EUROPEAN FINANCIAL CONGRESS

Instytut Badań
nad Gospodarką Rynkową
Do Studzienki Str. 63
80-227 Gdańsk, Poland

tel. +48 58 524 49 01
fax. +48 58 524 49 09

efc@ibngr.pl
www.efcongress.com

Stanowisko Europejskiego Kongresu Finansowego[1] w konsultacjach Europejskiego Urzędu Nadzoru Bankowego w sprawie wymogów dotyczących uwierzytelniania klientów i bezpieczeństwa komunikacji w ramach Dyrektywy PSD2[2]

Metodologia opracowania stanowiska

Opracowanie stanowiska przebiegało w czterech etapach.

Etap 1

Do wzięcia udziału w badaniu zaproszono grupę ekspertów obejmującą ponad 60 specjalistów. Przesłano im wybrane fragmenty dokumentu konsultacyjnego Europejskiego Urzędu Nadzoru Bankowego oraz przetłumaczone pytania konsultacyjne. Ekspertom zagwarantowana została anonimowość.

Etap 2

Do Instytutu Badań nad Gospodarką Rynkową wpłynęły 23 opinie od instytucji finansowych oraz indywidualnych ekspertów. Wszystkie odpowiedzi zostały zebrane i przedstawione w formie anonimowej ekspertom, którzy wzięli udział w konsultacjach. Zwrócono się do nich z prośbą o zaznaczenie w opiniach innych uczestników konsultacji tych sformułowań, które powinny znaleźć się w stanowisku końcowym, jak również tych, z którymi się nie zgadzają. Eksperci mogli także skorygować swoje odpowiedzi pod wpływem argumentów przedstawionych przez innych ekspertów.

Odpowiedzi uzyskano od:

- banków,
- firm z sektorów IT, FinTech, e-commerce oraz infrastruktury rynku finansowego,
- firm ubezpieczeniowych oraz funduszy inwestycyjnych,
- organów regulacyjnych,
- firm konsultingowych oraz kancelarii prawnych,
- środowiska akademickiego.

Etap 3

W ramach Projektu Europejskiego Kongresu Finansowego przeprowadzono seminarium na temat PSD2, w którym uczestniczyli eksperci zaproszeni do konsultacji.

Etap 4

Na bazie uzyskanych odpowiedzi opracowane zostało syntetyczne stanowisko Europejskiego Kongresu Finansowego.

---

[1] Celem Europejskiego Kongresu Finansowego (www.efcongress.com) jest debata nt. bezpieczeństwa i stabilności systemu finansowego Unii Europejskiej i Polski. Organizatorem EKF jest Instytut Badań nad Gospodarką Rynkową (IBnGR) – pierwszy niezależny think tank w Europie Środkowo-Wschodniej, założony w 1989 roku przez grupę ekonomistów związanych z opozycją demokratyczną i ruchem „Solidarność".

[2] www.eba.europa.eu/documents/10180/1548183/Consultation+Paper+on+draft+RTS+on+SCA+and+CSC+%28EBA-CP-2016-11%29.pdf

Odpowiedzi Europejskiego Kongresu Finansowego na pytania konsultacyjne

Pyt. 1

Czy zgadzacie się Państwo z argumentami EBA dotyczącymi silnego uwierzytelnienia klienta oraz wynikającymi stąd proponowanymi przepisami zawartymi w rozdziale 1 projektu regulacyjnych standardów technicznych (Regulatory Technical Standards, RTS)?

Generalnie zgadzamy się z argumentami EBA dotyczącymi konieczności wprowadzenia silnego uwierzytelniania (SCA – Strong Customer Authentication) a także z zaprezentowanymi propozycjami dotyczącymi procedury weryfikacji i wymogów. Dzisiejszy proces uwierzytelniania klienta stosowany przez instytucie prowadzące rachunki płatnicze (ASPSP) w Polsce w kontekście transakcji płatniczej jest już na zaawansowanym poziomie i wykorzystuje różnorakie rozwiązania (czyli np. kod autoryzacyjny jest przekazywany w postaci kodu sms, który klient wprowadza przez internet w celu potwierdzenia transakcji, ale również w ramach rozwiązania BLIK (system płatności elektronicznych oraz wypłat gotówkowych z bankomatów bazujący na aplikacji mobilnej) - klient najpierw pobiera kod sześciocyfrowy i w ramach procesu płatności wprowadza go na stronie internetowej po czym potwierdza kwotę i beneficjenta płatności w swoim telefonie komórkowym), dlatego sugerujemy aby nie definiować nowych wymogów zbyt szczegółowo i polegać na ocenie ryzyka stosowanej przez ASPSP. Szczególnie istotny w tym kontekście jest komentarz EBA, który sugeruje dowolność zastosowania rozwiązania technicznego, przy spełnieniu określonych warunków bezpieczeństwa, w tym kwestii dynamicznego łączenia kodu z kwotą i odbiorcą płatności (projekt RTS, str. 11, pkt 24-25), z czym się zgadzamy.

