EBA/GL/2014/12_Rev1

19 grudnia 2014 r.

Wytyczne końcowe

w sprawie bezpieczeństwa płatności internetowych

Spis treści

Wytyczne w sprawie bezpieczeństwa płatności internetowych

Status Wytycznych

Niniejszy dokument zawiera wytyczne wydane na podstawie art. 16 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1093/2010 z dnia 24 listopada 2010 r. w sprawie ustanowienia Europejskiego Urzędu Nadzoru (Europejskiego Urzędu Nadzoru Bankowego), zmieniającego decyzję nr 716/2009/WE oraz uchylającego decyzję Komisji 2009/78/WE („rozporządzenie w sprawie EUNB"). Zgodnie z art. 16 ust. 3 rozporządzenia w sprawie EUNB właściwe organy i instytucje finansowe dokładają wszelkich starań, aby zastosować się do wytycznych.

Wytyczne określają stanowisko EUNB w sprawie właściwych praktyk nadzorczych w ramach Europejskiego Systemu Nadzoru Finansowego lub sposobu, w jaki należy zastosować prawo unijne w danym obszarze. Zgodnie z powyższym EUNB oczekuje, iż wytyczne będą przestrzegane przez wszystkie właściwe organy i instytucje finansowe, do których są skierowane. Właściwe organy, wobec których wytyczne mają zastosowanie, powinny ich przestrzegać poprzez odpowiednie włączenie ich do swoich praktyk nadzorczych (np. poprzez zmianę swoich ram prawnych lub procesów w zakresie nadzoru), w tym także w przypadku, gdy wytyczne skierowane są głównie do instytucji finansowych.

Wymogi w zakresie sprawozdawczości

Zgodnie z art. 16 ust. 3 rozporządzenia w sprawie EUNB każdy właściwy organ ma obowiązek powiadomić Urząd do dnia 5 maja 2015 r. o tym, czy stosuje się lub zamierza stosować się do niniejszych wytycznych, a w przypadku, gdy nie stosuje się lub nie zamierza stosować się do wytycznych, musi przekazać Urzędowi stosowne uzasadnienie. W przypadku nieprzekazania Urzędowi powiadomienia w wyznaczonym terminie Urząd przyjmuje, że dany właściwy organ nie stosuje się do wytycznych. Powiadomienia należy przesyłać za pomocą formularza znajdującego się w pkt 5 na adres compliance@eba.europa.eu z dopiskiem „EBA/GL/2014/12". Powiadomienia powinny składać osoby posiadające odpowiednie uprawnienia do zgłaszania zgodności w imieniu swojego właściwego organu.

Powiadomienia zostaną opublikowane na stronie internetowej EUNB zgodnie z art. 16 ust. 3.

Tytuł I Zakres stosowania i definicje

Zakres

1. Niniejsze wytyczne określają zakres wymogów minimalnych dotyczących bezpieczeństwa płatności internetowych. Wytyczne opracowano w oparciu o zasady określone w dyrektywie 2007/64/WE[1] („dyrektywa w sprawie usług płatniczych") dotyczące wymogów informacyjnych odnoszących się do usług płatniczych i obowiązków dostawców usług płatniczych w zakresie świadczenia usług płatniczych. Ponadto art. 10 ust. 4 dyrektywy wymaga od instytucji płatniczych posiadania solidnych zasad zarządzania oraz odpowiednich mechanizmów kontroli wewnętrznej.

2. Wytyczne dotyczą świadczenia usług płatniczych oferowanych przez dostawców usług płatniczych przez internet zgodnie z definicją zawartą w art. 1 dyrektywy.

3. Wytyczne są skierowane do instytucji finansowych zdefiniowanych w art. 4 ust. 1 rozporządzenia (UE) nr 1093/2010 i do właściwych organów zdefiniowanych w art. 4 ust. 2 rozporządzenia (UE) nr 1093/2010. Właściwe organy w 28 państwach członkowskich Unii Europejskiej powinny zapewnić stosowanie niniejszych wytycznych przez dostawców usług płatniczych zdefiniowanych w art. 1 dyrektywy w sprawie usług płatniczych podlegających ich nadzorowi.

4. Dodatkowo właściwe organy mogą wymagać od dostawców usług płatniczych sprawozdawczości potwierdzającej spełnienie wytycznych.

