NSA złamała popularne narzędzia szyfrowania

7 września 2013

NSA może złamać lub obejść popularne narzędzia szyfrowania wykorzystywane w bankowości, usługach komunikacji oraz innych e-usługach – donoszą media, powołując się na dokumenty od Edwarda Snowdena.

Czołowe gazety nie przestają publikować przecieków opartych na dokumentów od Edwarda Snowdena. Wczoraj pojawiły się informacje o tym, że NSA posiada narzędzia pozwalające jej złamać lub obejść metody szyfrowania powszechnie używane w różnego rodzaju usługach internetowych, m.in. bankowych, zdrowotnych, e-handlu itd. Piszą o tym „New York Times" i „Guardian".

Już wcześniej, gdy ujawniono czarny budżet amerykańskiego wywiadu, niektórzy komentatorzy zwrócili uwagę, że miliardy dolarów pochłonął program kryptologiczny, przy którym pracowały dziesiątki tysięcy osób. Jeśli tak wielkie środki inwestuje się w łamanie szyfrów, to osiągnięcie jakichś sukcesów jest wysoce prawdopodobne. Najnowsze wycieki pokazują jednak, że amerykańskie służby, działając w tym obszarze, korzystały z pomocy innych wywiadów i firm.

Agencja Bezpieczeństwa Narodowego (NSA) współpracowała m.in. z brytyjską Centralą Łączności Rządowej (GCHQ), która opracowywała metody przechwytywania szyfrowanych informacji popularnych e-usługodawców – Google, Yahoo, Facebooka i Microsoftu. Do roku 2012 Brytyjczycy mieli opracować „nowe możliwości dostępu" do danych Google, czemu Google z pewnością będzie oficjalnie zaprzeczać.

NSA i GCHQ pracowały nad przełamaniem zabezpieczeń przy pomocy specjalistów i superkomputerów. Program był prowadzony od początku tego wieku, pompowano w niego setki milionów dolarów

rocznie, a w roku 2010 najwyraźniej dokonano istotnych przełomów. Dokumenty z tego roku wspominają, że „duże ilości zaszyfrowanych danych z internetu, które do tej pory były odrzucane, są teraz do wykorzystania”.

Jednak nie tylko superkomputery mogły zapewnić wywiadowi sukces. New York Times i Guardian twierdzą, że istotnym elementem programu była współpraca z firmami, które pod naciskiem NSA mogły umieszczać w swoich produktach „tylne furtki” dla wywiadu. Co więcej, agencja używała swoich wpływów, by współtworzyć standardy w zakresie szyfrowania, dbając oczywiście o ich słabe, a nie mocne strony.

Jeden z niejawnych dokumentów wspomina, że pewien standard przyjęty w roku 2006 przez Narodowy Instytut Standaryzacji i Technologii (NIST), a potem przez ISO został opracowany pod dyktando NSA. Już w roku 2007 niektórzy specjaliści sugerowali, że w tym standardzie mogły się znaleźć tylne furtki, o które zadbała NSA. Wówczas brzmiało to jak teoria spiskowa, a najnowsze wycieki po prostu to potwierdzają.

Najnowsze wycieki nie potwierdzają, że NSA lub GCHQ łamią prawo. Mogą one prowadzić własne prace badawcze i w pewnym zakresie współpracować z firmami, ale znów pojawia się problem z przejrzystością tych działań.

Jeśli NSA współpracuje przy tworzeniu standardów bezpieczeństwa jako „ekspert”, a działa na rzecz osłabienia tych standardów, to w gruncie rzeczy jest to ogromne kłamstwo. Efektem tego kłamstwa jest osłabienie ogólnego bezpieczeństwa w internecie. W ogóle pozostawianie „tylnych furtek” jest nierozsądne, bo nie wiadomo, kto z nich skorzysta.

„New York Times” zauważa, że w przeszłości NSA chciała oficjalnie wdrażać „tylne furtki” do rozwiązań szyfrowania, ale opinia publiczna wyraziła sprzeciw. Agencja najwyraźniej nie porzuciła tego pomysłu, ale zaczęła go realizować w tajemnicy. Oczywiście wszystko dla bezpieczeństwa obywateli,

dla walki z terroryzmem…

NSA zdaje się nie dostrzegać jednej rzeczy. Jeśli potężna i tajna organizacja robi coś, czego społeczeństwo nie chce, wielu ludzi poczuje zagrożenie. W kraju demokratycznym służby specjalne powinny robić tylko to, do czego społeczeństwo je upoważniło. Utajnianie ich działań ma służyć skuteczności, a nie samowolnemu poszerzaniu swoich wpływów.

Autor: Marcin Maj
Źródło: Dziennik Internautów