KNF | KOMISJA NADZORU FINANSOWEGO

15 lutego 2021 r.

Cyberbezpieczeństwo elektronicznych kanałów dostępu do usług bankowych – list Przewodniczącego KNF do sektora bankowego

Komisja Nadzoru Finansowego (dalej również: Komisja, KNF lub organ nadzoru) obserwuje dynamiczny rozwój elektronicznych kanałów dostępu do usług bankowych, w znaczący sposób determinowany obecną sytuacją epidemiczną, w której nieprofesjonalni uczestnicy rynku przenoszą swoją aktywność z tradycyjnych form kontaktu i współpracy z dostawcami tych usług na rzecz kontaktu drogą elektroniczną. Oprócz oczywistych korzyści dla klienta związanych z możliwością efektywnego zarządzania finansami poprzez m.in. redukcję czasu i kosztów związanych z kontaktami z bankiem, taka praktyka niesie za sobą również szereg ryzyk mających wpływ na bezpieczeństwo środków finansowych klientów. Informacje pozyskane w trybie nadzorczym, w trakcie pracy operacyjnej zespołu CSIRT KNF (realizującego zadania Sektorowego Zespołu Cyberbezpieczeństwa), z mediów oraz sygnałów kierowanych do UKNF od konsumentów świadczą jednoznacznie o utrzymującej się niskiej świadomości klientów w obszarze zagrożeń i ryzyk związanych z korzystaniem z nowoczesnych technologii oraz niedostatecznej znajomości podstawowych zasad bezpieczeństwa korzystania ze zdalnych kanałów dostępu do usług finansowych związanych z powierzonymi środkami pieniężnymi.

W ocenie Komisji, pomimo prowadzonych od wielu lat kampanii i działań edukacyjnych, których inicjatorami są m.in. podmioty rynku finansowego, obserwowana jest tendencja wzrostowa liczby oszustw, których ofiarami padają konsumenci, niejednokrotnie tracący oszczędności całego życia. Konkluzja ta dotyczy zarówno osób aktywnie korzystających z nowoczesnych technologii i form komunikacji, jak również osób starszych, które z usług bankowości elektronicznej korzystają sporadycznie.

Komisja, odnosząc się do swojego stanowiska z 2016 r.[1] , ponownie zwraca uwagę, że podczas działań bieżących oraz w odniesieniu do działań planowanych, w szczególności w obszarze usług wykorzystujących elektroniczne kanały dostępu, dostawcy usług bankowych powinni konsekwentnie stosować paradygmat określany jako „security first", determinujący prowadzenie pogłębionych analiz ryzyka, uwzględniających nie tylko kwestie bezpieczeństwa środowiska teleinformatycznego dostawcy bezpośredniego czy dostawców outsourcingowych, ale również ryzyk związanych z korzystaniem z usług finansowych przez klientów. KNF podkreśla przy tym, że potrzeby optymalizacji kosztowej czy procesowej, które mogłyby stanowić przyczyny reorganizacji modelu bankowości elektronicznej, nie mogą mieć wpływu na założenia i model tych analiz. Powyższe analizy powinny obejmować także wymagania wobec warunków świadczenia usług zdalnych, aby zapewnić maksymalny do osiągnięcia w danych warunkach poziom bezpieczeństwa środków finansowych klientów i uwzględniać

[1] DIB_ZIT/7113/3/1/2016/PT z dnia 29.06.2016 r.

obecne trendy zagrożeń, wektory ataków na klientów, sposoby działań cyberprzestępców a także potencjalne ryzyka wynikające z planowanych przez dostawcę działań nie tylko wobec swoich klientów, ale również w kontekście potencjalnego wpływu tych działań na cały sektor usług bankowych.

Dostawcy usług bankowych powinni mieć świadomość, że podejmowane przez nich indywidualne inicjatywy, które w ich ocenie nie wpływają negatywnie na poziom ryzyka w obszarze prowadzonej działalności biznesowej, w tym także na bezpieczeństwo środków finansowych klientów, w kontekście całego rynku finansowego i w konsekwencji wszystkich klientów tego rynku, mogą już takie ryzyko generować i stanowić czynnik ryzyka systemowego w obszarze cyberbezpieczeństwa. W kontekście powyższego, zaniepokojenie Komisji budzą obserwowane w ostatnim czasie działania dostawców mogące negatywnie wpływać na profil i poziom ryzyka związanego z bezpieczeństwem danych oraz środków finansowych klientów.

Zgodnie z art. 18 rozporządzenia delegowanego Komisji (UE) 2018/389 z dnia 27 listopada 2017 r. uzupełniającego dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 w odniesieniu do regulacyjnych standardów technicznych dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji (dalej „RTS"), dopuszczalne jest wyłączenie stosowania silnego uwierzytelnienia w przypadku konkretnej płatności niskokwotowej, w oparciu o indywidualną ocenę ryzyka, z uwzględnieniem właściwych w tym zakresie przepisów RTS.

