Szpieg w wersji smart

24 października 2014

Kogo znamy i z kim się przyjaźnimy; gdzie i z kim jesteśmy – w dzień i w nocy; czym się interesujemy; czego nie wiemy, a próbujemy się dowiedzieć; co planujemy: gdzie wybieramy się po pracy czy na urlop – to wszystko (i znacznie więcej) wie o nas szpieg tak mały, że mieści się w dłoni: nasz własny telefon w wersji smart. Mimo to kto raz zaczął z niego korzystać, łatwo się z nim nie rozstanie. Co warto wiedzieć o smartfonie, by używać go bardziej świadomie? Odpowiedź znajdziesz w tym tekście.

Rozwój telefonów komórkowych zmienił nasze życie. Najpierw z budek telefonicznych i zaciszy mieszkań wślizgnęły się one do naszych torebek i kieszeni, dając nam możliwość komunikacji na odległość z niemal dowolnego miejsca. A to był dopiero początek. Stałe podłączenie do Internetu i techniczne zaawansowanie urządzeń radykalnie zwiększyło nasze możliwości komunikacji ze światem, zdobywania informacji, dokumentowania tego, co dzieje się wokół i dzielenia się tym z innymi. Współczesny smartfon to zupełnie inne urządzenie niż komórka sprzed dekady. Rzadko jednak zastanawiamy się nad tym, jak wiele informacji na nasz temat zbiera. A jeszcze rzadziej – z kim się nimi dzieli.

POZIOM 1. COŚ WIĘCEJ NIŻ PIĘĆ CALI POŻĄDANIA

Niedawna premiera 6. generacji iPhone’ów pokazała, jakie emocje potrafi rozpalić mały elektroniczny gadżet. Na pierwszy rzut oka smartfon składa się głównie z… wyświetlacza. Jednak to, co producent telefonu ukryje głębiej, jest kluczowe nie tylko z punktu widzenia jego funkcjonalności, ale również ochrony naszej prywatności. Każdy smartfon wyposażony jest w procesor zawiadujący połączeniami i innymi działaniami telefonu oraz fizyczną pamięć (dysk i kartę pamięci), na której zapisywane są wszystkie te operacje. Ważnym elementem

telefonu jest bateria, która karmi coraz bardziej energochłonne urządzenie i utrzymuje je w kontakcie ze światem. Standardem staje się integracja baterii z resztą telefonu, co nie tylko stanowi utrudnienie w razie awarii (nie można wymienić baterii), ale też ogranicza naszą kontrolę nad urządzeniem (trudniej zabezpieczyć się przed namierzeniem czy podsłuchem).

Wiele elementów współczesnego telefonu służy zbieraniu informacji ze świata zewnętrznego. Poza mikrofonem, kamerą i aparatem smartfony wyposażone są m.in. w żyroskopy, czujniki światła, a nawet czytniki odcisków palca. Dzięki antenom są w stanie nie tylko odbierać sygnał komórkowy, ale także określać nasze położenie za pomocą sygnału satelitarnego (GPS) i komunikować się z innymi urządzeniami. To dzięki temu mamy możliwość korzystania w telefonie z domowego Internetu (Wi-Fi) czy płacenia za zakupy (NFC). Wszystkie te elementy smartfona są w stanie zbierać i udostępniać informacje, nawet gdy wydaje nam się, że je wyłączyliśmy. Dlatego tak ważne jest dokładne zapoznanie się z ustawieniami telefonu (np. Wi-Fi, GPS, Bluetooth, polecenia głosowe), zanim zaczniemy z niego skorzystać.

Telefon zabieramy ze sobą niemal wszędzie, więc dość łatwo może on wpaść w niepowołane ręce. Problemem staje się wówczas nie tylko utrata cennego gadżetu, ale przede wszystkim fakt, że tracimy kontrolę nad ogromem wrażliwych informacji na nasz temat. Opcją minimum jest ograniczenie dostępu do telefonu (np. PIN-em). Warto również zabezpieczyć hasłami dostępy do najważniejszych aplikacji (np. pocztowej) oraz zaszyfrować pamięć telefonu. I – co równie ważne – powściągliwie korzystać z urządzenia: nie robić zdjęć i nagrań w intymnych sytuacjach, nie przechowywać dokumentów zawierających wrażliwe informacje.

