Szyfruj z nami: bezpieczna komunikacja

20 listopada 2014

Najtrudniejsze w szyfrowaniu jest… przekonać się, że warto to robić. Korzyści – choć istotne – pozostają niewidoczne lub stają się odczuwalne dopiero po jakimś czasie, dlatego nie stanowią szczególnej zachęty do zmiany przyzwyczajeń. Bezpieczeństwo danych to dobry argument do szyfrowania maili służbowych, ale kogo miałyby interesować nasze sprawy osobiste? Ucieczka przed profilowaniem do celów komercyjnych? Przecież dzięki temu dostajemy bardziej spersonalizowane wyniki wyszukiwania i oferty dostosowane do swoich potrzeb. Zanim wyjaśnimy krok po kroku, jak szyfrować komunikację, postaramy się odpowiedzieć na pytanie: po co szyfrować.

KORZYŚCI Z SZYFROWANIA

Wielu specjalistów od bezpieczeństwa informacji dziwi się z kolei, dlaczego do szyfrowania w ogóle trzeba kogoś przekonywać. Nikt przecież nie kwestionuje korzyści z wysyłania listów w zamkniętych kopertach. Jednak szyfrowana komunikacja wymaga zmiany przyzwyczajeń i nie zawsze łączy się z pełną wygodą, zwłaszcza w przypadku osób, które korzystają z więcej niż jednego urządzenia do komunikowania się. Co więcej, trzeba przekonać drugą stronę, żeby również szyfrowała. Po co tyle zachodu? Jacob Appelbaum, współtwórca projektu Tor, przyrównał szyfrowaną komunikację do uprawiania seksu z zabezpieczeniem[1]: w danym momencie nie widać korzyści, ale za to jest szansa, że później nie spotka nas przykra niespodzianka. Cała trudność motywacyjna polega na tym, że – podobnie jak w powyższej analogii – korzyści są odłożone w czasie, a praktyczne utrudnienia odczuwalne od razu.

Jakkolwiek szyfrowanie jest czynnością techniczną, wiążą się z nim także pewne konsekwencje w znacznie szerszym wymiarze. Po

ujawnieniu przez Edwarda Snowdena informacji o programach masowej inwigilacji komunikacji elektronicznej nie powinno już budzić niczyjego zdziwienia (chociaż sprzeciw – owszem) to, że służby na całym świecie szczególną uwagę zwracają na usługi umożliwiające szyfrowanie. W czasach, kiedy „kto nie ma nic do ukrycia, nie ma czego się bać", osoby szyfrujące, a nawet tylko interesujące się szyfrowaniem, mogą stać się podejrzane.[2] Ale przecież nie ma nic złego w tym, że nie życzymy sobie, by osoby postronne czytały nasze listy. Wysyłanie korespondencji w zaklejonych kopertach, poufna rozmowa czy pisanie sekretnego pamiętnika raczej nie uchodzi za objaw działalności wywrotowej – naruszanie tajemnicy korespondencji uważa się za godzenie w wolności obywatelskie.

Szyfrowanie pozwala na „zapakowanie" komunikatu, żeby nie był widoczny gołym okiem dla osób postronnych. Większość szyfrujących decyduje się na nie z dwóch powodów: dla zasady chce zachować informacje o sobie w tajemnicy (prawo do tego gwarantuje im m.in. konstytucja) lub nie życzą sobie być obiektem targetowanych kampanii reklamowych (analizowanie treści komunikacji przez specjalnie do tego celu opracowane algorytmy pozwala na przypisanie każdemu użytkownikowi określonych cech; na ich podstawie dostosowywane są komunikaty, które mu się wyświetlają, od języka strony przez reklamy, po wyniki wyszukiwania). Szyfrowana komunikacja pomaga też prowadzić działalność opozycji i aktywistom na terenach ogarniętych konfliktem i wszędzie tam, gdzie rządy tłumią wolności obywatelskie. Oczywiście bywa też wykorzystywana do działalności przestępczej. Ale tak samo młotek może być użyty zarówno do wbijania gwoździ (w większości przypadków), jak i do zabójstwa (w skali marginalnej): trudno uznać to za powód wystarczający, by zacząć wydawać pozwolenia na posiadanie młotków i rejestrować wszystkich właścicieli.

