

Czy Cameron zabroni szyfrowania?

14 stycznia 2015

Nie można się zgadzać na takie formy komunikacji, których władze nie mogą odczytać – uważa brytyjski premier David Cameron, który obiecuje rozprawienie się z tą sprawą po wyborach. Prasa już sugeruje, że Cameron chce zabronić Snapchata albo WhatsApp, ale problem wydaje się nieco szerszy.

Obawialiśmy się, że po ataku na Charlie Hebdo wróci przyzwolenie na inwigilację i rzeczywiście tak się dzieje. Najpierw niektórzy dziennikarze pisali o tym, że inwigilacja właściwie nie jest taka zła. Teraz politycy zaczynają coraz odważniej zapowiadać wzmożenie inwigilacji i na tym tle zabłysnął brytyjski premier David Cameron.

– Czy możemy dopuszczać środki komunikacji pomiędzy ludźmi, których (...) nie możemy przeczytać? (...) Moja odpowiedź na to pytanie brzmi: nie, nie możemy. Pierwszym zadaniem każdego rządu jest zapewnienie bezpieczeństwa naszemu krajowi i ludziom. Ataki w Paryżu raz jeszcze pokazały skalę zagrożenia terrorystycznego, w obliczu którego stajemy... – mówił Cameron.

Brytyjska prasa zinterpretowała te słowa jako zapowiedź zakazania takich szyfrowanych form komunikacji, do których służby specjalne nie mają tylnej furtki. The Independent zasugerował, że może chodzić również o popularne narzędzia komunikacji, takie jak WhatsApp albo iMessage. Huffington Post UK pisał, że Cameron chciałby zabronić Snapchata. Te obawy są dziś powtarzane także przez prasę amerykańską.

Czy Cameron mógłby spróbować czegoś takiego? Cóż... mówimy o premierze, który wprowadził w swoim kraju absurdalny sposób blokowania pornografii. Cameron rzeczywiście mógłby spróbować zabronić Snapchata, co nie oznacza, że to by mu się udało. Byłby to przecież zamiar odcięcia Brytyjczyków od przydatnych

i lubianych aplikacji stosowanych przez miliony ludzi na całym świecie.

Dodajmy jeszcze, że niejeden polski polityk wzorował się na pomysłach Camerona. W przyszłości to też niewykluczone.

Mimo wszystko zakazanie Snapchata w UK wydaje się wątpliwe. Prawdziwie niepokojące jest coś innego – zaangażowanie tak ważnego polityka w kampanię przeciwko narzędziom do bezpiecznej, szyfrowanej komunikacji. Tę kampanię obserwujemy nie od dziś i to nie Cameron ją zaczął. We wrześniu ubiegłego roku pisaliśmy o tym, jak to szef FBI skrytykował Apple i Google za szyfrowanie w smartfonach. Niedługo potem prokurator generalny Stanów Zjednoczonych powiedział wprost, że nie mogą istnieć technologie bez tylnej furtki dla władz.

Szczerze powiedziawszy, służby nie chcą „tylnych furtek”. One chcą, żeby producenci rozwiązań do komunikacji zbudowali dla nich wygodne drzwi frontowe, dzięki którym zawsze mogłyby sprawdzić, co napisaliśmy. Dokumenty od Snowdena mówią, że komunikator Skype ma takie specjalne wejście dla władz.

Nagonkę na technologie szyfrowania uzasadnia się chęcią zapewnienia nam bezpieczeństwa. Należy jednak zadać pytanie, czy terroryści naprawdę używają WhatsApp, aby pisać do siebie wiadomości w rodzaju „Hej! Jutro spotykamy się z karabinami pod redakcją Charlie Hebdo!”? Niekoniecznie. Istnieje wiele możliwości zaszyfrowania wiadomości i przesłania jej. Zwykłym e-mailem da się przesłać szyfrowaną wiadomość. Z tej możliwości nierzadko korzystają dziennikarze, aby zapewnić bezpieczeństwo swoim źródłom. Ba! Nawet zwykłą pocztą można wysłać szyfrowaną wiadomość, na papierze albo na nośniku w kopercie!

Jednocześnie wycieki Snowdena udowodniły, że władze mogą ostro nadużywać dostępu do treści z komunikatorów. Według dokumentów Snowdena właśnie brytyjska agencja GCHQ z pomocą amerykańskiej NSA zapisywała obrazki z wideoczatów Yahoo i zbierała je w

swoich bazach danych. Wśród zebranych materiałów były obrazy przedstawiające ludzi nago. Czy naga fotka tego lub innego obywatela ma kluczowe znaczenie dla bezpieczeństwa kraju? To wysoce wątpliwe.

Generalnie można odnieść wrażenie, że po atakach na Charlie Hebdo politycy wrócili do przekonania, że wreszcie można coś zrobić z tym całym niegrzecznym internetem. Wczoraj wspominaliśmy o oświadczeniu ministrów spraw wewnętrznych, którzy chcą zwalczać radykalizację „zwłaszcza w internecie”.

Autorstwo: Marcin Maj

Źródło: [Dziennik Internautów](#)