5. Wytyczne nie naruszają ważności „zaleceń w sprawie bezpieczeństwa płatności internetowych" („Sprawozdanie")[2]. W szczególności Sprawozdanie nadal stanowi dokument, na podstawie którego banki centralne – wypełniając swoją funkcję nadzorowania systemów płatności i instrumentów płatniczych – powinny oceniać przestrzeganie obowiązujących wymogów w zakresie bezpieczeństwa płatności internetowych.

6. Wytyczne określają oczekiwania minimalne. Nie ograniczają one odpowiedzialności dostawców usług płatniczych za monitorowanie i ocenę ryzyk związanych z ich operacjami płatniczymi, opracowywanie własnych szczegółowych polityk bezpieczeństwa oraz wdrażanie środków w zakresie planowania awaryjnego, zarządzania incydentami i ciągłości działania, współmiernych do ryzyk związanych ze świadczonymi usługami płatniczymi.

7. Celem wytycznych jest określenie wspólnych minimalnych wymogów w odniesieniu do usług płatności internetowych określonych poniżej, niezależnie od urządzenia dostępowego:

[1] Dyrektywa Parlamentu Europejskiego i Rady 2007/64/WE z dnia 13 listopada 2007 r. w sprawie usług płatniczych w ramach rynku wewnętrznego zmieniająca dyrektywy 97/7/WE, 2002/65/WE, 2005/60/WE i 2006/48/WE i uchylająca dyrektywę 97/5/WE, Dz.U. L 319, 5.12.2007,

[2] http://www.ecb.europa.eu/press/pr/date/2013/html/pr130131_1.en.html

- [karty] realizacja płatności kartą przez internet, w tym przy użyciu kart wirtualnych, jak również rejestrowanie danych płatności kartą w celu ich wykorzystania w ramach „rozwiązań portfelowych”;

- [polecenia przelewu] realizacja poleceń przelewu przez internet;

- [polecenia zapłaty] wydawanie i modyfikacje elektronicznych poleceń zapłaty;

- [pieniądz elektroniczny] przelewy pieniądza elektronicznego pomiędzy dwoma rachunkami przez internet.

8. W przypadku gdy wytyczne przewidują osiągnięcie danego rezultatu, rezultat ten można osiągać różnymi metodami. W niniejszych wytycznych, oprócz wymogów określonych poniżej, zawarto również przykłady najlepszych praktyk (załącznik 1), do których stosowania zachęca się dostawców usług płatniczych, lecz które nie są obowiązkowe.

9. Gdy usługi i instrumenty płatnicze są oferowane za pośrednictwem systemu płatności (np. systemów płatności kartą, systemów poleceń przelewów, systemów poleceń zapłaty itp.), właściwe organy i właściwy bank centralny wypełniające funkcję nadzorczą w odniesieniu do instrumentów płatniczych powinny kontaktować się ze sobą w celu zapewnienia spójnego stosowania wytycznych przez podmioty odpowiedzialne za funkcjonowanie systemu.

10. Integratorzy płatności[3] oferujący usługi inicjowania płatności są uznawani bądź za agentów rozliczeniowych w zakresie usług płatności internetowych (a zatem za dostawców usług płatniczych), bądź za zewnętrznych dostawców usług technicznych obsługujących odpowiednie systemy lub dostawców usług płatniczych. W drugim przypadku integratorzy płatności powinni być umownie zobowiązani do przestrzegania niniejszych wytycznych.

11. Z zakresu stosowania wytycznych wyłączone są:

- inne usługi internetowe świadczone przez dostawców usług płatniczych poprzez ich strony internetowe przeznaczone do dokonywania płatności (np. elektroniczne usługi maklerskie, umowy online);

- płatności zlecane za pośrednictwem poczty tradycyjnej, polecenia telefonicznego, poczty głosowej lub przy użyciu technologii esemesowej;

- płatności mobilne inne niż realizowane przy użyciu przeglądarki internetowej;

- polecenia przelewu, w przypadku których dostęp do rachunku płatnika uzyskuje strona trzecia;

[3] Integratorzy płatności zapewniają odbiorcy płatności (tj. akceptantowi) standardowy interfejs umożliwiający dostęp do usług inicjowania płatności świadczonych przez dostawców usług płatniczych.