SZYFROWANIE E-MAILI ZA POMOCĄ KLIENTA POCZTY

Decydując się na szyfrowanie poczty, musimy liczyć się z

kilkoma ograniczeniami i utrudnieniami. Przyzwyczailiśmy się, że jeśli tylko mamy swoją skrzynkę pocztową i e-mail adresata, nie ma nic prostszego, niż wysłać maila. Do szyfrowania zaś potrzebne jest zaangażowanie drugiej strony, która również musi szyfrować. Jeżeli ktoś ceni sobie korzystanie z wygodnego interfejsu swojej poczty w przeglądarce internetowej, może mieć kłopot z przesiadką na klienta poczty. Jeżeli korzystał z funkcji zapamiętywania raz wpisanego hasła przez system operacyjny, będzie musiał zmienić ten nawyk i zapamiętać przynajmniej jedno hasło. Jeśli korzystał z wielu urządzeń do wysyłania i odczytywania poczty, będzie musiał ograniczyć ich liczbę, szyfrować tylko niektóre wiadomości lub odpowiednio skonfigurować każde urządzenie.

Czy korzyści z szyfrowania przewyższają te „koszty transakcyjne”? Nieprzekonanych zachęcamy do spróbowania. Jak to zrobić?

KROK 1: SKONFIGURUJ KLIENTA POCZTY

Mechanizm szyfrowania i podpisywania poczty, nazywany jest OpenPGP (akronim PGP oznacza Pretty Good Privacy). Najczęściej stosowane, a przy tym najprostsze, rozwiązanie to instalacja specjalnej wtyczki w programie pocztowym. Dlatego przygodę z szyfrowaniem najłatwiej będzie rozpocząć osobom, które korzystają z jednego komputera, a komunikację e-mailową prowadzą nie za pomocą przeglądarki internetowej, a specjalnego programu do czytania i wysyłania maili, tzw. klienta poczty.

Nie wszystkie programy pocztowe obsługują mechanizm OpenPGP, ale w zależności od systemu operacyjnego komputera, dostępnych jest kilka opcji:

– Mozilla Thunderbird (Windows, Linux, Mac OS, szyfrowanie jest możliwe po zainstalowaniu wtyczki Enigmail),

– KMail (Linux),

– Evolution (Linux, Windows),

– Claws Mail (Linux, Windows),

– Apple Mail (Mac OS, po zainstalowaniu pakietu narzędzi GPGTools).

Instrukcję, jak skonfigurować pocztę w wybranym programie, można znaleźć na stronie producenta lub w pomocy. W sieci znajduje się wiele instruktaży wideo „dla opornych”. Do konfiguracji konieczne będzie też zalogowanie się do poczty w przeglądarce w internetowej, gdzie można znaleźć nazwę serwera obsługującego pocztę przychodzącą i wychodzącą oraz zmienić ustawienia dostępu przez POP3/IMAP.

KROK 2: ZAINSTALUJ WTYCZKĘ SZYFRUJĄCĄ

W skonfigurowanym kliencie poczty należy zainstalować wtyczkę (inaczej: rozszerzenie, dodatek), która umożliwi obsługę mechanizmu szyfrowania. Dla Mozilla Thunderbird wtyczka ta nazywa się Enigmail, dla Apple Mail – GPGTools.

