DWUSTOPNIOWE UWIERZYTELNIANIE W BANKOWOŚCI ELEKTRONICZNEJ. JAKIE ZMIANY CZEKAJĄ KLIENTÓW?

Od soboty banki muszą wprowadzić dodatkowe zabezpieczenia w bankowości elektronicznej. 14 września wchodzą w życie przepisy wdrażające dyrektywę unijną PSD2, które wprowadzają nowe wymagania dotyczące potwierdzania tożsamości klientów.

Przepisy wzmacniają sposób uwierzytelniania w bankowości elektronicznej i uwierzytelniania się przy transakcjach zbliżeniowych, by zwiększyć bezpieczeństwo korzystania z usług płatniczych oferowanych elektronicznie i ograniczyć możliwości wystąpienia oszustw związanych z tymi usługami. Nowe przepisy zobowiązują banki do wprowadzenia dwustopniowego uwierzytelniania na etapie uzyskiwania dostępu do konta internetowego, dokonywania transakcji i płatności internetowych.

Banki już od tygodni prowadzą akcje informacyjne, przesyłając klientom smsy i wiadomości na skrzynki w aplikacjach oraz na kontach internetowych. Od dłuższego czasu informują także klientów o zmianie przepisów na swoich stronach internetowych. Niektóre z nich starają się, by nowe wymagania dotyczące np. logowania na konto były jak najmniej odczuwalne dla klientów, inne przy okazji zmieniają wygląd swoich serwisów internetowych i aplikacji. Zmienioną stronę logowania do serwisu iPKO przygotował np. bank PKO BP.

W związku z nowymi regulacjami wszystkie banki przewidują zmiany zasad korzystania z konta i aplikacji mobilnej, zwłaszcza w sposobie logowania do kont elektronicznych. Większość z nich planuje wykorzystać do tego znane już ich klientom narzędzia. Np. bank Millennium będzie wykorzystywał stosowane obecnie formy uwierzytelniania - hasło SMS i autoryzację mobilną.

Z kolei klienci banku Santander, którzy obecnie przy logowaniu się do bankowości internetowej muszą podać login oraz hasło, po 14 września będą także np. podawali sms kod lub składali mobilny podpis, w zależności od tego, z jakiego narzędzia autoryzacyjnego korzystają obecnie przy zleceniach przelewu. Dodatkowo bank umożliwi klientom oznaczenie w systemie wybranego przez nich urządzenia zaufanego - komputera, tabletu czy smartfona - co ograniczy wymagania przy logowaniu się do konta.

Dodatkowe wymagania będą dotyczyły także operacji na kontach lub np. wglądu w historię. Np. bank Pekao przy uzyskiwaniu dostępu do informacji o rachunku będzie wymagał nie rzadziej niż co 90 dni podania kodu sms lub kodu wygenerowanego przez aplikację PeoPay. Klient będzie musiał podawać kod również w przypadku wejścia w historię operacji starszą niż 90 dni.

Zmiany w potwierdzeniu tożsamości będą także wymagane np. przy logowaniu do aplikacji Moje ING mobile. Bank przewidział, że użytkownicy tej aplikacji mogą zalogować się na trzy sposoby: podając PIN do aplikacji, przedstawiając identyfikator biometryczny – odcisk palca lub obraz twarzy, albo obie

na raz. Za każdym razem, gdy użytkownik będzie się logować, automatyczny system bezpieczeństwa banku zdecyduje, czy dodatkowa autoryzacja jest konieczna.

Banki wycofują się z niektórych obecnych rozwiązań, które nie spełniają warunków silnego uwierzytelnienia. Np. Pekao wycofuje karty kodów jednorazowych, tokeny aplikacyjne i sprzętowe, a mBank listę haseł jednorazowych służących potwierdzaniu operacji.

Jak mówił PAP ekspert ds. danych osobowych Maciej Kawecki, trzeba wykazać szczególną czujność, by wchodzące od 14 września przepisy, nie dały okazji także oszustom. Jego zdaniem zmiany są potrzebne, "bo skala zjawiska związanego z oszustwami w sektorze finansowym jest ogromna".

Według Kaweckiego na początku można sie spodziewać fali oszustw nieco podobnych do tych, jakie miały miejsce np. przy wprowadzaniu RODO, kiedy pod pretekstem aktualizacji różnych polityk prywatności od wielu ludzi wyłudzono pieniądze, ale generalnie nowe przepisy poprawią bezpieczeństwo klientów banków, dzięki wprowadzeniu dwustopniowej weryfikacji tożsamości.