- transakcje płatnicze dokonywane przez przedsiębiorstwa poprzez dedykowane sieci;

- płatności kartą dokonywane przy użyciu anonimowych, jednorazowych fizycznych lub wirtualnych kart przedpłaconych, w przypadku gdy nie występuje trwała relacja pomiędzy wydawcą a posiadaczem karty;

- rozliczanie transakcji płatniczych.

Definicje

12. Do celów niniejszych wytycznych i w uzupełnieniu definicji zawartych w dyrektywie w sprawie usług płatniczych, użyte w niniejszych wytycznych terminy oznaczają:

- *Uwierzytelnienie* oznacza procedurę pozwalającą dostawcom usług płatniczych na potwierdzenie tożsamości klienta.

- *Silne uwierzytelnienie klienta* oznacza, do celów niniejszych wytycznych, procedurę obejmującą użycie dwóch lub więcej następujących elementów – klasyfikowanych jako wiedza, posiadanie i cecha klienta: i) coś, co jedynie użytkownik wie, np. hasło statyczne, kod, PESEL; ii) coś, co jedynie użytkownik posiada, np. token (generator kodów), karta inteligentna, telefon komórkowy; iii) coś, czym użytkownik jest, np. cecha biometryczna, taka jak odcisk palca. Ponadto wybrane elementy muszą być wzajemnie niezależne, tj. naruszenie bezpieczeństwa jednego nie naraża innego (innych). Co najmniej jeden z elementów powinien być niemożliwy do ponownego użycia i nieodtwarzalny (z wyjątkiem cech klienta), a także niemożliwy do niejawnego, nieautoryzowanego pozyskania przez internet. Procedura silnego uwierzytelnienia powinna być zaprojektowana w sposób chroniący poufność danych uwierzytelniających.

- *Autoryzacja* oznacza procedurę weryfikacji, czy klient lub dostawca usług płatniczych ma prawo do wykonywania określonej czynności, np. prawo do przelewu środków lub prawo dostępu do danych wrażliwych.

- *Dane uwierzytelniające* oznaczają informacje – co do zasady poufne – wprowadzane przez klienta lub dostawcę usług płatniczych na potrzeby uwierzytelniania. Dane uwierzytelniające mogą również oznaczać informacje zawarte w fizycznym narzędziu (np. generatorze haseł jednorazowych, karcie inteligentnej) czy też coś, co użytkownik pamięta lub czym jest (np. jego cechy biometryczne).

- *Poważny incydent bezpieczeństwa płatności* oznacza incydent, który ma lub może mieć istotny wpływ na bezpieczeństwo, integralność lub ciągłość działania systemów wykorzystywanych przez dostawcę usług płatniczych w zakresie płatności lub bezpieczeństwo wrażliwych danych płatniczych bądź środków. Oceniając istotność incydentu, należy uwzględnić liczbę klientów potencjalnie dotkniętych incydentem,

zagrożoną kwotę oraz wpływ na innych dostawców usług płatniczych lub inne infrastruktury płatnicze.

- *Analiza ryzyka transakcji* oznacza ocenę ryzyka związanego z daną transakcją, przeprowadzana z uwzględnieniem kryteriów takich jak np. wzorce płatności (zachowań płatniczych) klientów, wartość transakcji, rodzaj produktu i profil odbiorcy płatności.

- *Karty wirtualne* oznaczają kartowe rozwiązanie płatnicze, w ramach którego generowany jest alternatywny, tymczasowy numer karty o ograniczonym okresie ważności i predefiniowanym limicie wydatków, które może być wykorzystywane w celu dokonywania zakupów przez internet.

- *Rozwiązania portfelowe* to rozwiązania pozwalające klientom na zarejestrowanie danych związanych z jednym lub większą liczbą instrumentów płatniczych w celu dokonywania płatności u wielu akceptantów.

Tytuł II – Wytyczne dotyczące bezpieczeństwa płatności internetowych

Ogólne środowisko kontroli i bezpieczeństwa

Zarządzanie

1. Dostawcy usług płatniczych powinny wdrożyć i poddawać regularnemu przeglądowi formalną politykę bezpieczeństwa w zakresie usług płatności internetowych.

   1.1 Polityka bezpieczeństwa powinna być odpowiednio udokumentowana i poddawana regularnemu przeglądowi (zgodnie z wytyczną 2.4) oraz zatwierdzana przez kadrę kierowniczą wyższego szczebla. Polityka bezpieczeństwa powinna określać cele w zakresie bezpieczeństwa i apetyt na ryzyko.

