

Serwisy żądają coraz więcej naszych danych. Ich bezpieczeństwo to iluzja

Autor: Tomasz Jurczak

Artykuł z dnia: 2015-08-25, ostatnia aktualizacja: 2015-08-25 08:17



Kradzież danych użytkowników sieci nie należy do rzadkości, ale ostatni przypadek ma dodatkowy wymiar.

źródło: Shutterstock

Liczba danych jakie żądają od internautów firmy w sieci w zamian z użytkowaniem ich serwisów czy aplikacji osiąga coraz większe rozmiary. Co ważne, firmy nie mówią dość i czekają na kolejne informacje o swoich klientach pozyskane za ich zgodą lub bez. W zamian oferują iluzoryczną gwarancję ich bezpieczeństwa.

Seks-wpadka

Kradzież danych użytkowników sieci nie należy do rzadkości, ale ostatni przypadek ma dodatkowy wymiar. Cyberprzestępcy wykradli bazę 32 milionów użytkowników serwisu Ashley Madison. Nie jest to typowy serwis randkowy jak Badoo czy y Tinder, choć i wyciek danych z tych serwisów byłby dla wielu klientów problematyczny. AM przeznaczony jest dla osób, które są już w związku ale mają ochotę na romans. Na razie opublikowano głównie adresy mailowe użytkowników, miasta w których mieszkają oraz NICKi. Jeśli serwis nie

zostanie zamknięty, hakerzy grożą upublicznieniem danych osobowych, numerów kart kredytowych jak i upodobań seksualnych użytkowników.

W całej sprawie warto dodać, że hakerzy ostrzegali o upublicznieniu danych ale firma nie ustosunkowała się do ich żądań. Cyberprzestępcy działali też niejako w imieniu samych użytkowników serwisu, zarzucając właścicielowi AM - Avid Life Media brak definitywnego usuwania informacji o kontach, pomimo, że za tą usługę ALM życzyło sobie 19 dolarów. Zdaniem hakerów te dane nadal są na serwerach. I są gotowi je opublikować.

Przykład AM ma nie tylko wymiar całkowitego braku instynktu zachowawczego samych użytkowników, którzy bez najmniejszego problemu podawali swoje dane serwisowi randkowemu. Pokazuje to też prawdziwy obraz ochrony naszych danych przez firmy działające w sieci – pomimo zapewnień, gwarancji bezpieczeństwa nie ma żadnych. Co ważne sprawa nie kończy się na udostępnieniu samych danych. Osoby, które uzyskały do nich dostęp wysyłają maile do użytkowników serwisu, żądając od nich haracz za nieudostępnianie tych informacji dalej.

W japońskim stylu

Kilka lat temu boleśnie o zabezpieczeniach w jednym z największych koncernów na świecie przekonali się użytkownicy m. in. Playstation. W kwietniu 2011 roku na platformy japońskiego koncernu Sony przypuszczono dwa ataki, na skutek czego skradziono dane blisko 100 mln użytkowników. Pamiętne przeprosiny prezesa, który przez niemal minutę w ukłonie z pochyloną głową przeproszał przed kamerami, raczej nie poprawiły samopoczucia milionów niezadowolonych klientów, którzy przekazali firmie dane swoich kart kredytowych. Niewiele pomogłoby w tym momencie nawet rytualne seppuku, skoro już kilka miesięcy później hakerzy uderzyli ponownie, tym razem na Sony Pictures, wykradając dane miliona użytkowników producenta i dystrybutora filmowego.

Warto w tym momencie dodać, że włamanie na serwery nie dotyczą tylko koncernów ale także wydawałoby się niezwykle chronionych danych na serwerach departamentów amerykańskiego rządu. "Niestety ciężko jest zagwarantować pełne bezpieczeństwo bazy z danymi użytkowników. Nawet jeżeli dana firma poświęca temu zagadnieniu bardzo dużo uwagi, może się zdarzyć, że ktoś przy pomocy nieznanej dziury wykradnie cenne informacje. Z tego powodu najlepszym rozwiązaniem jest podawanie minimalnej ilości danych, niezbędnej np. do zarejestrowania się i korzystania z interesującego nas serwisu" – informuje Maciej Ziarek, ekspert ds. bezpieczeństwa IT, Kaspersky Lab Polska.

psav linki wyróżnione

iCloud czyli firma nie zawsze jest winna

Całkowicie inny przykład to włamanie się na konta użytkowników iCloud. We wrześniu 2014 roku pod znakiem zapytania postawiono bezpieczeństwo usługi Apple. Bardzo szybko okazało się jednak, że nie złamano zabezpieczeń iCloud. Hollywoodzkie celebrytki, których nagie zdjęcia przeniknęły do sieci ustawiły tak słabe hasła i pytania bezpieczeństwa, że włamanie do usługi nie stanowiło żadnego problemu. Tym samym Apple zachowało twarz. Zawiodły łatwe hasła i brak dwustopniowego uwierzytelniania w dostępie do usługi.