KROK 3: WYGENERUJ PARĘ KLUCZY

Do szyfrowania poczty niezbędna jest para kluczy: klucz publiczny adresata służy do weryfikacji podpisu nadawcy wiadomości przychodzącej i do zaszyfrowania wiadomości wychodzącej (nadawca musi znać klucz publiczny adresata, żeby wysłać do niego zaszyfrowaną wiadomość). Klucz prywatny odwrotnie: służy do podpisania wiadomości wychodzącej i do odszyfrowania przychodzącej (odbiorca ma pewność, że nadawca jest tym, za kogo się podaje; odbiorca może odszyfrować otrzymaną wiadomość).

Przez proces generowania kluczy użytkownika poprowadzi kreator, który będzie dostępny w programie pocztowym po instalacji wtyczki szyfrującej. Jeden z kroków to ustawienie hasła. Warto zwrócić uwagę, żeby było to hasło bezpieczne, znane tylko użytkownikowi.

Przy generowaniu kluczy pojawi się również możliwość wygenerowania tzw. certyfikatu rewokacji, który będzie niezbędny do likwidacji klucza w razie utraty hasła do niego. Certyfikat rewokacji warto zapisać dodatkowo na zewnętrznej pamięci, tak aby mieć do niego dostęp w razie utraty lub awarii komputera.

KROK 4: DO TANGA TRZEBA DWOJGA

Do szyfrowania komunikacji potrzebna jest współpraca drugiej strony: adresat musi przejść te same kroki, co nadawca, żeby móc odczytywać i wysyłać szyfrowane wiadomości. Osoby niekorzystające z szyfrowania warto zachęcić do podjęcia tego wysiłku, choćby informując, że można się z nami komunikować w ten sposób. Do dyspozycji mamy co najmniej dwie metody – polecamy zastosowanie obydwu jednocześnie:

– Umieść klucz publiczny na serwerze kluczy. Możesz to zrobić poprzez menadżer kluczy OpenPGP w kliencie poczty. W ten sposób każdy, kto będzie chciał wysłać do Ciebie zaszyfrowaną wiadomość, będzie mógł to łatwo zrobić, pobierając Twój klucz publiczny z serwera.

– Popularyzuj ideę szyfrowania. Na przykład zespół Fundacji Panoptykon zachęca innych do szyfrowania poczty hasłem „Szyfruj ze mną! Mój klucz publiczny to: …” w stopce wysyłanych wiadomości. W ten sposób informujemy osoby, z którymi się komunikujemy, że mogą nam bezpiecznie wysyłać informacje.

SZYFROWANIE E-MAILI PRZEZ PRZEGLĄDARKĘ I URZĄDZENIA MOBILNE

Szyfrowanie za pośrednictwem klienta poczty jest najpowszechniejszym i najbezpieczniejszym rozwiązaniem, ale nie jedynym. Dodatek Mailvelope umożliwia szyfrowanie poczty w przeglądarce internetowej. Minus tego rozwiązania: wiadomości szyfrowane są dopiero przy wysyłce. Oznacza to, że wersje robocze automatycznie zapisywane na serwerze dostawcy poczty (np. Google, Wirtualna Polska) są odszyfrowane. Mówiąc w

uproszczeniu, wiadomości nie będzie mogła odczytać osoba nie będąca jej adresatem, ale dostawca (lub podmiot mający dostęp do jej serwerów, np. amerykańska NSA) będzie mógł przeanalizować wersję roboczą naszego maila i na jej podstawie podsunąć nam spersonalizowaną reklamę (lub uznać nas za obiekt bardziej lub mniej podejrzany).

