**Sieć jest twoja, bądź jej panem**

Michał „Rysiek” Woźniak

Źródło: <http://m.wyborcza.pl/wyborcza/1,132749,14264762,Siec_jest_twoja__badz_jej_panem.html>

Gdy wysyłamy pocztą list, wkładamy go do koperty. W oknach mamy firanki. Nie rozmawiamy na ulicy głośno o sprawach prywatnych. Dlaczego nie trzymamy się tych zasad w sieci?

PRISM, ujawniony niedawno amerykański program podsłuchiwania komunikacji elektronicznej, nie jest niczym nowym. Kilkanaście lat temu podobne, choć nieco mniejsze, emocje wywoływał program Echelon, globalna sieć wywiadu elektronicznego. Rządy zawsze chciały mieć dostęp do naszej komunikacji. Tyle że dziś mają po temu możliwości techniczne. Nikt prócz nas samych nie zadba dobrze o bezpieczeństwo naszych danych, co potwierdza współpraca z PRISM największych firm z branży IT.

**Cyfrowa higiena**

Bezpieczeństwo często nie idzie w parze z wygodą. Przyzwyczajamy się jednak do pewnych uciążliwości życia codziennego - jak pasy bezpieczeństwa czy mycie rąk przed posiłkami - w imię zabezpieczenia naszego życia i zdrowia. Powinniśmy mieć podobne nawyki dotyczące naszej „higieny informacyjnej”.

Gdy wysyłamy pocztą ważne dokumenty (albo zwykły list), wkładamy je w kopertę, by nikt nie mógł ich przeczytać bez pozostawiania śladów. W oknach mamy firanki. Nie rozmawiamy o wrażliwych sprawach prywatnych głośno i w miejscach publicznych. Nie wynika to z chęci ukrycia jakichś niecnych sprawek, lecz z poczucia, że prywatność trzeba chronić. Tego poczucia i nawyków zupełnie nie przenosimy jednak na komunikację elektroniczną. Czas zacząć.

Przykładem podstawowej higieny w domenie cyfrowej jest wylogowywanie się z usług, z których nie korzystamy. Skończyliśmy sprawdzać swoje konto pocztowe? Nie korzystamy w danej chwili z portalu społecznościowego? Wylogujmy się i wyczyśćmy „ciasteczka” (cookies - patrz niżej) - każda przeglądarka na to pozwala. Warto też zadbać o takie ustawienia - np. w preferencjach przeglądarki - by „ciasteczka” akceptowane były tylko na konkretną sesję, a zatem automatycznie czyszczone po zamknięciu przeglądarki. Tak, oznacza to, że następnym razem będzie trzeba zalogować się ponownie. Za cenę paru sekund uzyskujemy jednak to, że zdecydowanie trudniej będzie połączyć nasze nawyki czy miejsca, które odwiedzamy w sieci, z naszym kontem.

Jeżeli chcemy być wyjątkowo higieniczni, korzystajmy z tzw. trybu prywatnego. Dostępny jest w każdej przeglądarce (zwykle w głównym menu) i pozwala stworzyć nową, oddzielną sesję, która po zamknięciu przeglądarki jest całkowicie czyszczona. Warto zastanowić się nad korzystaniem z tego trybu w przypadku m.in. stron banków, zakupów w internecie czy nawet sieci społecznościowych.

**Firanki**

Przeglądarka internetowa to dziś coraz częściej nasze najważniejsze okno na świat. Okno jednak powinno służyć nam samym do wyglądania na zewnątrz, nie zaś obcym do obserwowania nas. Niestety, podczas korzystania z internetu śledzeni jesteśmy niemal bez przerwy. „Ciasteczka”, przyciski „Lubię to”, reklamy ładowane z zewnętrznych serwerów dużych firm reklamowych, historia naszego wyszukiwania - wszystko to pozwala budować niepokojąco dokładny profil użytkownika sieci.

Przede wszystkim zatem warto zastanowić się nad wyborem samej przeglądarki. Te tworzone przez wielkie korporacje, opierające swoje modele biznesowe na śledzeniu użytkowników i sprzedaży ich danych (jak Google'owy Chrome, Internet Explorer Microsoftu czy Safari firmy Apple), mogą nie być najszczęśliwszym wyborem. Znacznie lepiej przesiąść się na wolne i otwarte, rozwijane przez społeczność przeglądarki jak Mozilla Firefox (przez lata najpopularniejsza przeglądarka w Polsce) czy projekt Chromium (Chrome bez śledzących modyfikacji Google'a).