Firmy lubią nasze dane, i to bardzo

Każdy serwis wymaga od nas podania pewnej liczby danych, aby uwierzytelnić nasze logowanie. Są dane, które udostępnienie czasem jest konieczne, są jednak informacje zbędne dla serwisu – oczywiście teoretycznie. „Afera” z kwietnia 2015 roku pokazała, że firmy lubią też pozyskiwać dane o klientach bez ich wiedzy. Belgijski GIODO zakwestionował działania amerykańskiego koncernu Facebook.

Wszystko opierało się na prostym mechanizmie. Przede wszystkim dotyczyło to wykorzystania przez FB swoich wtyczek społecznościowych jak np. „Like” porozrzucanych po milionach miejsc w sieci. Nie trzeba w nie nawet klikać. Innym sposobem są cookies. Nawet po wylogowaniu z serwisu, w przeglądarce użytkownika pozostawiane są odpowiednie „ciasteczka”, które pomagają w śledzeniu internautów. Co ważne, nawet po dezaktywowaniu konta, ciasteczka nadal działają, co nie przeszkadza FB w inwigilowaniu swoich użytkowników. Nigdy nie zakładałeś konta na FB? To nic nie zmienia. Wystarczy, że wszedłeś na stronę z wtyczką FB lub wydarzenie na serwisie, a ciasteczko zostaje podrzucone. Cel Facebooka jest jeden – profilowanie użytkowników aby jak najskuteczniej wykorzystywać treści reklamowe. Belgijski GIODO podała serwis do sądu.

GIODO ostrzega: Internauci są przymuszani do przekazania danych

Rozwój technologiczny powoduje, iż trzeba wypracować nowe, skuteczne sposoby ochrony prywatności i danych osobowych w Internecie. Obecne przepisy dotyczące ochrony danych osobowych były tworzone w czasach, kiedy nowe technologie, w tym Internet, dopiero raczkowały. Wówczas nikt nie myślał np. o serwisach społecznościowych, RFID, Internecie przedmiotów czy przetwarzaniu danych w chmurze, a istniejące strony internetowe miały raczej statyczny charakter, gdyż oferowały dostęp do informacji wybranych przez ich autorów. Dzisiaj zaś wszyscy mogą korzystać z narzędzi umożliwiających publikację dowolnych treści w sieci.

W opinii Generalnego Inspektora Ochrony Danych Osobowych (GIODO), wiele serwisów społecznościowych wymusza zgodę swoich użytkowników na przetwarzanie danych, nie informując ich jednocześnie o tym, w jaki sposób ich dane będą wykorzystywane. Internauci są przymuszani do przekazania bardzo szerokiego zestawu danych o sobie, stojąc przed „groźbą” nieuzyskania dostępu do serwisu. Tymczasem jest to sprzeczne z zasadą minimalizacji przetwarzania danych osobowych, która stanowi, że należy przetwarzać jedynie te dane, które są niezbędne dla osiągnięcia celu, w którym je zebrano, w tym przypadku - prawidłowego funkcjonowania serwisu.

Kolejnym grzechem większości właścicieli serwisów społecznościowych jest to, że dane użytkowników wykorzystują często nie tylko do tworzenia serwisu czy wprowadzania w nim nowych rozwiązań, ale i do celów komercyjnych, o czym nie informują osób, których dane dotyczą.

Gdy zaś będziemy chcieli dochodzić swoich praw wynikających z przepisów o ochronie danych osobowych, to w przypadku serwisów internetowych, które są zlokalizowane w państwach poza Unią Europejską, często np. w USA, a świadczą usługi na rzecz mieszkańców państw unijnych, możemy napotkać poważne trudności. Nie zawsze bowiem ewentualne spory będą rozstrzygane na podstawie prawa unijnego w sądach na obszarze UE, choć Unia Europejska stoi na stanowisku, że tak powinno być.