Należałoby jednak uwzględnić następujące sugestie:

1. W artykule 7 powinno się ograniczyć podmioty przeprowadzające taki audyt jedynie do „external independent and certified auditors". Wydaje się także, że należałoby wskazać konkretne okresy, w jakich takich audyt musi być dokonywany.
2. Doprecyzować środki mające ograniczyć ryzyko kradzieży lub przejęcia kontroli nad „multi-purpose device" – zdaniem niektórych ekspertów warto wskazać takie środki przynajmniej na zasadzie wyliczenia.
3. Dodać wymogi logicznej autoryzacji urządzenia – zdaniem niektórych ekspertów dodatkowym wymaganiem w artykule 1 pkt. 3e) powinno być wymaganie dotyczące nie tylko informacji o urządzeniu, ale także logiczna jego autoryzacja. Co oznacza, że zaufane urządzenie jest przypisane do klienta, tak jak to się obecnie praktykuje w aplikacjach bankowych.
4. Doprecyzować zasady generowania kodów autoryzacji – system powinien zapewnić bezpieczeństwo procesu autoryzacji uniemożliwiając odtworzenie (wygenerowanie) poprawnego kodu autoryzacji na podstawie większej, wcześniej wykorzystywanej, ilości kodów autoryzacji. Aktualnie artykuł 1 pkt. 2b) mówi wyłącznie o zabezpieczeniu polegającym na braku możliwości odtworzeniu poprawnego kodu autoryzacji na podstawie pojedynczego, wcześniej wykorzystanego kodu autoryzacji.
5. Określić sposób przechowywania poprawnych kodów autoryzacji – system powinien definiować sposób przechowywania (przetwarzania) poprawnych kodów autoryzacji, tak jak

to jest definiowane dla danych poufnych w opracowaniu Payment Card Industry Data Security Standards (PCI DSS).

6. Wskazać konieczność wykorzystania Public Key Infrastructure związany z udziałem Certificate Authority – zastosowanie standardu wymiany informacji „HTTP over TSL" (HTTPS) wymaga zastosowania zaufanego środowiska PKI (Public Key Infrastructure). W szczególności niedopuszczalne jest zastosowanie tzw. Self-signed certificates bez udziału strony zaufanej (Certificate Authotity). Jeżeli dokument wskazuje protokół HTTPS, powinien również wskazać konieczność zastosowania PKI.

Ponadto zdaniem części ekspertów warto rozważyć:

i. Konieczność szerszego uwzględnienia wymogów doświadczenia użytkownika i klienta (UX, CX) – przykładem dotyczącym uwzględnienia doświadczenia klienta może być zapis art. 2 pkt 2 b) – wymóg zastosowania oddzielnego kanału, aplikacji i urządzenia do komunikacji w celu potwierdzania szczegółów transakcji. Bezwzględne wprowadzenie tego wymogu pogorszy jakość usług świadczonych poprzez aplikacje mobilne służące do realizacji płatności. W przypadku płatności mobilnych użytkownicy usług płatniczych korzystają z jednego urządzenia i aplikacji w celu dokonania, weryfikacji i autoryzowania transakcji.

   Dlatego część ekspertów sugeruje zastosowanie w RTS odpowiednich wyłączeń od zasady odrębności kanałów adekwatnie do zastosowanej technologii i polityki zarządzania ryzykiem przez PSP, a także, że powinny być określone mniej restrykcyjne reguły dotyczące SCA dla płatności typu one-click oraz płatności powtarzalnych (automatycznych).

   Należy jednak stwierdzić, że w razie zainstalowania na urządzeniu złośliwego oprogramowania, brak rozdzielenia kanałów może zagrozić bezpieczeństwu użytkownika i jego środków finansowych.