Specjaliści od bezpieczeństwa informacji odradzają szyfrowanie e-maili za pośrednictwem urządzeń mobilnych (smartfonów, tabletów), które dużo łatwiej utracić (a wraz z nimi klucze OpenPGP) niż chociażby laptop. Zdecydowanie lepiej ściągnąć aplikację TextSecure do wysyłania szyfrowanych SMS-ów albo skorzystać z szyfrowanego czatu (w wersji mobilnej np. Xabber). Jeśli jednak komuś bardzo zależy na obsłudze szyfrowanej poczty za pomocą telefonu, na urządzeniach mobilnych można zainstalować klienta K-9 Mail oraz współpracującą z nim aplikację szyfrującą APG. Dla tych, którzy chcą mieć swoją pocztę zawsze pod ręką, ale niekoniecznie na laptopie czy komórce, rozwiązaniem będzie Thunderbird Portable, który wraz z wtyczką Enigmail umożliwi komunikację szyfrowaną uruchamianą ze zwykłego pendrive'a.

SZYFROWANY CZAT

Standardem szyfrowania rozmów prowadzonych przez komunikatory internetowe (ang. IM, instant messenger) jest protokół Off-The-Record (często nazywany w skrócie OTR). Jeśli jest zainstalowany na komunikatorach obu rozmówców, szyfrowana rozmowa nawiązywana jest automatycznie. Tym bardziej warto więc poświęcić chwilę czasu na skonfigurowanie swojego komunikatora – może okazać się, że niektórzy nasi znajomi już korzystają z szyfrowanego czatu.

Jednym z najpopularniejszych komunikatorów jest Pidgin (dla systemów Windows i GNU/Linux; odpowiednikiem dla Mac OS jest Adium). Po instalacji komunikator poprosi nas o skonfigurowanie konta. Jeśli jesteśmy zarejestrowani w usługach Google'a lub Facebooka, możemy wykorzystać je do

czatowania, jednak musimy liczyć się z tym, że nasze nieszyfrowane rozmowy mogą zostać użyte do celów marketingowych tych firm. Zdecydowanie lepiej założyć konto Jabber/XMPP na jednym z wielu darmowych serwerów (np. jabber.ccc.de, jabber.org, chrome.pl; lista publicznych serwerów) – umożliwi nam to kreator przy pierwszym uruchomieniu komunikatora.

Na koniec potrzebujemy jeszcze ściągnąć i zainstalować wtyczkę Off-The-Record (Adium jest w nią domyślnie wyposażony) oraz wygenerować klucz OTR w ustawieniach komunikatora – dokładne instrukcje można znaleźć na stronach pomocy Pidgin/Adium. Od tej chwili możemy cieszyć się szyfrowanymi rozmowami. Jeśli nasi rozmówcy jeszcze nie używają OTR, warto ich do tego zachęcić, podsyłając ten artykuł.

W przypadku urządzeń mobilnych popularnymi komunikatorami z obsługą Off-The-Record są Xabber (dla Android) oraz ChatSecure (Android oraz iOS). Ich konfigurowanie jest analogiczne do Pidgina.

HIGIENA KORZYSTANIA Z URZĄDZEŃ ELEKTRONICZNYCH

Stosowanie mechanizmu szyfrowania jest najlepszym możliwym zabezpieczeniem poufności komunikacji, ale nie zadziała, jeżeli nie zachowamy podstawowych zasad dotyczących „higieny" korzystania z komputerów i innych urządzeń. Należy do nich na przykład aktualizowanie systemu operacyjnego i oprogramowania (m.in. przeglądarki internetowej oraz programu pocztowego), instalacja dobrego programu antywirusowego, przechowywanie haseł w sposób bezpieczny, instalowanie oprogramowania z zaufanych źródeł. Warto również zdecydować się na szyfrowanie danych zapisywanych na urządzeniach, z których korzystamy. Jak to zrobić? Podpowiemy już w kolejnym tekście poświęconym szyfrowaniu.

Autorzy: Anna Obem, Michał „czesiek" Czyżewski
Współpraca: Małgorzata Szumańska

Źródło: Fundacja Panoptykon

PRZYPISY

[1] Let’s talk about sex baby, lets talk about PGP https://www.youtube.com/watch?v=BBgZyV4iltw

[2] http://boingboing.net/2014/07/03/if-you-read-boing-boing-the-n.html