   1.2 Polityka w zakresie bezpieczeństwa powinna określać role i obowiązki, w tym funkcję ds. zarządzania ryzykiem z bezpośrednim raportowaniem do szczebla zarządu, oraz porządek podległości służbowej w zakresie świadczonych usług płatności internetowych, w tym zarządzania szczególnie chronionymi danymi płatniczymi z uwzględnieniem oceny, kontroli i przeciwdziałania ryzyku.

Ocena ryzyka

2. Dostawcy usług płatniczych powinni przeprowadzać i dokumentować szczegółowe oceny ryzyka dotyczące bezpieczeństwa płatności internetowych i powiązanych usług, zarówno przed wprowadzeniem usługi (usług), jak i regularnie po jej (ich) wprowadzeniu.

   2.1 Dostawcy usług płatniczych – poprzez swoje funkcje ds. zarządzania ryzykiem – powinni przeprowadzać i dokumentować szczegółowe oceny ryzyka w zakresie płatności internetowych i usług w ich zakresie. Dostawcy usług płatniczych powinni uwzględniać rezultaty bieżącego monitorowania zagrożeń bezpieczeństwa w zakresie usług płatności internetowych, które oferują lub planują oferować, uwzględniając: i) stosowane przez siebie rozwiązania technologiczne, ii) usługi zlecane dostawcom zewnętrznym oraz iii) środowisko techniczne klientów. Dostawcy usług płatniczych powinni uwzględniać ryzyko związane z wybranymi platformami technologicznymi, architekturą aplikacji, technikami programistycznymi oraz procedurami, zarówno po swojej stronie[4], jak i po stronie klientów[5], a także wyniki procesu monitorowania incydentów bezpieczeństwa (zob. wytyczna 3).

[4] Takie jak podatność systemu na przechwycenie sesji płatniczej, „wstrzykiwanie SQL", „skrypty krzyżowe", przepełnienie bufora itp.

[5] Takie jak ryzyka związane z używaniem aplikacji multimedialnych, „wtyczek" do przeglądarek, ramek, linków zewnętrznych itp.

2.2 Na tej podstawie dostawcy usług płatniczych powinni ustalać, czy i w jakim zakresie niezbędne może być wprowadzenie zmian do istniejących środków bezpieczeństwa, wykorzystywanych technologii i oferowanych procedur i usług. Dostawcy usług płatniczych powinni brać pod uwagę czas niezbędny na wprowadzenie zmian (w tym również po stronie klientów) raz podjąć odpowiednie kroki w okresie przejściowym w celu zminimalizowania incydentów bezpieczeństwa i przypadków oszustwa, jak również potencjalnych zakłóceń działalności.

2.3 Ocena ryzyka powinna uwzględniać potrzebę ochrony i zabezpieczenia wrażliwych danych płatniczych.

2.4 Dostawcy usług płatniczych powinni przeprowadzać przegląd scenariuszy ryzyka i istniejących środków bezpieczeństwa po wystąpieniu poważnych incydentów mających wpływ na świadczone przez nich usługi, przed wprowadzeniem istotnych zmian infrastruktury lub procedur oraz w przypadku stwierdzenia nowych zagrożeń w ramach monitorowania ryzyka. Dodatkowo przynajmniej raz w roku należy przeprowadzać ogólny przegląd oceny ryzyka. Rezultaty oceny ryzyka i przeglądów powinny być zatwierdzane przez kadrę kierowniczą wyższego szczebla.

Monitorowanie i zgłaszanie incydentów

3. Dostawcy usług płatniczych powinni zapewnić spójne i zintegrowane podejście do monitorowania, postępowania w razie wystąpienia incydentów bezpieczeństwa i działań następczych, w tym skarg klientów związanych z bezpieczeństwem. Dostawcy usług płatniczych powinni wprowadzić procedurę zgłaszania takich incydentów kierownictwu, a w przypadku poważnych incydentów bezpieczeństwa płatności – właściwym organom.

3.1 Dostawcy usług płatniczych powinni stosować proces monitorowania, postępowania w razie wystąpienia incydentów bezpieczeństwa i działań następczych oraz skarg klientów związanych z bezpieczeństwem, i zgłaszać takie incydenty kierownictwu.