ii. Możliwość oparcia się na ocenie ryzyka oraz uzgodnionych zasadach „liability shift" pomiędzy ASPSP a PSP – według jednego z ekspertów tzw. zasada „przeniesienia odpowiedzialności" chroni użytkowników przed poniesieniem strat. Tego rodzaju przeniesienie Odpowiedzialności stosuje się w przypadku kart płatniczych, na czym korzystają zarówno sprzedawcy, jak i kupujący. Sprzedawcy mogą oferować klientom większą wygodę i sprawną obsługę transakcji, w tym płatność za jednym kliknięciem. Wszystko to jest dziś możliwe, ponieważ centra autoryzacyjne/PSP mogą przyjąć podejście oparte na ryzyku, które często zapewnia taki sam poziom bezpieczeństwa jak SCA. EBA powinna rozważyć możliwość oparcia tego podejścia w większej mierze na ryzyku i na kwestiach praktycznych niż na sztywnych zasadach. Powinna istnieć możliwość niestosowania SCA, jeżeli ASPSP oraz PSP ustalą zasady „przeniesienia odpowiedzialności", jak ma to miejsce w przypadku obsługi kart płatniczych (gdzie organizacje płatnicze odpowiadają za wyznaczanie zasad funkcjonowania systemu) lub umów dwustronnych pomiędzy emitentami instrumentów płatniczych a ich nabywcami.

<u>Pyt.2</u>

W szczególności, czy w odniesieniu do procedury „dynamicznego linkowania" zgadzacie się Państwo z argumentami EBA, zgodnie z którymi projektowany standard nie powinien przesądzać, kiedy „dynamiczne linkowanie" powinno mieć miejsce, pod warunkiem, że kanał, aplikacja mobilna lub urządzenie udostępniające informacje o wysokości kwoty i tożsamości odbiorcy płatności z tytułu transakcji są niezależne lub odrębne od kanału, aplikacji

mobilnej albo urządzenia, za pomocą którego płatność została zainicjowana, jak to opisano w paragrafie 2.2 projektu RTS?

Warto szerzej wyjaśnić pojęcie rozdzielenia kanału, aplikacji mobilnej lub urządzenie udostępniającego informacje o wysokości kwoty i tożsamości odbiorcy płatności z tytułu transakcji od kanału, aplikacji mobilnej albo urządzenia, za pomocą którego płatność została zainicjowana. W związku z tym należy doprecyzować zapisy określające wymogi w tym zakresie. Wydaje się, że rozdzielenie informacji o wysokości kwoty i tożsamości odbiorcy od kanału, w którym płatność została zainicjowana może zostać zrealizowane na tym samym fizycznym urządzeniu.

Może się to odbywać na przykład za pomocą innych sesji, w ramach których są inicjowane zlecenia oraz przesyłany kod uwierzytelniający lub też poprzez wykorzystanie 2 kanałów SSL. W takim przypadku proponowane rozwiązania nie pogorszyłyby funkcjonowania aplikacji mobilnych w stosunku do tego, co jest obserwowane dzisiaj na rynku polskim.

Jeżeli taka definicja nie zostanie zastosowana to eksperci zwracają uwagę na możliwe pogorszenie jakość usług świadczonych za pośrednictwem aplikacji mobilnych wykorzystywanych do realizacji płatności. W przypadku płatności mobilnych użytkownicy usług płatniczych korzystają w praktyce z jednego urządzenia i aplikacji w celu wykonania, weryfikacji i autoryzacji transakcji. W takiej sytuacji warto rozważyć zastosowanie w RTS odpowiednich włączeń od zasady odrębności kanałów adekwatnie do zastosowanej technologii i polityki zarządzania ryzykiem przez dostawcę usług.

Dodatkowo uważamy, że określenie zasad dynamicznego linkowania powinno w szerszym zakresie bazować na ocenie ryzyka przeprowadzonej przez ASPSP. Wynika to z tego, że Standard przewiduje, iż gdy dochodzi do oszustwa spowodowanego niedostatecznymi zabezpieczeniami stosowanymi przez ASPSP, a skutkującego stratami dla klienta, odpowiedzialność finansowa ponosi ASPSP. Zatem, przy odpowiednio wysokich wymogach minimalnych, można mu pozostawić decyzję w sprawie restrykcyjności stosowanych środków bezpieczeństwa.

<u>Pyt. 3</u>
W szczególności, czy w odniesieniu do ochrony elementów uwierzytelnienia znane są inne zagrożenia, oprócz tych wymienionych w paragrafach 3, 4 i 5 projektu RTS, przed którymi elementy uwierzytelnienia powinny być zabezpieczone?

Większość ekspertów wskazuje na to, że definicje zawarte w artykułach 3 – 5 są bardzo pojemne i obejmują już swoim zakresem wystarczający zbiór potencjalnych ryzyk. Naszym zdaniem projekt RTS zawiera wystarczającą listę zagadnień w zakresie ochrony elementów uwierzytelniania, przy czym wg nas taka lista nie powinna być listą specyficznie zdefiniowaną. Powinno się raczej podawać przykładowe składowe definicji, gdyż stopień i tempo rozwoju świata przestępczego w omawianym obszarze jest bardzo duże i na obecnym etapie nie da się w przepisach odpowiednio przewidzieć wszystkich możliwych scenariuszy.