KNF oczekuje, że rozwiązania wpływające na bezpieczeństwo środków finansowych klientów, a w oczywisty sposób za takie należy uznać decyzję o możliwości niestosowania silnego uwierzytelnienia w odniesieniu do zdalnych elektronicznych transakcji płatniczych, które dostawca uznaje za charakteryzujące się niskim poziomem ryzyka zgodnie z mechanizmami monitorowania transakcji, będą wdrażane jedynie w sposób pozostawiający klientom celową i świadomą decyzję, podjętą z wykorzystaniem elektronicznego kanału dostępu lub innej zdefiniowanej w umowie z klientem formy komunikacji, o generalnym wyłączeniu silnego uwierzytelniania dla wszystkich transakcji niskokwotowych w proponowanym przez dostawcę zakresie. Elementem poprzedzającym podjęcie tej decyzji powinna być akceptacja przez klientów informacji o potencjalnym ryzyku utraty środków finansowych, w tym przypadku związanym z wyłączeniem silnej autoryzacji dla transakcji niskokwotowych.

Dodatkowo uwzględniając stosowanie zasady „security first", nadzór oczekuje wdrożenia w systemie transakcyjnym funkcjonalności dającej klientowi możliwość ustawienia potwierdzenia silnym uwierzytelnieniem każdej płatności.

Główną metodą ataków na klientów instytucji finansowych są działania socjotechniczne, wykorzystywane przez cyberprzestępców do podszywania się pod legalnie działające instytucje finansowe i inne organizacje w celu pozyskania danych i poświadczeń klientów do logowania do bankowości elektronicznej, wykorzystywane następnie do kradzieży środków finansowych. Przestępcze działania i ataki realizowane są poprzez wszystkie dostępne kanały komunikacji zdalnej wykorzystywane również przez dostawców do kontaktów z klientami, tj. kanał telefoniczny, wiadomości SMS, wiadomości mailowe oraz social media, a

działania te są w czasie rzeczywistym dostosowywane przez przestępców do dynamicznie zmieniającej się rzeczywistości.

Od wielu lat zarówno instytucje finansowe, jak i organizacje działające na rzecz edukacji w zakresie cyberbezpieczeństwa, ostrzegają przed nierozważnym uruchamianiem linków otrzymywanych w wiadomościach SMS lub wiadomościach mailowych, zwracając uwagę na wysokie ryzyko poniesienia strat finansowych oraz ujawnienia i w konsekwencji przestępczego wykorzystania danych osobowych.

Prowadzone przez cyberprzestępców kampanie phishingowe wykorzystujące SMS oraz wiadomości mailowe do rozsyłania linków internetowych kierujących do fałszywych stron bankowości elektronicznej, pośredników płatności lub też stron zawierających złośliwe oprogramowanie wykradające poświadczenia klientów do logowania do bankowości elektronicznej są źródłem poważnych strat finansowych klientów. W związku z powyższym, organ nadzoru stoi na stanowisku, że wysyłanie aktywnych linków do stron internetowych w wiadomościach mailowych (włącznie z osadzaniem takich linków w grafikach) oraz wiadomościach SMS adresowanych do klientów, stoi w sprzeczności z tworzonym i od lat komunikowanym klientom przekazem związanym z ryzykiem utraty danych i środków finansowych i powinno zostać wyeliminowane z praktyki na rzecz informacji statycznych, nie generujących wskazanego wyżej ryzyka oszustwa lub na rzecz przekazywania klientom informacji poprzez aplikacje mobilne oraz portale bankowości elektronicznej.

Kolejnym istotnym czynnikiem ryzyka dotyczącym bezpieczeństwa środków finansowych i danych klientów jest sposób zabezpieczania komunikacji z klientem, prowadzonej z wykorzystaniem poczty elektronicznej. Stosowane przez dostawców praktyki polegające na zabezpieczaniu załączników przekazywanych w korespondencji mailowej prostymi hasłami, składającymi się np. z fragmentów numeru PESEL klienta, kombinacji elementów numeru PESEL z datą urodzenia, numerem telefonu lub innymi hasłami, które są możliwe do odgadnięcia przy pomocy ogólnodostępnych narzędzi informatycznych w skończonym czasie, organ nadzoru uznaje za nieakceptowalne ze względu na fakt, że informacje te noszą znamiona informacji chronionych bądź też zawierają dane osobowe, a budowanie prostych haseł jest sprzeczne z dobrymi praktykami w zakresie bezpieczeństwa.

Stosowana przez dostawcę umowna forma komunikacji z klientem oraz przyjęte w tej komunikacji metody jej ochrony powinny być poprzedzone pogłębioną analizą ryzyka, ukierunkowaną na zabezpieczenie danych i informacji uwzględniającą również aspekty użyteczności i jakości interakcji użytkownika z systemem bankowości elektronicznej (User eXperience). Analiza ta powinna w szczególności obejmować aspekty techniczne, w tym przypadku rozumiane jako stanowisko właściwej ds. cyberbezpieczeństwa komórki dostawcy, która będzie w stanie w rzetelny sposób oszacować czy planowany sposób zabezpieczania korespondencji można uznać za bezpieczny. Niewłaściwe zabezpieczenie tych danych może być wykorzystane w celach przestępczych np. do phishingu ukierunkowanego na konkretną osobę bądź grupę osób (spearphishing), a także skutkować naruszeniem ochrony danych

osobowych, narażając dostawcę na straty wizerunkowe oraz ryzyko nałożenia administracyjnej kary pieniężnej, zgodnie z art. 83 rozporządzenia 2016/679[2].