3.2 Dostawcy usług płatniczych powinni posiadać procedurę niezwłocznego informowania właściwych organów (tj. organów nadzoru oraz organów ds. ochrony danych), o ile takie organy istnieją, w przypadku wystąpienia poważnych incydentów bezpieczeństwa w zakresie świadczonych usług płatniczych.

3.3 Dostawcy usług płatniczych powinni posiadać procedurę współpracy z właściwymi organami ścigania w zakresie poważnych incydentów bezpieczeństwa, w tym naruszenia danych.

3.4 Dostawcy usług płatniczych będący centrami autoryzacji powinni umownie wymagać od akceptantów przechowujących, przetwarzających lub przesyłających wrażliwe dane płatnicze współpracy w zakresie poważnych incydentów bezpieczeństwa płatności, w tym naruszenia danych, zarówno z samymi dostawcami usług płatniczych, jak i właściwymi organami ścigania. Jeżeli dostawca usług płatniczych uzyska wiedzę o tym,

że akceptant płatności elektronicznych nie współpracuje zgodnie z wymaganiami umownymi, powinien podjąć kroki mające na celu wyegzekwowanie tego zobowiązania umownego lub rozwiązać umowę.

Kontrola i przeciwdziałanie ryzyku

4. W celu przeciwdziałania zidentyfikowanym ryzykom dostawcy usług płatniczych powinni wdrożyć środki bezpieczeństwa zgodne ze stosowanymi przez nich politykami bezpieczeństwa. Środki te powinny uwzględniać wiele linii obrony, tak by przełamanie jednej linii obrony było niwelowane przez kolejną linię obrony („obrona w głąb").

4.1 Projektując, rozwijając i utrzymując usługi płatności internetowych, dostawcy usług płatniczych powinni przykładać szczególną wagę do odpowiedniego podziału zadań w środowiskach informatycznych (np. środowiskach rozwojowych, testowych i produkcyjnych) oraz właściwego wdrożenia zasady minimalnych uprawnień jako podstawy należytego zarządzania tożsamością i dostępem.[6]

4.2 Dostawcy usług płatniczych powinni stosować odpowiednie rozwiązania w zakresie bezpieczeństwa w celu ochrony sieci, stron internetowych i łączy komunikacyjnych przed nadużyciami i atakami. Dostawcy usług płatniczych powinni wyłączać w serwerach wszelkie zbędne funkcje w celu ich ochrony („utwardzenia") i wyeliminowania lub ograniczenia podatności narażonych aplikacji. Dostęp poszczególnych aplikacji do danych i zasobów należy ograniczyć do bezwzględnego minimum zgodnie z zasadą minimalnych uprawnień. Aby ograniczyć wykorzystywanie „fałszywych" stron (imitujących rzeczywiste strony dostawców usług płatniczych), transakcyjne strony internetowe udostępniające usługi płatności internetowych powinny być identyfikowane za pomocą rozszerzonych certyfikatów walidacyjnych dostawcy usług płatniczych lub zbliżonych metod uwierzytelniania.

4.3 Dostawcy usług płatniczych powinni wdrożyć odpowiednie procesy monitorowania, śledzenia i ograniczania dostępu do: i) wrażliwych danych płatniczych oraz ii) krytycznych zasobów logicznych i fizycznych, takich jak sieci, systemy, bazy danych, moduły bezpieczeństwa itp. Dostawcy usług płatniczych powinni tworzyć, przechowywać i analizować odpowiednie dzienniki zdarzeń i ścieżki audytu.

4.4 Projektując[7], rozwijając i utrzymując usługi płatności internetowych, dostawcy usług płatniczych powinni dopilnować, by kluczowym elementem podstawowej funkcjonalności była minimalizacja danych[8]: gromadzenie, przesyłanie, przetwarzane,

[6] „Każdy program i każdy uprawniony użytkownik systemu powinien go obsługiwać, korzystając z jak najmniejszych uprawnień niezbędnych do wykonywania swojej pracy." Zobacz Saltzer, J.H. „Protection and the Control of Information Sharing in Multics", komunikaty ACM, tom 17, nr 7, str. 388.

[7] Uwzględnienie ochrony prywatności już w fazie projektowania.