POZIOM 2. KTO MA OPROGRAMOWANIE, TEN MA WŁADZĘ

Oprogramowanie instalowane w smartfonie (np. Android, iOS, Windows Phone) decyduje o jego działaniu. Ten kto sprawuje nad

nim kontrolę – przede wszystkim producent oprogramowania (odpowiednio: Google, Apple, Microsoft) – jest prawdziwym panem naszego telefonu. I nie waha się ze swojej władzy korzystać. Google'owi zdarzało się na przykład odgórnie wyłączyć wszystkim użytkownikom funkcję blokowania dostępu poszczególnych aplikacji do danych i czujników w telefonie z Androidem 4.4. Producent oprogramowania ma również najłatwiejszy i najszerszy dostęp do informacji, które są generowane w trakcie korzystania ze smartfona.

Urządzenie i zainstalowane na nim oprogramowanie są ze sobą ściśle związane. Najwyraźniej widać to w przypadku iPhone'ów: tu wszystkie karty rozdaje jeden producent – firma Apple. Jednak ten związek występuje również w przypadku innych smartfonów: producenci telefonów ingerują w to, co jest instalowane na ich sprzęcie, na przykład tak modyfikują oprogramowanie, by wyłączenie niektórych programów nie było możliwe. Dlatego Android w telefonie LG jest czymś innym niż Android w wersji Samsunga czy HTC.

Trudno ograniczyć kontrolę producentów telefonu i oprogramowania nad naszym urządzeniem. Bardziej zdeterminowani użytkownicy smartfonów z Androidem mogą zainstalować alternatywną wersję systemu operacyjnego (np. CyanogenModa), a posiadacze iPhone'ów zdecydować się na tzw. root, czyli zdjęcie zabezpieczeń, które zabraniają instalacji aplikacji spoza sklepu firmy.

POZIOM 3. EKOSYSTEM APLIKACJI

Korzystanie z funkcjonalności smartfona możliwe jest w praktyce dzięki aplikacjom. Część z nich instalowana jest przez producenta telefonu – warto je przejrzeć po zakupie aparatu i odinstalować te, z których nie mamy zamiaru korzystać (o ile jest to możliwe). Pozostałe ściągamy sami. Podczas instalacji nowej aplikacji otrzymujemy informację, do jakich danych i funkcji telefonu będzie ona miała dostęp. Większość komunikatów jest bardzo ogólna, co utrudnia

zrozumienie, jak naprawdę działa program i jak zebrane przez niego dane mogą zostać wykorzystane w przyszłości. Tymczasem na przykład dostęp aplikacji do mikrofonu w najnowszych urządzeniach z systemami Android i iOS umożliwia ich ciągły nasłuch w oczekiwaniu na komendy głosowe. Dlatego warto uważnie wczytywać się w informację udostępniane przy instalacji, a także szukać recenzji aplikacji i wybierać te, które nie wymagają dostępu do zbędnych danych, a przede wszystkim nie wysyłają ich na serwery producentów.

Najprostszą metodą ściągnięcia aplikacji jest skorzystanie z oficjalnego sklepu. To rozwiązanie ma swoje zalety, ale też wady. Z jednej strony niesie mniejsze ryzyko pobrania zawirusowanego programu (częściowo możemy się przed nimi chronić, instalując program antywirusowy). Z drugiej jednak trudno znaleźć tam aplikacje naprawdę przyjazne dla prywatności. Zdarzało się, że Google i Apple usuwały ze swoich sklepów programy blokujące reklamy (np. popularne dodatki do przeglądarek AdBlock czy Disconnect). Co więcej, firmy te obligują producentów aplikacji korzystających z ich sieci dystrybucji do zasysania informacji o użytkownikach (wykorzystywanych później np. do celów statystycznych), nawet wówczas gdy sami producenci tych danych nie potrzebują.

Przy ściąganiu aplikacji warto zwracać uwagę na to, jakimi danymi się posługujemy. Ze smartfonem nigdy nie będziemy anonimowi, ale z punktu widzenie bezpieczeństwa informacji dobrym rozwiązaniem jest skonfigurowanie telefonu z wykorzystaniem nowego adresu e-mail (a nie naszego najważniejszego konta) oraz unikanie wykorzystywania tych samych danych dostępowych (np. konta Gmail) do wszystkich programów instalowanych na telefonie. Utrudnia to wymianę danych między firmami, integrowanie informacji na nasz temat i profilowanie.

