

Koń trojański wpuuszczony do smartfona

Wojciech Rafał Wiewiórowski Proponujemy wprowadzenie do rozporządzenia UE dotyczącego ochrony danych osobowych zasad podobnych do obowiązujących w ochronie konsumentów

Grupa Robocza Art. 29, czyli zgromadzenie skupiające pana odpowiedników ze wszystkich krajów UE, właśnie sporządziła opinię na temat smartfonów i związanych z nimi zagrożeń dla ochrony danych osobowych. Dlaczego zajęliście się tym problemem?

Tak naprawdę opinia bardziej dotyczy aplikacji mobilnych. To one stwarzają zagrożenie dla naszej prywatności. Coraz więcej aplikacji znajduje się w telefonach już w chwili, gdy je kupujemy. Coraz więcej aplikacji sami też instalujemy. Później orientujemy się, że nasz smartfon wysłał gdzieś zgromadzone na nim dane, a my nie wiemy, co wysłał, nie wiemy dokąd, nie wiemy po co. Grupa Robocza Art. 29 uznała, że stwarza to zagrożenie dla naszej prywatności. Dlatego przez rok prowadziła badania dotyczące aplikacji mobilnych.

I jakie wnioski wynikają z tych badań?

Bardzo interesujące. Okazało się chociażby, że operatorzy telekomunikacyjni, od których przecież najczęściej kupujemy smartfony, sami nie wiedzą, jakie dane są transmitowane i dokąd. Charakterystyczny jest sposób zachowania niektórych operatorów, gdy abonenci składają reklamację dotyczącą zawyżonego ich zdaniem transferu danych. Otóż zdarza się, że nie odpowiadają na nie w terminie, prawdopodobnie dlatego, by nie musieć tłumaczyć, jakie dane i dokąd były transmitowane.

Można powiedzieć, że instalując aplikacje, często przecież darmowe, godzimy się na ograniczenie naszej prywatności. Tak, ale powinniśmy to robić świadomie. Tymczasem twórcy czy dystrybutorzy aplikacji nie informują nas, co one tak naprawdę robią. Kupujemy po trosze kota w worku, a może nawet konia trojańskiego.

Badaliście, jakie informacje o użytkownikach smartfonów są zbierane?



Dr Wojciech Rafał Wiewiórowski, generalny inspektor ochrony danych osobowych

Najczęściej dane lokalizacyjne, czyli to, w jakim miejscu znajdujemy się w danej chwili, oraz podstawowe informacje dotyczące samego użytkownika. Jednak ani operatorzy, ani dostawcy usług nie są w stanie dokładnie określić, czy też nie chcą określić, co zawierają te transmisje. Argumentują, że osoba, która używa aplikacji, wyraziła zgodę na to, że może ona przesyłać pewne informacje.

A rzeczywiście się zgodziła?

Teoretycznie tak, bo kliknęła jakiś potwierdzenie podczas instalacji czy uruchomienia aplikacji. Praktycznie jednak trudno mówić o świadomej decyzji, bo zazwyczaj użytkownik jest zainteresowany jak najszybszym skorzystaniem z usługi i nie zwraca uwagi na to, co potwierdza. Zgodnie z przepisami, zarówno polskimi, jak i europejskimi, o zgodzie możemy zaś mówić tylko wtedy, gdy została ona udzielona dobrowolnie, przez prawidłowo poinformowaną osobę. Do tej drugiej części mam największe wątpliwości. Czy osoba, która decyduje się na używanie danej aplikacji, rzeczywiście jest świadoma, na co się godzi.

Jakieś informacje są jej przedstawiane podczas instalacji, tyle że często w taki sposób, że nawet średnio zaawansowany użytkownik nie jest w stanie ich zrozumieć. Niepokój budzi przede wszystkim zakres informacji, który jest podawany, oraz to, czy konsument rzeczywiście dysponuje pełną wiedzą dotyczącą tego, na co się godzi, a więc czy robi to świadomie. Podam przykład – jeżeli zsynchronizujemy naszego smartfona z komputerem pokładowym w samochodzie, to powinniśmy zdawać sobie sprawę z tego, że chociaż chcemy jedynie mieć dostęp do muzyki, to w rzeczywistości przesyłamy dane z naszego kalendarza, z naszego spisu adresów i inne informacje zapisane w pamięci naszego smartfona. Dostęp do nich może mieć każdy pracownik serwisu, w którym naprawiamy swój samochód.

Wiemy już, że nie jest najlepiej.

Czy to wina złego prawa?

Tak bym tego nie ocenił, bo zwiększenie ochrony prywatności i świadomości użytkowników można osiągnąć na podstawie obowiązujących przepisów. Kluczowa jest tu kwestia dopełniania obowiązku informacyjnego i tego, by wszyscy do tego zobowiązani zdawali sobie z niego sprawę. Zacząć trzeba od uświadomienia tego twórcom aplikacji mobilnych, tym bardziej że często nie są to duże firmy, lecz wręcz pojedyncze osoby. Na przykład Polacy są bardzo aktywni na tym rynku. Muszą oni mieć świadomość, że tworzą narzędzie, które może służyć do przetwarzania danych, nawet jeśli oni sami ich nie pobierają. To zaś oznacza, że powinni informować o tym, co robią ich programy. Tę samą świadomość muszą mieć sprzedawcy programów, czyli podmioty, które je dystrybuują, a także operatorzy – i to nie tylko dlatego, że sprzedają telefony wraz z już zainstalowanymi aplikacjami, ale i odpowiadają za transmisję danych.

Zważywszy na to, że większość aplikacji mobilnych jest dystrybuowanych spoza Unii Europejskiej, macie chyba niewielką możliwość egzekwowania tych obowiązków? Dlatego proponujemy zmianę prawa i wprowadzenie do unijnego rozporządzenia dotyczącego ochrony danych osobowych, nad którym właśnie trwają prace, zasad podobnych do tych, jakie obowiązują przy ochronie konsumentów. Założenie jest takie, że jeśli ktoś kieruje swoje usługi na rynek europejski, to powinien być traktowany tak, jakby przetwarzał dane w UE.

Gdyby chodziło o użytkowników w Polsce, mógłby pan wówczas wysuwać żądania wobec firm amerykańskich? Takie jest założenie. Dodatkowo chcielibyśmy posiadać uprawnienia, dzięki którym moglibyśmy wymagać od producentów oprogramowania systemowego, by umożliwiali odinstalowywanie aplikacji. Nie jesteśmy do końca pewni, czy jest to możliwe na podstawie obowiązujących przepisów.

Warto chyba zwrócić uwagę, że sam użytkownik smartfona też może naruszać prawo. Jeśli jest przedsiębiorcą i ma w swym telefonie dane klientów, po czym przekazuje je do chmury, to może nieświadomie przetwarzać dane poza terytorium UE. A to wymaga zgody GIODO. Rzeczywiście, czasem może to wymagać zgody GIODO.

Czy przedsiębiorcy zgłaszają się z takimi wnioskami?

Nie mieliśmy ani jednego tego typu wniosku od pojedynczego przedsiębiorcy. Z pewnością większość zwyczajnie nie zdaje sobie sprawy z takiej konieczności. Niemniej i tak ze świadomością dotyczącą ochrony danych osobowych jest coraz lepiej. Liczba wniosków o przekazywanie danych do państw trzecich w ciągu ostatnich lat znacznie wzrosła.

Rozmawiał Sławomir Wikariak