Przykłady ryzyk oraz metod ich ograniczenia obejmują:

1. Zagadnienia wymagane przez regulacje kartowe (Payment Card Industry Data Security Standard):
    a. Budowa i zarządzania systemem uwierzytelniania

b. Zabezpieczenia składowania danych poufnych wymaganych do pracy systemu uwierzytelniania
c. Wykrywanie i eliminacji błędów w systemie uwierzytelniania
d. Budowa i zarządzania systemem kontroli prawami dostępu do systemu uwierzytelniania

2. Zasady zarządzania certyfikatami – nadawanie / odbieranie certyfikatów; sposób wymiany informacji między podmiotami.
3. Behawioralne i „inteligentne" systemy oceny ryzyka bazujące na niestandardowych i niedozwolonych działaniach użytkownika. Część podmiotów wnioskuje, że w przypadku stwierdzenia tego typu zachowań (nawet pomimo certyfikacji AIS/ PIS) odpowiedni ASPSP powinien mieć możliwość odmówienia dostępu lub wykonania usługi.

Pyt. 4

Czy zgadzacie się Państwo z argumentami EBA w sprawie wyjątków od obowiązku stosowania silnego uwierzytelnienia klienta i środków bezpieczeństwa, zgodnie z artykułem 97 PSD 2 oraz wynikającą stąd propozycją przepisów zawartych w rozdziale 2 projektu RTS?

EBA w projekcie RTSów de facto usztywniła swoje stanowisko w zakresie dozwolonych wyjątków dla procedury silnego uwierzytelniania klienta, w porównaniu do swoich Wytycznych z sierpnia 2015 roku dotyczących bezpieczeństwa płatności internetowych. Naszym zdaniem jednolite i sztywne określanie wyjątków od procedury silnego uwierzytelnienia, której stosowanie jest obowiązkiem banku, nie jest dobrym rozwiązaniem. Tempo rozwoju świata przestępczego i stosowanych przez niego technik w omawianym obszarze, jest bardzo duże i dlatego sztywne definiowanie sposobu podejścia do wyłączeń z jednej strony niewystarczająco zabezpiecza banki przed przyszłymi scenariuszami przestępstw, jak również nie pozwala stosować zaawansowanych technik zarządzania ryzykiem w tej dziedzinie. Na całości zaś straci doświadczenie klienta. Według nas stosowany w Polsce balans pomiędzy silnym uwierzytelnianiem sensytywnych operacji i transakcji płatniczych a prostym, pasywnym dostępem online do konta klienta bez dodatkowego uwierzytelniania jest lepszym rozwiązaniem.

Z zebranych głosów wyłaniają się dwie istotne uwagi do propozycji przedstawionych w rozdziale 2 RTS. Pierwsza grupa uwag dotyczy poziomu limitów określonych w artykule 8 (50 i 150 EUR dla contactless payment electronic transactions oraz 10 i 100 EUR dla remote electronic payment transactins). Zdecydowana większość ekspertów wyraża pogląd, że maksymalne kwoty transakcji niewymagających silnego uwierzytelniania powinny być definiowane na poziomie krajowym w oparciu m.in. o inne uwarunkowania lokalne (np. limity dla transakcji kartowych, realną wartość nabywczą pieniądza itd.).

Druga uwaga wyrażana przez większość środowiska finansowego w Polsce dotyczy dopuszczenia możliwości uwzględnienia bardziej restrykcyjnej również listy wyjątków od SCA na podstawie wyników analizy ryzyka przeprowadzonej przez ASPSP lub też potraktowanie zaprezentowanej listy odstępstw jako maksymalnych. W takiej sytuacji ASPSP miałyby możliwość wprowadzania dodatkowych wymogów dotyczących SCA, np. w oparciu o własne algorytmy oceny ryzyka.

Możliwe do zastosowania dodatkowe mechanizmy dotyczące oceny ryzyka (lub też dodatkowe wyłączenia z SCA) dla poszczególnych transakcji mogłyby dodatkowo uwzględniać czynniki ryzyka nieujęte dziś w regulacjach takie jak np.:

1. wartości dotyczące prędkości realizacji transakcji,
2. położenie geograficzne określane na podstawie geolokalizacji adresu IP, położenia telefonu komórkowego lub sprzedawcy
3. przyzwyczajenia związane z rodzajem towaru - np. biżuteria, zabawki, żywność
4. przyzwyczajenia związane z rodzajem dostawy - np. wysyłka elektroniczna (wirtualna) a standardowa
5. wykorzystywane urządzenie:
    a. komputer osobisty - używanie plików typu „cookies" i identyfikacja urządzenia oraz w razie potrzeby indywidualne certyfikaty
    b. urządzenia mobilne (telefony, tablety, smartwatche) - unikatowy identyfikator aplikacji mobilnej, jeżeli jest stosowany, lub identyfikator urządzenia
    c. Internet rzeczy (telewizory, lodówki) - unikatowy identyfikator urządzenia

Powyższe elementy powinny być wykorzystywane do monitorowania transakcji i zachowania użytkownika w celu wykrywania nieoczekiwanych aktywności, w przypadku których istnieje możliwość zastosowania silnego uwierzytelniania.