POZIOM 4. ŻYCIE W CHMURZE

Zapisując na telefonie kolejne filmy, zdjęcia i setki innych

informacji, nie każdy myśli o tym, że mogą one trafiać również na serwery znajdujące się na drugim końcu świata. Tymczasem coraz częściej kopie zapasowe wszystkich zbieranych na smartfonie danych są tworzone w chmurze przez producentów oprogramowania. Daje to nam możliwość sięgnięcia po te informacje z dowolnego urządzenia, a w przypadku utraty telefonu pomaga je odzyskać i przenieść na nowy aparat. Niestety w praktyce rozwiązanie to niesie poważne zagrożenia: poza naszą kontrolą gromadzony jest ogrom cennych informacji na nasz temat. Boleśnie przekonało się o tym kilka amerykańskich aktorek, których intymne zdjęcia zostały wykradzione z iClouda i trafiły do sieci.

Podobne problemy dotyczą zapisywania w chmurze danych pochodzących z poszczególnych aplikacji. Jak się przed nimi wszystkimi zabezpieczyć? Warto zwrócić uwagę na ustawienia programów oraz zapisywania kopii zapasowych telefonu i zablokować możliwość ich gromadzenia w chmurze. Zamiast tego można samodzielnie robić back up-y danych na swoim komputerze lub zewnętrznym dysku. To trochę bardziej pracochłonne rozwiązanie, ale zdecydowanie bezpieczniejsze.

WIERZCHOŁEK GÓRY LODOWEJ

To jeszcze nie koniec układanki. Używając smartfona, korzystamy z sieci komórkowej oraz Internetu. Dlatego informacje o naszych połączeniach telefonicznych i internetowych gromadzone są przez operatorów. Nie możemy zapominać również o administratorach stron internetowych i współpracujących z nimi reklamodawcach, którzy zbierają informacje na temat odwiedzanych przez nas stron, zapisują hasła do witryn internetowych, profilują serwowane nam reklamy. Jeśli zależy nam na ograniczeniu udostępnianych im informacji, powinniśmy pamiętać o odpowiednich ustawieniach przeglądarek, z których korzystamy w telefonie. Warto też zadbać o szyfrowanie swojej komunikacji: poczty e-mail, SMS-ów (np. dzięki aplikacji TextSecure) i połączeń (np. za pomocą RedPhone’a).

Jeśli jakaś firma gromadzi informacje na nasz temat, zawsze mogą po nie sięgnąć instytucje państwowe. Polskim służbom najłatwiej uzyskać dane telekomunikacyjne (np. billingi, dane geolokalizacyjne). Operatorzy mają obowiązek przechowywać je przez 12 miesięcy i udostępniać na żądanie uprawnionych podmiotów. Odbywa się to bez jakiejkolwiek zewnętrznej kontroli, często za pomocą specjalnego interfejsu umożliwiającego łatwe ściąganie danych bez udziału operatora. Dlatego służby najchętniej korzystają z tej właśnie możliwości. Oprócz tego mogą zwracać się o udostępnienie innych rodzajów danych do firm, które są w ich posiadaniu, np. producenta oprogramowania zainstalowanego w naszym telefonie czy administratora strony internetowej, na którą wchodziliśmy. Dostęp do danych generowanych za pomocą telefonu mają również służby innych państw, w tym amerykańska NSA. Niestety ta wyspecjalizowana w uzyskiwaniu informacji od amerykańskich korporacji agencja nie jest prawnie zobligowana do poszanowania prawa do prywatności nie-Amerykanów.

Jak widać, nie na wszystkie problemy związane z korzystaniem z telefonu jesteśmy w stanie odpowiedzieć w pojedynkę. Świadome zarządzanie ustawieniami swojego urządzenia to tylko jeden z elementów prywatnościowej układanki. Co jeszcze możesz zrobić?

1. Dziel się wiedzą na temat świadomego korzystania z telefonu ze swoją rodziną i przyjaciółmi.

2. Wyłącz telefon, jeśli go nie potrzebujesz; zostaw go w domu, gdy zależy ci na zachowaniu poufności.

3. Wspieraj działania na rzecz lepszego prawa. Jest o co walczyć.

Autor: Małgorzata Szumańska, Kamil Śliwowski
Źródło: Fundacja Panoptykon