Gazeta Prawna

28-01-2009

PRAWO

Banki nie mogą ukrywać wycieku danych

Uważam, że ustawowo należy nakazać, aby banki – w sytuacji gdy dojdzie do wycieku danych osobowych – obowiązkowo informowały o tym klientów – mówił podczas zorganizowanej przez GP debaty Michał Serzycki, generalny inspektor ochrony danych osobowych. Jego zdaniem cyberprzestępcy, mając świadomość przepływu wielkich kwot w e-bankowości, coraz częściej atakują jej systemy. Banki chcą więc stosować zabezpieczenia biometryczne jako dodatkowy element bezpieczeństwa obrotu danymi klientów.■

strona 10

Gazeta Prawna

28-01-2009

O wycieku danych osobowych z banków powinni być poinformowani klienci

Ustawowo należy nakazać, aby firmy – w sytuacji gdy dojdzie do wycieku danych osobowych – obowiązkowo informowały o tym opinię publiczną. A definicja danych osobowych powinna być uzupełniona o hasła elektroniczne.

MICHAŁ SERZYCKI

Coraz więcej dyspozycji klientów banków dokonywanych jest za pomocą nowych technologii, takich jak SMS-y czy internet. Obowiązek należytego zabezpieczenia tych transakcji ma bank, ale ogromną czujność muszą wykazywać też osoby korzystające z nowych form komunikacji. Nasuwa się więc pytanie, czy jesteśmy przygotowani do e-bankowości? Czy klienci zdają sobie sprawę z zagrożeń? Wydaje się, że nie. Natomiast cyberprzestępcy, mając świadomość ogromu pieniędzy przepływających w wirtualnej bankowości oraz nieznajomości zagrożeń ze strony klientów, coraz częściej atakują systemy bankowości elektronicznej. Komputery czy telefony korzystających z nich osób prywatnych także są w niebezpieczeństwie.

Dane jak tajemnica bankowa

KRZYSZTOF PIETRASZKIEWICZ

Warto pamiętać, że w Polsce 75 proc. rodzin korzysta z usług bankowych i 65 proc. osób powyżej 15 roku życia posiada rachunek bankowy. Polska jest krajem nieubankowionym. Pod tym względem zajmujemy jedno z ostatnich miejsc w Europie. Przeciętnie Polacy korzystają z produktów bankowych od 6 do 12 razy rzadziej niż obywatele UE.

Pomimo tych złych statystyk postęp, jaki się dokonał w ostatnich latach, jest ogromny. Możliwość dostępu do rachunku bankowego przez internet ma 12 mln osób. Wydaliśmy ok. 30 mln kart płatniczych. Około 6,5 mln osób korzysta z e-bankowości na co dzień. Ale zajmujemy jedno z końcowych miejsc pod względem użycia kart płatniczych. Korzyści płynące z użycia elektroniki w bankowości to oszczędność czasu i bezpieczeństwo. Polska bankowość pod względem bezpieczeństwa należy do najlepszych. Wynika to m.in. z tego, że nie przesyłamy już danych między bankami na papierze.

Dzieje się tak dlatego, że bankowcy traktują w taki sam sposób ochronę danych osobowych jak zachowanie tajemnicy bankowej.

Wiele podmiotów ma dostęp do informacji bankowej, ale jest sukcesem, że urzędy skarbowe mają dostęp do danych w sposób ustawowo zdefiniowany. Policja w sprawach ważnych też kieruje się przepisami ustawy. Wprowadziliśmy dwa standardy – dostęp do danych klientów banków odbywa się na podstawie ich zgody lub z ich inicjatywy. Ponadto dostęp do danych prokuratury, policji i urzędów odbywa się pod nadzorem sądów.

Prawie 85 proc. dużych firm korzysta z usług bankowych przez internet, ale tylko 65 proc. małych przedsiębiorstw.

MICHAŁ SERZYCKI
generalny inspektor ochrony danych osobowych

KRZYSZTOF PIETRASZKIEWICZ
prezes Związku Banków Polskich

WIESŁAW PALUSZYŃSKI
wiceprezes Zarządu Głównego Polskiego Towarzystwa Informatycznego

ARWID MEDNIS
Uniwersytet Warszawski, partner w Kancelarii Wierzbowski Eversheds

Zdjęcia Marek Matusiak

Jesteśmy dziwnym krajem, gdzie elektroniczna bankowość rozwija się szybciej niż gospodarka.