Wymiana naszych cyfrowych okien na świat na szczelniejsze to pierwszy krok; drugim jest zawieszenie w nich „firanek”. Najłatwiej to zrobić za pomocą kilku rozszerzeń, czyli modyfikacji, które można łatwo zainstalować w przeglądarce, by dostosować ją do naszych potrzeb. Rozszerzenia pobrać można zwykle ze strony twórców przeglądarki, której używamy. Zacząć można od rozszerzenia AdBlock Plus - usuwając reklamy ze stron, które przeglądamy, usuwa ono przy okazji jedną z podstawowych metod śledzenia nas w internecie. Nie dość zatem, że dostajemy strony bez irytujących często reklam - dbamy jeszcze o swoją prywatność.

„Ciasteczka”, czyli niewielkie informacje zapisywane „na prośbę” stron internetowych przez przeglądarkę, są niezbędne np. do obsługi logowania się czy preferencji użytkowników na stronach internetowych. Są też jednak podstawowym mechanizmem używanym do ich śledzenia. Rozszerzenie CookieMonster pozwoli nam decydować, które strony i na jak długo mogą ustawiać „ciasteczka”.

Rozszerzenie to powinno być jednym z podstawowych narzędzi każdego dbającego o cyfrową higienę internauty. Rozszerzenie HTTPS Everywhere wymusza stosowanie szyfrowania na wszystkich połączeniach do stron internetowych, które to szyfrowanie wspierają. Gdy nasza przeglądarka kontaktuje się ze stroną internetową, by móc ją nam wyświetlić, zarówno zapytanie przeglądarki, jak i odpowiedź serwera podróżują przez szereg węzłów w sieci. Szyfrowanie HTTPS dba o to, by treść tej komunikacji dostępna była tylko dla nas i dla serwera, uniemożliwiając czytanie po drodze.

Przyzwyczailiśmy się do wszechobecnych przycisków typu „Lubię to”, pozwalających nam w łatwy sposób dzielić się czytanymi materiałami w sieciach społecznościowych. Niestety, przyciski te służą przede wszystkim do śledzenia nas (i to niezależnie od tego, czy jesteśmy zalogowani na odpowiedni portal społecznościowy czy nie). Rozszerzenie Ghostery pomaga wykrywać i kontrolować takie elementy stron służące do śledzenia użytkowników.

**Małe kroki też się liczą**

Wraz ze wzrostem naszych oczekiwań dotyczących ochrony bezpieczeństwa i prywatności w sieci wzrasta skomplikowanie techniczne rozwiązań, które trzeba w tym celu zastosować. Np. maile stale wysyłamy w formie niezaszyfrowanej - to tak jakbyśmy wysyłali pocztówki zamiast listów: każdy pracownik poczty mógłby je przeczytać, tak jak nasze maile dostępne są dla każdego administratora urządzeń, przez które nasze maile „przechodzą”. Jeszcze większym problemem są scentralizowane sieci społecznościowe, gdzie oddajemy de facto pełną kontrolę nad naszą komunikacją (razem z pełną jej treścią) jednej konkretnej firmie (jak Facebook czy Twitter). Mało tego - na co dzień większość z nas korzysta z zamkniętego oprogramowania, którego działania nie możemy sprawdzić ani ulepszyć, a które (jak się wielokrotnie okazywało) często śledzi nasz każdy krok.

Przy czym do firm, które, jak się okazało, współpracują z projektem PRISM, należą zarówno te oferujące popularne usługi poczty elektronicznej (jak Google), obsługujące scentralizowane sieci społecznościowe (Facebook), jak i tworzące zamknięte oprogramowanie (Apple i Microsoft).

Maile możemy szyfrować, scentralizowane sieci społecznościowe zastąpić zdecentralizowanymi, wolnymi i otwartymi odpowiednikami (jak Diaspora czy Friendica), zamiast zamkniętego oprogramowania możemy korzystać z wolnych i otwartych odpowiedników. Każdy z tych kroków wymagać od nas będzie więcej wiedzy, czasu i samozaparcia.

Coraz częściej powstają inicjatywy oferujące w tym pomoc - jak Linux w Laboratorium Technik Mobilnych Brama, Warszawskim Hackerspace czy projekt Edukacja Medialna.

Nie jesteśmy w stanie osiągnąć w sieci stuprocentowej ochrony. Nie szkodzi - przecież zwykłe mydło jest mniej skuteczne od środków bakteriobójczych, ale regularne korzystanie z niego wydatnie (i zwykle wystarczająco) ogranicza zagrożenie. W codziennym korzystaniu z internetu już wprowadzenie podstaw higieny informacyjnej i zawieszenie „firanek” znacznie utrudni śledzenie naszego każdego kroku.