Stoimy także na stanowisku, że przy stosowaniu różnych czynników związanych z profilem i zachowaniem klienta można je uznać za samodzielny element o charakterze przyrodzonym użytkownikowi. W odróżnieniu od niektórych innych elementów wykorzystywanych do silnego uwierzytelniania (np. tymczasowe kody SMS, których bezpieczeństwo ogranicza możliwość utraty urządzenia mobilnego przez użytkownika) wzorców zachowania nie można łatwo i szybko zmienić.

Dodatkowo oprócz opisanych powyżej zostały wskazane specyficzne wyjątki, które powinny być uwzględnione w wyłączeniach lub też ograniczenia od wskazanych wyłączeń:

1. Odnośnie artykułu 8 pkt 1 a – okres po jakim Użytkownik musi ponownie użyć silnego uwierzytelnienia powinien być uzależniony od precyzyjnie zdefiniowanego rodzaju danych jakie są dostępne po uwierzytelnieniu.
2. Odnośnie artykułu 8 pkt 1 b – doprecyzowanie sposobu liczenia limitów kumulatywnych 150 EUR np. okresu czasu branego pod uwagę
3. Odnośnie artykułu 8 pkt 2 a – lista zaufanych adresatów płatności powinna być zabezpieczona przed nieautoryzowaną zmianą. Wszelkie zmiany dotyczące listy zaufanych adresatów płatności powinny być audytowane (kto, kiedy, jak dokonał zmiany). Należy jeszcze raz podkreślić, że szczególnie to wyłączenie powinno podlegać dodatkowej ocenie ryzyka ASPSP, ponieważ znane są na rynku polskim przypadki fraudów z wykorzystaniem tego mechanizmu.
4. Odnośnie artykułu 8 pkt 2 d – doprecyzowanie sposobu liczenia limitu kumulatywnego 100 EUR np. okresu czasu branego pod uwagę.

Pyt. 5

Czy macie Państwo uwagi do listy wyjątków zawartych w rozdziale 2 projektu RTS przy założeniu, że dostawcy usług płatniczych nie będą mogli stosować silnych algorytmów uwierzytelniania w przypadku transakcji, które znajdują się na liście wyjątków?

Generalnie, ponownie większość ekspertów za zdecydowanie lepsze uważa rozwiązanie, które uwzględnia indywidualną ocenę ryzyka dla każdej transakcji i na tej podstawie podejmowanie ostatecznej decyzji przez ASPSP o konieczności wykorzystania silnego uwierzytelnienia.

Zakładamy, że stosowanie wyjątków zgodnie z podanymi definicjami będzie jednak opcjonalne dla banków. Innymi słowy, jeżeli bank podejmie informację, że konto klienta może być przedmiotem ataku przestępczego, procedura silnego uwierzytelniania w takich przypadkach zawsze będzie mogła być zastosowana (np nawet dla transakcji o bardzo niskiej wartości). Ostateczną decyzję w tym zakresie będzie mógł zawsze podjąć bank.

Podejście to opiera się na zasadzie, że odpowiedzialność spoczywa na podmiotach świadczących usługi płatnicze, zaangażowanych w transakcję. Podmiot obsługujący płatność powinien mieć możliwość podjęcia potencjalnie dodatkowych czynności uwierzytelniających w oparciu o własne polityki i procedury bezpieczeństwa. W przypadku wystąpienia nieoczekiwanego zachowania ryzyko związane z ewentualnym przyznaniem przedłużenia powinno w szczególności obciążać usługodawcę.

Dodatkowo wydaje się, że limity dotyczące poszczególnych rodzajów transakcji powinny być ustalane na poziomie krajowym w oparciu m.in. o inne uwarunkowania lokalne (np. limity dla transakcji kartowych, realną wartość nabywczą pieniądza itd.).

Pyt. 6

Czy zgadzacie się Państwo z argumentami EBA w sprawie ochrony poufności i integralności spersonalizowanych danych logowania użytkownika usług płatniczych oraz wynikających stąd proponowanych przepisów zawartych w rozdziale 3 projektu RTS?