WIESŁAW PALUSZYŃSKI

Trudno rozdzielić bezpieczeństwo danych od bezpieczeństwa transakcji bankowych. Klasycznym motywem przejęcia danych osobowych jest chęć zdobycia ich dla celów marketingowych, handlowych, przestępczych. W przypadku przesyłu transakcji bankowych drogą elektroniczną bardzo rzadko występuje nasze nazwisko. Najczęściej posługujemy się nadanym przez bank numerem identyfikacyjnym. Przejęcie tego rodzaju danych przez osobę nieuprawnioną powoduje najczęściej utratę naszych pieniędzy.

Trzeba powiedzieć, że sektor bankowy wyznaczył jako jeden z pierwszych pewne praktyczne standardy, które mówiły o bezpieczeństwie kanałów komunikacji między bankiem a klientem.

Systemy bankowe rejestrują gigantyczną liczbę obywateli i ich danych. Dotyczy to kont, systemu przyznawania kredytów i rejestrów dłużników oraz jednostek, którym bank te informacje udostępnia. Z tego wynikały pewne kuriozalne sytuacje. System nie nadążał za rzeczywistością i podawał jako dłużników osoby niezadłużone.

W przypadku konsolidacji banków, gdy bank-matka pozostawał za granicą, powstał problem miejsca przechowywania danych. Jak zabezpieczyć dane obywateli polskich, które pozostają za granicą, w sytuacji gdy nie można ich skontrolować? Banki twierdziły, że system cyfrowy nie pozwala na zidentyfikowanie konkretnych klientów. Jednak ten system nie jest doskonały, należy go uszczelnić.

Hasło i IP też jest daną

MICHAŁ SERZYCKI

Nie zgodzę się z tezą, że w przypadku gdy dane osobowe nie są przesyłane, a przesyła się jedynie elektronicznie hasła, to dane są bezpieczne. Pytanie, czy dla banku hasło użytkownika nie będzie daną osobową? Rozwój nowych technologii powoduje, że definicja danych osobowych się rozszerza. Na przykład Internet Protocol – protokół komunikacyjny (IP) komputera do niedawna nie należało do tej kategorii. Co więcej, także nick i pliki cookie należałoby już uznać za dane osobowe. Za rok czy dwa może się okazać, że i hasło bankowe jest daną osobową podlegającą ochronie. Taką zmianę w podejściu do definicji danych osobowych wymusza na nas rozwój nowoczesnych technologii. Ponadto, moim zdaniem, klient musi wyrazić zgodę na przesłanie i przetwarzanie wszelkich informacji związanych z korzystaniem z usług bankowych.

WIESŁAW PALUSZYŃSKI

Jednak przy zakładaniu kont kseruje się dowód osobisty klienta banku i nie ma on nic w tej sprawie do powiedzenia. Może się nie zgodzić na kopiowanie, ale wtedy nie będzie miał konta.

Outsourcing nie jest uregulowany

ARWID MEDNIS

Jeśli chodzi o kopiowanie dokumentów, to mylimy formę zbierania danych i zakres zbierania danych. Najistotniejsze jest to, jakie dane są zbierane, a nie w jaki sposób. Kilka lat temu zapadł wyrok w sprawie kserowania dowodów osobistych. Sąd stwierdził, że zbierane dane, takie jak imiona rodziców oraz stare adresy są adekwatne do potrzeb związanych z udzielaniem kredytów. Są potrzebne bankowi, aby dotrzeć do kredytobiorcy.

Wyliczyłbym cztery istotne czynniki bezpieczeństwa: po pierwsze – prawo. Często spotykam się z opinią, że prawo bankowe jest nadregulacją.

Ta dziedzina wymaga bardzo precyzyjnej regulacji i nie śmieję się np. z przepisu, który pozwala udostępnić dane bankowe adwokatowi lub radcy prawnemu, który prowadzi sprawy banku. Ważne jest, aby wszystkie występujące sytuacje uregulować.

Moim zdaniem m.in. outsourcing nie jest wystarczająco uregulowany w prawie bankowym.

