Narzędzia wysokiego ryzyka

13 marca 2015

Jak reaguje władza, gdy to, co postrzega jako zagrożenie, wymyka się jej spod kontroli? Sięga po nowe zakazy i represje. Ta logika sprawdza się pod każdą szerokością geograficzną, mimo że przyzwyczailiśmy się do kojarzenia jej z reżimami autorytarnymi. W reakcji na ostatnie zamachy terrorystyczne w Paryżu, David Cameron i Barack Obama wypowiedzieli wojnę narzędziom, które umożliwiają bezpieczną komunikację. Ta retoryka otwiera drogę do stygmatyzacji osób, które próbują zachować prywatność i anonimowość w sieci. Do czego to prowadzi? Co ryzykujemy, korzystając z tzw. bezpiecznych narzędzi komunikacji?

EFEKT SNOWDENA

W ciągu ostatnich dwóch lat coś drgnęło w podejściu wiodących korporacji technologicznych do prywatności i bezpieczeństwa danych. Apple zwiększyło poziom zabezpieczenia danych na swoich serwerach – od niedawna są one szyfrowane w sposób, który w zasadzie wyklucza możliwość ich masowego przechwytywania przez NSA i FBI. Podobne zmiany w systemie zabezpieczeń wprowadziła w ofercie biznesowej firma Box.com. Jeszcze dalej poszła popularna aplikacja WhatsApp, wprowdzając domyślne szyfrowanie komunikacji swoich użytkowników (na bazie oprogramowania Open WhisperSystems). W nowej linii telefonów komórkowych firma Apple zablokowała również możliwość przekazania policji danych bez udziału osoby, której telefon jest przeszukiwany.

Trudno oceniać, na ile ten trend to trwały „efekt Snowdena”, a na ile testowanie nowej strategii marketingowej, którą za chwilę zastąpić może coś innego. W końcu rozmawiamy o przedsiębiorstwach zorientowanych na zysk i żyjących z komercjalizacji danych, przed którą nie sposób się chronić tak długo, jak powierzamy nasze dane tego typu pośrednikom. Realna

zmiana, którą proponują kolejne firmy, to ochrona przed masowym, niejawnym przeczesywaniem wirtualnych serwerów przez służby wywiadowcze.

IMPERIUM KONTRATAKUJE

Władze tolerowały ten wolnościowy trend – być może ze względu na oburzenie wywołane doniesieniami Edwarda Snowdena. Teraz zmieniły jednak zdanie: wystarczył jeden tragiczny incydent, by antyterrorystyczna retoryka i wszystko, co się z nią wiąże, wróciło z pełną mocą. Premier Wielkiej Brytanii publicznie skrytykował dostawców usług komunikacyjnych, których zabezpieczenia nie pozwalają na przechwycenie komunikacji: „Czy w naszym kraju naprawdę chcemy pozwolić na narzędzia umożliwiające taką komunikację między ludźmi, której nie możemy przechwycić?”. Wtóruje mu Barack Obama: „Jeśli mamy dowody na istnienie siatki terrorystycznej, znamy numer telefonu podejrzanej osoby, jej konto społecznościowe albo adres e-mail, a mimo to nie możemy zapoznać się z przekazywanymi komunikatami, to mamy problem”. Prezydent Obama zasugerował, że tę właśnie kwestię próbują rozgryźć firmy z Doliny Krzemowej, które w imię patriotyzmu przekazują dane NSA i FBI. Do ofensywy dołączyły też same służby bezpieczeństwa, domagając się zagwarantowania łatwego dostępu do zaszyfrowanej komunikacji elektronicznej (tzw. backdoor). Głos w tej debacie zabrali szef FBI, europejski koordynator antyterrorystyczny Gilles de Kerchove, dyrektor GCHQ i dyrektor NSA. Wszystkich połączyła jedna obawa: jeśli pozwolimy każdemu szyfrować komunikację, z pewnością skorzystają z tej możliwości również przestępcy i terroryści. Ta logika prowadzi donikąd: równie dobrze można by rozważyć zakaz swobodnego przemieszczania się (z pewnością korzystają z niego przestępcy), a już na pewno zakaz produkcji broni (z definicji służy do zabijania; cóż z tego, że czasem w obronie własnej).

Cytowane wystąpienia szefów rządów i służb trudno odczytać inaczej, niż jako próby wywarcia politycznego nacisku na firmy, które nie chcą ułatwiać masowej inwigilacji. Nawet,

jeśli nie wszystkie liczące się firmy ulegają tej presji, retoryka wpływowych polityków przebija się do głównego nurtu i inspiruje inne organy. I tak, na przykład w Hiszpanii grupa anarchistów została oskarżona o bezprawne działania m.in. dlatego, że korzystała z bezpiecznego serwisu e-mail (Riseup.net). Oskarżyciel oraz badający sprawę sędzia uznali, że sam fakt podejmowania wysiłku dla zachowania poufności komunikacji jest okolicznością obciążającą w sprawie.