Instytucje prowadzące rachunki płatnicze (ASPSP) w Polsce, w tym w szczególności sektor bankowy , w sposób fundamentalny traktują zasadę ochrony danych do logowania użytkownika, od wielu lat stosując praktykę i wymóg nieujawniania tych danych osobom trzecim przez użytkownika. Zasada ta jest zawarta zarówno w dokumentacji umownej z klientem, jak również jest ona powtarzana w ramach nieustannej edukacji klientów, od wielu lat. Proponowana w RTSach zmiana, czyli brak jednoznacznego określenia zakazu przekazywania danych do logowania poza instytucje prowadzącą rachunek płatniczy klienta, jest przez nas oceniana bardzo negatywnie. Wydaje się ona wprost wychodzić naprzeciw oczekiwaniom świata przestępczego i w sposób niezmiernie istotny zwiększa prawdopodobieństwo powodzenia akcji przestępczych skierowanych wobec klientów, w tym w szczególności ataków phishingowych. Uważamy, że istnieją w praktyce rozwiązania, które mogą spełniać oczekiwania regulatora zawarte w PSD2, które nie polegają na przekazywaniu stronom trzecim danych do logowania.

Zgadzamy się z przedstawionymi propozycjami rozwiązań zawartymi w rozdziale 3 RTS.

Należy podkreślić, że na rynku polskim PSP przy wsparciu regulatorów wypracowały i przezlata propagowały wśród PSU odpowiednie standardy i niedopuszczalne w naszym przekonaniu byłoby zezwalanie na rozluźnienie tych reguł, które mogłoby prowadzić do ujawniania lub przyzwolenia na ujawnianie przedmiotowych danych stronom trzecim.

W tym kontekście chcemy zwrócić uwagę na stosowane w Polsce w świecie ecommerce pay-by-linki (przekierowanie klienta na stronę jego banku, na której, po zalogowaniu, pojawia się wypełniony formularz przelewu) - to rozwiązanie powinno zostać szczegółowo przeanalizowane przez EBA w celu potencjalnego zastosowania takiego podejścia przy implementacji PSD2 i omawianych RTSów.

Pyt. 7

Czy zgadzacie się Państwo z argumentami EBA dotyczącymi wymagań stawianych powszechnym i bezpiecznym otwartym standardom komunikacji w zakresie identyfikacji, uwierzytelniania, powiadamiania i udostępniania informacji oraz wynikających stąd proponowanych przepisów zawartych w rozdziale 4 projektu RTS?

Stosowanie w jak największym stopniu powszechnie akceptowanych standardów zapewni wszystkim uczestnikom rynku podstawę stabilnego rozwoju działalności. Rozwiązanie otwartego i wystandaryzowanego API, które umożliwi dostęp podmiotów trzecich do rachunków klientów w bankach wydaje się bezpieczniejsze od bardzo ryzykownego modelu dzielenia się danymi uwierzytelniającymi z podmiotem trzecim (screen scraping).

Niemniej należy zaznaczyć, że wprowadzenie nowej kategorii interfejsów dla potrzeb komunikacji z AIS/PSP, PIS/PSP, PSP wydającym karty będzie z pewnością znaczącym, a także kosztownym wyzwaniem wdrożeniowym dla ASPSP, posiadających zwykle złożoną infrastrukturę do obsługi płatności, działającą w oparciu także o inne standardy niż proponowane w RTS, szczególnie w obszarze kart.

Zgodnie z propozycją EBA w zakresie opracowania standardów komunikacji w oparciu o wymogi międzynarodowych lub europejskich organizacji normalizacyjnych pragniemy podkreślić, że w niektórych krajach (w tym w Polsce) możemy już zaobserwować rozwiązania pozwalające na komunikację pomiędzy ASPSP a TPP. Dlatego też jesteśmy przekonani, że powinna istnieć możliwość opracowania norm opartych także na standardzie ISO 20022. Ważne jest jednak zapewnienie ogólnoeuropejskiego rozwiązania API, które będzie mogło funkcjonować na różnych rynkach lokalnych. W państwach europejskich prowadzi się obecnie kilka inicjatyw zmierzających do wdrożenia krajowych norm (np. CAPS, CSI, UK Open Banking Group czy Berlin Group). Znacząco różnią się one od siebie pod względem modeli technicznych, operacyjnych i biznesowych.