[8] Minimalizacja danych oznacza politykę gromadzenia najmniejszych ilości danych osobowych niezbędnych do wykonywania danej funkcji.

przechowywanie lub archiwizowanie oraz wizualizację wrażliwych danych płatniczych należy ograniczyć do minimum.

4.5 Środki bezpieczeństwa stosowane w odniesieniu do usług płatności internetowych powinny być testowane pod nadzorem funkcji ds. zarządzania ryzykiem w celu zapewnienia ich solidności i skuteczności. Wszelkie zmiany powinny podlegać formalnemu procesowi zarządzania zmianą zapewniającemu odpowiednie planowanie, testowanie, dokumentowanie i zatwierdzanie zmian. W zależności od przeprowadzanych zmian oraz zaobserwowanych zagrożeń testy powinny być regularnie powtarzane i powinny obejmować scenariusze istotnych i znanych potencjalnych ataków.

4.6 Środki bezpieczeństwa stosowane przez dostawcę usług płatniczych w odniesieniu do usług płatności internetowych powinny być przedmiotem okresowych audytów w celu zapewnienia ich solidności i skuteczności. Wdrażanie i funkcjonowanie usług płatności internetowych również powinno być przedmiotem audytu. Częstotliwość i tematyka audytów powinny uwzględniać i być proporcjonalne do ryzyk w zakresie bezpieczeństwa. Audyty powinny być przeprowadzane przez zaufanych i niezależnych ekspertów (wewnętrznych lub zewnętrznych), którzy nie powinni być w żaden sposób zaangażowani w rozwój, wdrażanie lub operacyjne zarządzanie świadczonymi usługami płatności internetowych.

4.7 W przypadku gdy dostawcy usług płatniczych zlecają zadania w zakresie bezpieczeństwa usług płatności internetowych zewnętrznym podmiotom, treść umowy powinna określać wymogi dotyczące przestrzegania zasad i wytycznych określonych w niniejszym dokumencie.

4.8 Dostawcy usług płatniczych świadczący usługi agenta rozliczeniowego powinni wymagać w umowach zawieranych z akceptantami obsługującymi (tj. przechowującymi, przetwarzającymi lub przesyłającymi) wrażliwe dane płatnicze wdrożenia środków bezpieczeństwa w ramach ich infrastruktury IT, zgodnie z wytycznymi 4.1 do 4.7, w celu uniknięcia kradzieży tych wrażliwych danych płatniczych z wykorzystaniem ich systemów. W przypadku gdy dostawca usług płatniczych uzyska wiedzę o tym, że akceptant płatności elektronicznych nie stosuje wymaganych środków bezpieczeństwa, powinien podjąć kroki mające na celu wyegzekwowanie wspomnianego zobowiązania umownego lub rozwiązać umowę.

Śledzenie

5. Dostawcy usług płatniczych powinni stosować procesy zapewniające, aby wszystkie transakcje, jak również przebieg procesu polecenia zapłaty, były odpowiednio śledzone.

5.1 Dostawcy usług płatniczych powinni dopilnować, aby świadczone przez nich usługi uwzględniały mechanizmy bezpieczeństwa umożliwiające szczegółowe rejestrowanie transakcji i danych dotyczących poleceń zapłaty, w tym numerów porządkowych

transakcji, znaczników czasowych danych transakcyjnych, zmian parametryzacji, a także danych dotyczących dostępu do transakcji i poleceń zapłaty.

5.2 Dostawcy usług płatniczych powinni stosować dzienniki zdarzeń umożliwiające śledzenie wprowadzania nowych oraz modyfikowania i usuwania istniejących danych transakcyjnych i poleceń zapłaty.

5.3 Dostawcy usług płatniczych powinni kwerendować i analizować dane dotyczące transakcji oraz poleceń zapłaty i posiadać narzędzia do oceny dzienników zdarzeń. Poszczególne aplikacje powinny być wyłącznie dostępne upoważnionym pracownikom.

Szczególne środki kontroli i bezpieczeństwa w zakresie płatności internetowych

Wstępna identyfikacja klienta, informacje o kliencie

6. Klienci powinni być odpowiednio identyfikowani – zgodnie z europejskim prawodawstwem dotyczącym przeciwdziałania praniu pieniędzy[9] – i potwierdzać swoją wolę dokonania płatności internetowej z wykorzystaniem danej usługi przed uzyskaniem dostępu do niej. Dostawcy usług płatniczych powinni zapewniać klientom odpowiednie informacje, przed skorzystaniem przez nich z danej usługi, regularnie, lub – o ile ma to zastosowanie – doraźnie, dotyczące wymagań (np. sprzętu, procedur) w zakresie bezpiecznego przeprowadzania transakcji płatności internetowych i powiązanych ryzyk.