Mając na względzie potrzebę ograniczania niebezpiecznych z punktu widzenia organu nadzoru praktyk stosowanych przez dostawców, korespondencja mailowa zawierająca załączniki, zwłaszcza z danymi osobowymi, powinna być szyfrowana w sposób zapewniający poufność informacji, a hasło niezbędne do jej odszyfrowania powinno być przekazywane osobnym kanałem komunikacji, np. przez portal bankowości elektronicznej, aplikacje mobilną lub SMS.

Z kolei umożliwienie klientowi ustawienia w bankowości internetowej indywidualnego hasła do załączników przekazywanych drogą mailową, uwzględniającego powyższe założenia i zgodnego z polityką haseł przyjętą przez dostawcę, bądź informacja o umieszczeniu załącznika w systemie bankowości elektronicznej, są rozwiązaniami, które mogą przyczynić się do pogodzenia potrzeby zapewnienia bezpieczeństwa informacji z wygodnym dostępem klienta do tych informacji. Takie rozwiązania przyczynią się do zwiększenia bezpieczeństwa danych klienta bez zmniejszenia użyteczności zdalnych kanałów dostępu.

Kwestie edukacji i świadomość w obszarze cyberbezpieczeństwa są jednym z gwarantów bezpieczeństwa środków finansowych klientów i powinny być nadal adresowane przez dostawców usług bankowych. Jednakże dotychczasowe działania w tym obszarze są w ocenie nadzoru niewystarczające i nie przynoszą spodziewanych efektów, o czym świadczy skala skutecznych ataków na użytkowników usług bankowych i związany z tym poziom fraudów. W ocenie organu nadzoru budowanie świadomości klientów w zakresie cyberbezpieczeństwa nie powinno obecnie skupiać się tylko i wyłącznie na bezpieczeństwie bankowości elektronicznej i być prowadzone w formie ograniczonej do publikowania informacji na stronie internetowej dostawcy. Prowadzone przez część dostawców działania edukacyjne i kampanie medialne, znacząco wykraczające poza działania adresowanie tylko do swoich klientów, jak np. organizacja ogólnodostępnych szkoleń, aktywny udział w procesie edukacji, prowadzenie w mediach tradycyjnych kampanii społecznych budujących kulturę cyberbezpieczeństwa, powinno stać się udziałem wszystkich podmiotów sektora usług bankowych. Organ nadzoru zwraca uwagę, że ograniczenie działań edukacyjnych wykorzystujących jako medium przekazu Internet, prowadzi do ograniczenia lub pomijania pewnych grup konsumentów, co w konsekwencji skutkuje luką kompetencyjną w zakresie cyberbezpieczeństwa.

Takie podejście koresponduje z zaleceniami Rady Unii Europejskiej z 22 maja 2018 r. w sprawie kompetencji kluczowych w procesie uczenia się przez całe życie[3] , w których wskazuje się m.in. na udział czynnika biznesowego w kształtowaniu kompetencji cyfrowych społeczeństwa, charakteryzującego się krytycznym i odpowiedzialnym korzystaniem z technologii cyfrowych.

[2] Rozporządzenie Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.05.2016, str. 1 ze zm.)

[3] Zalecenia Rady z dnia 22 maja 2018 r. w sprawie w sprawie kompetencji kluczowych w procesie uczenia się przez całe życie (2018/C 189/01) (Dz. Urz. UE C 189 z 4.06.2018, str. 1)

Powyżej wskazane zagadnienia odnoszą się również do dynamicznie rozwijających się elektronicznych kanałów dostępu do usług bankowych w spółdzielczych kasach oszczędnościowo-kredytowych i krajowych instytucjach płatniczych. Informacje pozyskane w trybie nadzorczym wskazują na niską świadomość członków kas w obszarze zagrożeń i ryzyk związanych z korzystaniem z nowoczesnych technologii. Kasy i krajowe instytucje płatnicze powinny wdrożyć działania edukacyjne podnoszące świadomość istnienia zagrożeń w obszarze cyberbezpieczeństwa wśród swoich członków i klientów.

Przekazując powyższe organ nadzoru oczekuje, że wzmocnienie wspólnych i konsekwentnych działań w zakresie budowania świadomości klientów w obszarze cyberzagrożeń związanych z wykorzystaniem nowoczesnych technologii, będzie miało bezpośrednie przełożenie na poziom bezpieczeństwa ich środków finansowych. Działania dostawców usług bankowych w tym zakresie, ze szczególnym uwzględnieniem aspektów wskazanych w niniejszym piśmie, będą podlegały analizom i ocenom podczas czynności nadzorczych prowadzonych przez Komisję Nadzoru Finansowego.