Ponadto wyjaśnienia wymaga kwestia po czyjej stronie będzie odpowiedzialność za zapewnienie wystarczających środków na pokrycie kosztu transakcji oraz ryzyko ich braku. Dostawcy usług płatniczych prowadzącego rachunek (ASPSP), wydawcy karty (PSP) czy jej użytkownika (PSU)? Na to pytanie nie dają odpowiedzi zapisy Dyrektywy PSD 2 wprost zakazujące blokowania kwot na rachunku przez dostawcę usług płatniczych prowadzącego rachunek art. 65 pkt. 4 Dyrektywy PSD 2. Dlatego wskazane jest doprecyzowanie zapisów w ramach wydawania RTS lub wdrażania Dyrektywy PSD 2 do prawodawstwa krajowego w zakresie odpowiedzialności za zapewnienie środków na pokrycie kosztów transakcji inicjowanej z przez PSP wydawcę karty z rachunku prowadzonego przez ASPSP.

Uważamy jednak, że w RTS brakuje zapisów zabezpieczających instytucje prowadzące rachunki płatnicze (ASPSP) przed nieoczekiwanymi skutkami zwiększonej ilości zapytań i komunikacji ze strony AIS/PIS, co w pierwszej kolejności może się potencjalnie negatywnie odbić na jakości obsługi całej bazy istniejących klientów. Uważamy, iż w tym zakresie wprost powinno

przewidywać się procedury nadzwyczajne, gdzie instytucja prowadząca rachunek płatniczy mogłaby podejmować działania ochronne w w/w sytuacji. RTSy w niewystarczający sposób definiują obowiązki oraz odpowiedzialność Third Party Providers (AIS/PIS) w przypadku awarii czy incydentów bezpieczeństwa, pozostawiając sporą przestrzeń do interpretacji i dowolności, co szczególnie w omawianej tu tematyce bezpieczeństwa jest według nas niewskazane.

Pyt. 8

W szczególności, czy należy wymagać używania elementów, komponentów i zatwierdzonych definicji komunikatów ISO 20022 (jeśli takie są dostępne), aby – pomimo stosowania różnych technik – umożliwić komunikację pomiędzy firmami oferującymi systemy obsługi płatności w celu udostępniania usług AIS (Account Information System – informacja o koncie), PIS (Payment Initiation System – inicjowanie płatności) i usług potwierdzania dostępności środków finansowych na koncie? Czy są przeszkody techniczne, które uniemożliwiłyby wdrożenie takich standardów?

Propozycje ujednolicenia standardów w postaci używania elementów, komponentów i zatwierdzonych definicji komunikatów ISO 20022 mogą być traktowane jako jak najbardziej słuszne. Z tej perspektywy, z pewnością usprawnią one komunikację pomiędzy firmami oferującymi systemy obsługi płatności, pomimo stosowania różnych technik i rozwiązań, ponieważ większość firm płatniczych szeroko stosuje standardy ISO 20022.Również odniesienie do standardów bezpieczeństwa określonych w normie 27001 jest jak najbardziej uzasadnione.

Niezależnie jednak od samego określenia norm w zakresie bezpieczeństwa warto na etapie definiowania RTS oraz określenia zasad dla poszczególnych uczestników rynku i regulatorów przewidzieć sposób weryfikowania i audytu wdrożenia standardów bezpieczeństwa (w tym w szczególności wdrożenia ISO 27001 przez TPP), wyników analiz ryzyka i klasyfikacji informacji na których opiera się TPP mając dostęp do wrażliwych informacji.

Ponadto RTS wyraźnie uprzywilejowują obecnie uznane standardy komunikacyjne. Brak w RTS precyzyjnego określenia kiedy dany nowy standard można będzie traktować jako międzynarodowy/europejski standard zgodny z wymogami RTS. Trudno będzie uznać za zgodny z wymogami określonymi w RTS jakikolwiek nowy standard powstały w jednym państwie, dopóki nie zostanie zastosowany poza tym państwem. Bez jasnego określenia takich warunków nie ma możliwości by nowy standard krajowy został uznany za standard międzynarodowy zgodny z RTS.

Pyt. 9

W odniesieniu do wzajemnej identyfikacji dostawców usług płatniczych, czy certyfikaty stron internetowych wystawiane przez kwalifikowanych dostawców usług zaufania zgodnie z polityką e-IDAS byłyby właściwe i pozwalałyby na używanie wszystkich popularnych urządzeń – takich jak komputery, tablety i telefony komórkowe – do wykonywania różnych usług płatniczych?