Druga sprawa – zabezpieczenia techniczne. Są banki, które stosują zabezpieczenia niewystarczające. Następny czynnik to świadomość klientów banków. Czynnik mocno niedoceniany. Z jednej strony polepszamy standardy techniczne, ale nie idzie za tym większy poziom świadomości klientów. Przykładem jest zjawisko phishingu, wykradania danych: przychodzi e-mail i rzekomy bank prosi o potwierdzenie danych, a naiwny klient podaje np. swoje hasło. Czwarty czynnik to jest kultura organizacji, czyli banku. Dlatego że oprócz klienta słabym ogniwem jest pracownik. Kultura organizacji to są szkolenia w zakresie bezpieczeństwa danych, regulaminy wewnętrzne, prawne regulacje sektorowe. Takie szkolenia powinny być obowiązkowe. Ponadto pracownik powinien wiedzieć, do kogo ma się zwrócić w firmie w przypadku naruszeń bezpieczeństwa, np. włamania.

MICHAŁ SERZYCKI

Zgadzam się, że najsłabszym ogniwem przy zabezpieczaniu danych osobowych są ludzie. Trzeba budować świadomość klientów i pracowników. Bo choć sondaże dowodzą, że jest ona coraz wyższa, a nawet przodujemy pod tym względem w Europie, to często nie idzie ona w parze ze stosowaniem odpowiednich zabezpieczeń na co dzień. A jest to ważne, gdyż postęp technologiczny rodzi kolejne, coraz bardziej wyrafinowane zagrożenia dla ochrony danych osobowych oraz prywatności.

Sądzę, że potrzebna jest nowelizacja prawa bankowego, które uwzględni zachodzące zmiany związane z rozwojem nowoczesnych technologii.

Zabezpieczenia biometryczne

KRZYSZTOF PIETRASZKIEWICZ

Chcemy szeroko stosować zabezpieczenia biometryczne jako dodatkowy element bezpieczeństwa obrotu i ochrony danych. Budowanie biur informacji kredytowej i niektórych baz danych powoduje większy komfort dla klientów i mniejsze koszty. Ale wtedy trzeba rezygnować z części praw do prywatności.

MICHAŁ SERZYCKI

Mamy w takim przypadku do czynienia z klasycznym konfliktem wartości. Wchodzi tu w grę także bezpieczeństwo obrotu gospodarczego, czyli kwestia tego, jak daleko można dla bezpieczeństwa tego obrotu pozwolić na wkraczanie w prywatność człowieka. Chciałbym, żeby prawo do prywatności było ograniczane aktem rangi ustawy, a najlepiej, aby odbywało się za zgodą obywatela.

Uważam też, że ustawowo należy nakazać, aby firmy – w sytuacji gdy dojdzie do wycieku danych osobowych – obowiązkowo informowały o tym opinię publiczną.

WIESŁAW PALUSZYŃSKI

Kontrowersje budzi hasło Bezpieczeństwo obrotu gospodarczego, często stosowane przy uzasadnianiu ingerencji w prywatność. Jest też inne często cytowane cenne dobro: Porządek publiczny. Gwarantuje ono oczekiwane przez społeczeństwo standardy życia codziennego. Bezpieczeństwo obrotu gospodarczego jest właśnie elementem bezpieczeństwa publicznego. Dlatego wymiana informacji o nieuczciwych dłużnikach czy uczciwych kredytobiorcach jest bardzo ważna.

Ujawniać nieuczciwych dłużników należy nawet bez ich zgody. Moim zdaniem dane pozytywne, np. o historii rachunku, powinny być przetwarzane za zgodą klienta. Jednak informacje o zobowiązaniach wymagalnych nie muszą już wymagać zgody zainteresowanego.

Co do powszechnego stosowania metod biometrycznych w postaci linii papilarnych lub układu naczyń krwionośnych, to trzeba pamiętać, że jeśli stracę swoje dane biometryczne, to jestem bez szans. Wystarczy jeden moment przejęcia fragmentu mojej elektronicznej tożsamości i jestem pozbawiony całkowicie ochrony. Biometria nie jest panaceum na wszystkie problemy identyfikacji, a jej stosowanie powinno podlegać szczególnie starannej i technicznie zaawansowanej ochronie. Zaryzykuję stwierdzenie, że dane biometryczne to najważniejszy zestaw z moich danych osobowych.■

Dyskusję prowadziła KATARZYNA ZACZKIEWICZ-ZBORSKA

WNIOSKI

- Dane klientów o poziomie zadłużenia dla potrzeb banków powinny być udostępniane z mocy prawa
- Zgody klienta wymaga udostępnianie historii kredytowej innym uczestnikom obrotu
- Pracownicy banków powinni być lepiej szkoleni w zakresie prawa i regulaminów bezpieczeństwa
- Powinien być nałożony na instytucje administrujące danymi osobowymi obowiązek informowania o wycieku tych danych