To prosta droga do konstatacji, że każdy, kto zabezpiecza swoją komunikację, zasługuje na status podejrzanego. Dokładnie tą logiką posługują się służby wywiadowcze i policja w wielu krajach, wyodrębniając użytkowników takich usług jak TOR czy poczty e-mail z funkcją szyfrowania (jak OpenPGP) i przyglądając się ich aktywności z większą uwagą (tzw. „flagowanie"). W efekcie, osoby, które powinny wykorzystywać bezpieczną komunikację (np. dziennikarze, prawnicy, aktywiści walczący z autorytarnymi reżimami), stają przed trudnym dylematem: czy korzystać z popularnych i niezabezpieczonych narzędzi, ryzykując przechwycenie komunikacji, czy własnoręcznie umieścić się na celowniku służb?

Antyprywatnościowa ofensywa uderza też w graczy rynkowych. W Stanach Zjednoczonych pojawiły się pierwsze ataki prawne na firmy, które oferują i eksportują narzędzia umożliwiające skuteczne szyfrowanie. Departament Handlu USA nałożył 750 tys. dolarów kary na spółkę-córkę korporacji Intel. Dzięki dokumentom ujawnionym przez Edwarda Snowdena dowiedzieliśmy się też o licznych atakach technicznych służb brytyjskich i amerykańskich na protokoły zabezpieczające poufność komunikacji (TLS, SSL, SSH), które są wykorzystywane przez najpopularniejsze serwisy internetowe, oraz na prywatne, wirtualne sieci (VPN), które do tej pory uważane były za bezpieczny sposób zdalnego komunikowania się w ramach dużych firm i organizacji.

DO CZEGO TO WSZYSTKO PROWADZI?

Walka z narzędziami, które umożliwiają zaszyfrowaną lub anonimową komunikację, uderza w istotę prawa do prywatności – a w sferze komunikacji elektronicznej w zasadzie je eliminuje. Ze względu na techniczne zasady działania Internetu (gdzie każdy pakiet przechodzi przez wiele urządzeń i węzłów), jedyna szansa na zabezpieczenie treści komunikatu to jego zaszyfrowanie, a na zachowanie anonimowości – „zgubienie" numeru IP w sieci takiej jak TOR. Władza, która walczy z bezpieczną komunikacją, sama generuje nowe zagrożenia, nie tylko w sferze inwigilacji, ale również szeroko pojętej przestępczości. Z osłabionych zabezpieczeń równie chętnie, co brytyjskie, polskie czy amerykańskie służby, skorzystają chińscy i rosyjscy cyberżołnierze, ale też zwyczajni włamywacze. Wprowadzenie backdooru do oprogramowania czy osłabianie szyfrowania – tak by jedna służba miała dostęp do danych – nieuchronnie oznacza, że prędzej czy później z tej luki skorzystają też inni gracze. Rzeczywistą stawką w tej grze jest zatem nasze bezpieczeństwo – to samo, w imię którego władza odbiera nam kolejne sfery wolności i prywatności.

Ten paradoks unaocznił Edward Snowden. Wielokrotnie podkreślał, że rozwijając złośliwe oprogramowanie typu Stuxnet, eksploatując luki w bezpieczeństwie systemów informatycznych (Heartblead), łamiąc zabezpieczenia największych firm internetowych i wbudowując tzw. tylne drzwi w rozmaite urządzania i usługi, służby bardziej nas narażają, niż chronią. Przy czym skutki tych działań są dalekosiężne – użytkownicy tracą zaufanie do firm i serwisów; odpowiedzialni usługodawcy rezygnują z oferowania bezpiecznych rozwiązań, ponieważ czują, że nie są w stanie ich zagwarantować (kazus firmy Lavabit); aktywiści, dziennikarze i wszyscy, którzy promują lub wykorzystują bezpieczne narzędzia komunikacji – w tym organizacje pozarządowe – tracą grunt pod nogami.

POTRZEBUJEMY STOGU SIANA

Którędy prowadzi droga odwrotu z tej ślepej uliczki? Oczywiste wydaje się, że firmy internetowe pokroju Google, Apple czy

WhatsApp powinny zrobić wszystko, by odeprzeć polityczne ataki na podejmowane przez nie próby lepszego zabezpieczenia danych. Na uległości w tej sferze mogą tylko stracić. Ale to nie rozwiązuje problemu zwiększonej widoczności tych użytkowników, którzy – idąc wbrew trendowi – decydują się na korzystanie z takich narzędzi jak TOR czy OpenPGP. Z myślą o ich ochronie (przed inwigilacją, ujawnieniem źródeł dziennikarskich czy wręcz bezpośrednim zagrożeniem zdrowia i życia w krajach, gdzie trwa otwarty konflikt), każdy z nas powinien rozważyć podjęcie dodatkowego wysiłku, jakim niewątpliwie jest szyfrowanie czy korzystanie z TOR-a – bo w większym stogu siana trudniej znaleźć igłę. Rozwiązaniem najprostszym, z propozycją którego znowu wypada zwrócić się do biznesu, byłoby jednak zintegrowanie bezpiecznych narzędzi, takich jak OpenPGP, z najpopularniejszymi usługami (np. Gmail, Snapchat czy WhatsApp). W tak wielkim stogu siana namierzenie garstki osób, którym naprawdę zależy na bezpiecznej komunikacji, stanie się niemożliwe.

Autorstwo: Katarzyna Szymielewicz, Kamil Śliwowski
Źródło: Fundacja Panoptykon