, dzięki czemu możliwe jest przesyłanie sygnałów pomiędzy różnymi sieciami. Wiadomo, że NSA przechwytywała dokumentację oznaczoną jako IR.21s. Korzysta z niej większość operatorów telefonii komórkowej, a

zawiera ona ustalenia dotyczące technicznych szczegółów współpracy. Ich przeanalizowanie przez specjalistów z NSA pozwala na odkrycie luk czy opracowanie szkodliwego kodu. W IR.21s znajdują się też szczegóły dotyczące zabezpieczeń kryptograficznych. Tego typu informacje są szczególnie poszukiwane przez NSA.

Autor: Mariusz Błoński
Na podstawie: Ars Technica
Źródło: Kopalnia Wiedzy