Podzielamy stanowisko EBA w zakresie konieczności certyfikowania pośredników w dostępie do rachunku przez dedykowane urzędy powołane w ramach dyrektywy e-IDAS. W naszej ocenie ten aspekt istotnie wpłynie na kwestie związane z weryfikacją PSP w rejestrach przed wydaniem certyfikatu i przyjęciem odpowiedzialności przez podmiot wydający certyfikat. Takie podejście powinno jednocześnie zapewnić skuteczną ochronę i stabilność usług wykonywanych w oparciu

o Dyrektywę PSD 2. Zasada oparcia bezpieczeństwa wymiany informacji o kwalifikowane certyfikaty jest jak najbardziej słuszna i nie utrudnia korzystania ze wskazanych urządzeń.

Poza stosowaniem certyfikatów kwalifikowanych dla stron internetowych należy również rozważyć możliwość wykorzystania kwalifikowanych certyfikatów pieczęci elektronicznych (zgodnych z e-IDAS), szczególnie biorąc pod uwagę, że taki sposób będzie bardziej adekwatny w przypadku komunikacji z użyciem API.

Zwracamy jednocześnie uwagę, że nie ma jeszcze na rynku polskim potwierdzonej praktyki certyfikacji zgodnej z e-IDAS, w tym zgodnie z naszą najlepszą wiedzą nie ma jeszcze na rynku kwalifikowanych dostawców usług zaufania. Dlatego też ostateczne potwierdzenie w praktyce skuteczności zapewnienia bezpieczeństwa na podstawie certyfikatów zgodnych z e-IDAS będzie możliwe dopiero w przyszłości.

Pyt. 10

W odniesieniu do tego, jak często dostawcy usług AIS mogą żądać danych z wyznaczonych rachunków płatniczych, gdy użytkownik usług płatniczych nie zwraca się wprost o takie dane, czy proponowany limit dwóch żądań dziennie jest właściwym kompromisem między umożliwieniem dostawcom usług AIS dostarczania aktualnych informacji użytkownikom tych usług z jednej strony i zapewnieniem niezakłóconego dostępu do interfejsu komunikacyjnego dostawców usług ASPSP (account servicing payment service provider) z drugiej strony? Jeśli nie, to jaka byłaby właściwa częstotliwość i dlaczego?

Stanowisko poszczególnych ekspertów wypowiadających się w kwestii wykorzystania danych z rachunków płatniczych wtedy gdy użytkownik nie zwraca się wprost o takie dane nie jest jednolite. Spotkaliśmy się w tym zakresie ze skrajnymi opiniami, m.in. mówiącymi o potrzebie nieograniczonego dostępu do informacji z rachunków bez dodatkowego silnego uwierzytelnienia ze strony klienta. Po rozważeniu wszystkich argumentów opowiadamy się zdecydowanie po stronie rozwiązania przeciwnego, czyli wyłączenia możliwości pobierania informacji na temat rachunków klientów bez dodatkowego zgłoszenia ze strony klienta ze względów bezpieczeństwa.

Obecna technika zapewnia możliwość dostatecznie szybkiego odczytania wszystkich danych niezbędnych do udzielenia odpowiedzi klientowi w przypadku zapytania z jego strony bez konieczności zapytań generowanych automatycznie bez udziału klienta.

Sięganie do rachunków w regularnych odstępach czasu, a nie na żądanie użytkownika, będzie umożliwiało śledzenie stanu rachunku, operacji na nim, pozwoli gromadzić dane o charakterze behawioralnym, w szczególnych sytuacjach umożliwiające podszywanie się pod klienta. Taka informacja w rękach grup przestępczych bezbłędnie wskazywałaby osoby, które warto by było okraść oraz wskazywała mechanizmy jak to zrobić. Dlatego należałoby raz jeszcze przemyśleć celowość usługi AIS i oszacować ryzyko związane z jej funkcjonowaniem.

Uważamy, że w zakresie dostępu do rachunku klienta (usługi typu AIS), tego typu dostęp powinien każdorazowo być świadomie inicjowany przez klienta. Według nas nie zachodzi więc potrzeba definiowania liczby zapytań automatycznych.

Jednocześnie doprecyzowania wymaga kwestia czy dopuszczenie żądania dostępu do informacji o rachunku (AIS), jeśli zostanie jednak wprowadzone, objęte będzie rygorem stosowania silnego uwierzytelnienia wobec użytkownika, tj. co najmniej raz na miesiąc (zgodnie z Projektem RTS). Brak tego wymogu bezpośrednio w Projekcie RTS może spowodować niespójność procedur

bezpieczeństwa w zakresie dostępu do informacji o rachunku bezpośrednio przez użytkownika oraz za pośrednictwem AIS. W naszej opinii reguły uwierzytelnienia powinny być wspólne, a jednocześnie dostawca usług prowadzący rachunek powinien mieć możliwość wymuszenia stosowania silnego uwierzytelnienia zgodnie z wewnętrznymi politykami zarządzania ryzykiem.