Ostrzeżenie UKNF dot. wyłudzania poufnych informacji w zw. z PSD2

Od 14 września 2019 r. dostawców usług płatniczych (w tym banki, skoki, instytucje płatnicze) zacznie w pełni obowiązywać unijne rozporządzenie wykonawcze do dyrektywy PSD2, dotyczące silnego uwierzytelniania klienta oraz otwartych i bezpiecznych standardów komunikacji. Rozporządzenie to ma na celu m.in. podwyższenie poziomu zabezpieczeń stosowanych przy świadczeniu usług płatniczych za pośrednictwem kanałów elektronicznych (bankowość internetowa, płatności kartami płatniczymi, płatności internetowe), a w efekcie zwiększenie poziomu bezpieczeństwa klienta w jego relacjach z dostawcami usług płatniczych.

Podwyższenie poziomu zabezpieczeń transakcji elektronicznych oparte zostanie o silne uwierzytelnienie klienta. W wyniku wprowadzanych przez dostawców usług płatniczych nowych rozwiązań, zmianie ulegnie przede wszystkim sposób logowania do serwisów bankowości elektronicznej. Konieczne będzie w szczególności użycie dodatkowej, obok loginu i hasła, metody autoryzacji. Wybór konkretnych rozwiązań pozostaje w gestii właściwych dostawców usług płatniczych, a szczegółowe informacje na ten temat dostępne są na ich stronach internetowych. W obszarze płatności kartowych zmiany dotyczyć będą sposobu autoryzacji transakcji internetowych – bez fizycznego użycia karty, a także płatności zbliżeniowych, przy których częściej niż dotychczas, nie tylko przy przekroczeniu kwoty 50 zł, wymagane będzie potwierdzenie transakcji PIN-em.

Urząd Komisji Nadzoru Finansowego zwraca uwagę, że związana z wdrażaniem nowych rozwiązań konieczność wzmożonych kontaktów ze strony dostawców usług płatniczych ze swoimi klientami może zostać wykorzystana przez przestępców do prób wyłudzenia poufnych informacji, w tym poprzez przeprowadzanie ataków phishingowych, a w konsekwencji do kradzieży tożsamości lub kradzieży środków finansowych.

W związku z powyższym Urząd KNF zwraca uwagę na konieczność zachowania szczególnej ostrożności oraz apeluje do klientów instytucji finansowych o postępowanie zgodne z ustalonymi przez te instytucje standardami w zakresie komunikacji. Uzasadnione podejrzenia powinny wzbudzić wszelkiego rodzaju wiadomości mailowe, SMS oraz próby kontaktu telefonicznego powołujące się na wejście w życie nowych rozwiązań, gdzie klient proszony jest o przekazanie informacji zawierających dane wrażliwe, w szczególności:

- dane logowania do bankowości elektronicznej;
- kody autoryzacyjne i kody PIN;
- dane osobowe;

lub informowany jest o zablokowanym koncie albo proszony jest o:

- kliknięcie w przesłany mailem lub SMSem link internetowy;
- zmianę hasła lub innych danych do logowania za pomocą przesłanego linku internetowego;
- otworzenie podejrzanego załącznika, uruchomienie lub instalację przesłanej aplikacji;
- wykonanie podejrzanej płatności lub przelewu internetowego.

W przypadku jakichkolwiek wątpliwości zalecamy bezpośredni kontakt z właściwym dostawcą usług płatniczych. Jednocześnie zachęcamy do zaktualizowania posiadanej wiedzy w zakresie bezpiecznego korzystania z usług finansowych poprzez odwiedzenie stron internetowych instytucji finansowych, na których zamieszczone są szczegółowe informacje i ostrzeżenia w zakresie bezpiecznego korzystania z ich usług.