

Szyfrowanie to wielki problemem w walce z terroryzmem

30 marca 2015

Firmy udostępniające oprogramowanie do szyfrowania powinny rozważyć swój wpływ na organy ścigania – uważa dyrektor Europolu Rob Wainwright, który dołączył do grona ludzi narzekających na technologie prywatności bez tylnych furtek.

Od kilku miesięcy politycy i przedstawiciele organów ścigania narzekają na szyfrowanie informacji w smartfonach oraz na komunikatory zapewniające szyfrowanie. Do tej pory narzekania płynęły głównie z USA, ale to się zaczyna zmieniać.

Dyrektor Europolu Rob Wainwright w wypowiedzi dla BBC stwierdził, że szyfrowana komunikacja coraz bardziej utrudnia ściganie terrorystów. Jego zdaniem firmy technologiczne powinny rozważyć, jaki wpływ mają ich produkty na możliwości organów ścigania.

– To staje się prawdopodobnie największym problemem dla policji i służb bezpieczeństwa w radzeniu sobie z zagrożeniami terroryzmem. To zmieniło naturę pracy antyterrorystycznej z takiej, która polegała na dobrym monitorowaniu komunikacji, na taką, która już na to nie pozwala – mówił Wainwright.

Szef Europolu wyraził również rozczarowanie stanowiskiem firm technologicznych, które postanowiły sprzedawać prywatność. Zauważył jednak, że same służby specjalne są tu trochę winne i powinny odbudować zaufanie społeczne. Wainwright zwrócił też uwagę na zjawisko, jakim jest używanie przez terrorystów... Twittera. Jego zdaniem Państwo Islamskie ma ponad 50 tys. kont na Twitterze.

Jak już wspomnieliśmy, przedstawiciele władz amerykańskich

również narzekali na szyfrowanie w sieci. We wrześniu ubiegłego roku szef FBI był zmartwiony szyfrowaniem w Androidzie i iOS. Wyraził on przekonanie, że sprzedawanie ludziom produktów szyfrujących pliki to „stawianie ludzi ponad prawem”.

W październiku ubiegłego roku Eric Holder, prokurator generalny Stanów Zjednoczonych, mówił że trzeba zapewnić organom ścigania dostęp do otrzymywania informacji w ramach dochodzenia (czytaj: trzeba stworzyć „tylne furtki”).

W styczniu tego roku premier Wielkiej Brytanii David Cameron powiedział, że jego zdaniem nie można się zgadzać na takie formy komunikacji, których władze nie mogą odczytać. Prasa zaczęła wówczas na poważnie pytać, czy premier ma zamiar zabronić Snapchata?

Jak widzimy, najnowsza wypowiedź szefa Europolu mieści się w ustalonych już trendach. Przedstawiciele władz i organów ścigania w Stanach Zjednoczonych i Europie domagają się wycofania z rynku produktów opartych o szyfrowanie albo przynajmniej udostępnienia władzom „tylnych furtek”.

Specjaliści od bezpieczeństwa oraz obrońcy prywatności zawsze reagują podobnie na tego typu apele. Wskazują przede wszystkim na to, że tworzenie „tylnych furtek” dla władz oznacza generalnie osłabianie technologii, która ma służyć bezpieczeństwu. Szyfrowana komunikacja jest potrzebna w wielu dziedzinach życia, aby chronić przed przestępczością i nadużyciami. Poza tym ludzie mogą zwyczajnie chcieć prywatności, a afera Snowdena pokazała, że służby specjalne tego nie szanują. Z dokumentów Snowdena wynika, że NSA i GCHQ śledziły wideoczaty, także te intymne i nie bardzo wiadomo, jak to się miało do walki z terroryzmem.

Osobnym problemem jest to, że w dzisiejszym świecie mamy ogrom informacji i sposobów ich przekazywania. Terroryści wcale nie muszą korzystać z szyfrowanego komunikatora. Nie muszą w ogóle

szyfrować, by ukryć informację np. dzięki steganografii. Jest to sposób polegający na umieszczeniu ukrytego przekazu w innej treści, która wcale nie wygląda jak ukryty przekaz. Przykładowo w sieci są miliony zdjęć i czy da się ustalić, które z nich może zawierać ukryty przekaz?

W ubiegłym roku Navi Pillay, Wysoka Komisarz ONZ ds. Praw Człowieka, porównała masową inwigilację do „szukania igły w stogu siana”. Po aferze Snowdena politycy i przedstawiciele służb robią wrażenie, jakby dostrzegali tylko wybrane problemy związane ze skutecznością działań (np. szyfrowanie), jednocześnie unikając dyskusji o takich problemach, jak nadmierna nieselektywna inwigilacja, która może odciągać uwagę służb od istotnych zagrożeń.

Autorstwo: Marcin Maj

Źródło: [Dziennik Internautów](#)