Zdaniem dr Edyty Bielak – Jomaa, Generalnego Inspektora Ochrony Danych Osobowych, istotne znaczenie dla poprawy praw osób, których dane przetwarzane są m.in. przez serwisy internetowe prowadzone przez podmioty spoza państw Unii Europejskiej, będzie miało unijne rozporządzenie w sprawie ochrony danych osobowych, nad którym prace dobiegają właśnie końca. Ma ono bowiem przesądzić, czy do jego postanowień będą musiały się stosować także przedsiębiorstwa spoza UE, które oferują towary lub usługi w Unii Europejskiej (np. za pośrednictwem Internetu), lub monitorują zachowania obywateli UE.

Dane użytkownika mają wymierną wartość pieniężną - Csaba Krasznay, Product Manager of Shell Control Box, BalaBit

Więcej danych to większa wartość – zarówno dla usługodawców, jak i przestępców. Więcej danych o użytkownikach może poprawić jakość usług ale także podnieść poziom ryzyka, to fakt bezsporny. Z tego powodu bezpieczeństwo IT nigdy nie było aż tak ważne jak obecnie. System kontroli nie działa sprawnie w dzisiejszym Internecie opartym na usługach. Innowacyjne firmy tworzą wyróżniające się, ciekawe usługi dla niszowych rynków, użytkownicy chcieliby z nich korzystać, ale władze krajowe, ustawodawca nie są w stanie spełnić obowiązku ochrony konsumenta/ klienta.

Wszystkie strony powinny zrozumieć swoje obowiązki. Przedsiębiorstwa powinny zwrócić szczególną uwagę na dane użytkowników, państwa powinny rozwijać międzynarodowe programy ochrony prywatności i klientów z wystarczającą siłą przymusu. I rzecz ostatnia, ale również ważna - użytkownicy powinni zrozumieć ryzyko związane z ich obecnością w sieci, bo każdy zostawiając po sobie cyfrowy ślad musi być świadomy, że zostawia o sobie informacje w sieci. Ustawodawcy i użytkownicy końcowi działają powoli, dlatego w pierwszej kolejności to firmy powinny zrozumieć, że muszą inwestować w swoje programy i systemy bezpieczeństwa. Duże wycieki danych z powodu ataków wewnętrznych lub zewnętrznych zdarzają się co tydzień i mogą całkowicie zniszczyć ich biznes.

Korzystamy z dóbr oferowanych przez firmy, płacąc za usługi naszymi danymi - Michał Guzek, Członek Zarządu Hicron

Obecnie, kiedy głośno mówi się o wycieku danych, podważenie wiarygodności firmy w obszarze bezpieczeństwa danych powodowałoby odpływ masy klientów. Stąd coraz więcej firm: Dropbox, Google, Twitter, Facebook i inne wprowadzają nowe zabezpieczenia. Przysnajmy - kolejne inwestycje w bezpieczeństwo danych to spory wydatek. Ale nie podjęcie go byłoby jak gra w rosyjską ruletkę. Inny przykład – Apple, Yahoo, Facebook i Microsoft jawnie występują przeciwko udostępnianiu NSA danych swoich klientów. Microsoft podejmuje najbardziej stanowcze kroki planując program, dzięki któremu klienci będą mogli przenieść swoje dane z serwerów w USA na serwery w innych krajach. Oprócz ogromnych kosztów związanych z tym przedsięwzięciem, gigant naraża się władzy. Zyskuje jednak zaufanie i poparcie klientów, którzy decydują o jego być albo nie być. Patrząc na sprawę bezpieczeństwa pod innym kątem, należałoby odpowiedzieć sobie szczerze na pytanie, jak sami o nie dbamy. Moim zdaniem największym problemem nie są nieodpowiednie zabezpieczenia, a złe nawyki użytkowników: stosowanie haseł łatwych do mechanicznego odgadnięcia, odpowiadanie na podejrzane maile, klikanie linków, stosowanie jednego hasła dla wielu kont itp.

Pozostaje pytanie o to, czy żądanie dostępu do danych jest moralne. Tak długo, jak jesteśmy informowani o tym, co przekazujemy i komu – tak, bo daje to nam możliwość podjęcia decyzji. Wyszukiwarki, aplikacje dedykowane, google maps, – wszyscy korzystamy z tych

dóbr, płacąc za usługi naszymi danymi. Co więcej – dzięki tym danym producenci ulepszają te aplikacje, także dla nas - klientów. Jest to działanie komercyjne, ale z obopólną korzyścią.

Autor: Tomasz Jurczak

