Komisja Nadzoru Finansowego

14 lipca 2014 r.

Ryzyko związane z podawaniem innemu bankowi danych do logowania do rachunku bankowego

W ostatnim czasie nadzór zidentyfikował przypadki, w których banki proszą potencjalnych klientów w procesie wnioskowania o kredyt o podanie danych logowania do rachunków tych klientów prowadzonych przez inne banki (login/identyfikator oraz hasło). Umożliwia to m.in. dostęp do historii rachunku danej osoby w innym banku.

Niektóre banki udostępniają też klientom funkcjonalność pozwalającą na wprowadzenie danych logowania do kont w innych bankach, pod hasłem wglądu we wszystkie rachunki w jednym miejscu.

Powyższe działania realizowane są na dwa sposoby:

1) Dane logowania podawane są przez klienta bankowi (np. poprzez stronę internetową), który następnie w zastępstwie klienta loguje się do serwisu bankowości internetowej banku, w którym prowadzony jest dany rachunek;
2) Dane logowania wprowadzane są przez klienta do aplikacji instalowanej na urządzeniu końcowym klienta (analogicznie do przeglądarki internetowej), która odpowiada za zalogowanie się do serwisu bankowości internetowej banku, w którym prowadzony jest dany rachunek, automatyczne pobranie stamtąd odpowiednich informacji oraz ich dalsze przetworzenie.

Takie praktyki banków budzą zaniepokojenie Urzędu Komisji Nadzoru Finansowego (Urzędu KNF). W związku z tym, wobec banków stosujących kwestionowane praktyki podjęte zostały indywidualne działania nadzorcze zmierzające do zmiany postępowania tych banków. Dodatkowo jednak, publikując niniejszy komunikat, KNF zwraca klientom oraz bankom uwagę, że podawanie przez klientów danych logowania do bankowości internetowej w sposób wyżej opisany wiąże się z następującymi czynnikami ryzyka:

1) W przypadku, gdy logowanie do serwisu bankowości internetowej banku prowadzącego rachunek klienta realizowane jest w jego zastępstwie przez inny bank, zaś klient przy użyciu tego kanału ma możliwość realizacji zleceń płatniczych, prowadzi to do złamania przez klienta przepisów art. 42 ust. 2 *ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych* oraz warunków umownych dotyczących korzystania z bankowości internetowej w zakresie konieczności zachowania poufności danych logowania. Wiąże się to z ryzykiem utraty prawa do reklamacji ewentualnych nieautoryzowanych transakcji.
2) Niezależnie od sposobu realizacji przedmiotowych praktyk należy podkreślić, że podstawową zasadą bezpiecznego korzystania z usług bankowych i płatniczych z wykorzystaniem elektronicznych kanałów dostępu jest podawanie nazwy użytkownika i hasła do konta jedynie na stronie internetowej banku prowadzącego dany rachunek lub w udostępnianej przez niego aplikacji (np. instalowanej na telefonie). Praktyka niektórych banków zachęca klientów do łamania tej zasady.
3) Takie postępowanie może zaprzepaścić wieloletnie działania edukacyjne środowiska bankowego uświadamiające klientom banków istotność powyższej zasady. Jest prawdopodobne, że spowoduje to zmniejszenie czujności klientów w odniesieniu do miejsc, w których wprowadzają oni swoje dane logowania, co może przyczynić się do wzrostu skuteczności ataków typu phishing i pojawienia się nowych scenariuszy ataków tego rodzaju. Niepożądanym pośrednim efektem może być zmniejszenie zaufania klientów do korzystania z usług bankowych i płatniczych świadczonych przez Internet.

W tym kontekście należy zwrócić uwagę na podejmowane w ramach Związku Banków Polskich (ZBP) działania mające na celu wypracowanie rozwiązań pozwalających na bezpieczną, autoryzowaną przez wszystkie zaangażowane strony wymianę danych klientów, które w opinii KNF mogą pozwolić na istotne ograniczenie ryzyka w tym zakresie.