6.1 Dostawcy usług płatniczych powinni dopilnować, aby klienci byli poddawani procedurom należytej staranności oraz dostarczali odpowiednie dokumenty tożsamości[10] oraz powiązane informacje przed uzyskaniem dostępu do usług płatności internetowych.[11]

6.2 Dostawcy usług płatniczych powinni dopilnować, by informacje dostarczane klientom przed skorzystaniem przez nich z danej usługi[12] szczegółowo określały kwestie związane z usługami płatności internetowych. Powinny one, w stosownych przypadkach, uwzględniać:

[9] Na przykład dyrektywa 2005/60/WE Parlamentu Europejskiego i Rady z dnia 26 października 2005 r. w sprawie przeciwdziałania korzystaniu z systemu finansowego w celu prania pieniędzy oraz finansowania terroryzmu. Dz.U. L 309 z 25.11.2005, s. 15-36. Zobacz również dyrektywę Komisji 2006/70/WE z dnia 1 sierpnia 2006 r. ustanawiającą środki wykonawcze do dyrektywy 2005/60/WE Parlamentu Europejskiego i Rady w odniesieniu do definicji „osoby zajmującej eksponowane stanowisko polityczne", jak również w odniesieniu do technicznych kryteriów stosowania uproszczonych zasad należytej staranności wobec klienta oraz wyłączenia z uwagi na działalność finansową prowadzoną w sposób sporadyczny lub w bardzo ograniczonym zakresie, Dz.U. L 214 z 4.8.2006, s. 29-34.

[10] Na przykład paszport, krajowy dokument tożsamości lub zaawansowany podpis elektroniczny.

[11] Proces identyfikacji klienta podlega odstępstwom przewidzianym w krajowych przepisach dotyczących prania pieniędzy. Dostawcy usług płatniczych nie muszą przeprowadzać osobnego procesu identyfikacji klienta na potrzeby usług płatności internetowych, o ile taka identyfikacja została już przeprowadzona, np. w związku z innymi istniejącymi usługami płatniczymi lub przy otwieraniu rachunku.

[12] Ta informacja stanowi uzupełnienie art. 42 dyrektywy ws. usług płatniczych, który określa zakres informacji, jakie dostawcy usług płatniczych są zobowiązani dostarczyć użytkownikom usług płatniczych przed zawarciem umowy o świadczenie usług płatniczych.

- jasne informacje dotyczące wymogów w zakresie sprzętu klienta, jego oprogramowania lub innych niezbędnych narzędzi (np. oprogramowania antywirusowego, zapór sieciowych);

- wytyczne dotyczące właściwego i bezpiecznego używania spersonalizowanych danych uwierzytelniających służących zapewnieniu bezpieczeństwa;

- opis, krok po kroku, procedury przesyłania i autoryzowania przez klienta transakcji płatniczej lub uzyskiwania informacji, w tym dotyczących skutków poszczególnych czynności;

- wytyczne dotyczące właściwego i bezpiecznego używania sprzętu i oprogramowania dostarczanego klientowi;

- sposób postępowania na wypadek utraty lub kradzieży spersonalizowanych danych uwierzytelniających lub sprzętu bądź oprogramowania klienta wykorzystywanych do logowania lub przeprowadzania transakcji;

- procedury postępowania w przypadku wykrycia lub podejrzenia nadużycia;

- opis obowiązków i zakresu odpowiedzialności odpowiednio dostawcy usług płatniczych i klienta w zakresie korzystania z usług płatności internetowych.

6.3 Dostawcy usług płatniczych powinni dopilnować, aby umowa ramowa z klientem przewidywała możliwość zablokowania przez dostawcę usług płatniczych określonej transakcji lub instrumentu płatniczego[13] ze względów bezpieczeństwa. Umowa powinna określać metodę i terminy powiadamiania klienta oraz sposób, w jaki klient może się skontaktować z dostawcą usług płatniczych w celu odblokowania transakcji lub usług płatności internetowych, zgodnie z dyrektywą w sprawie usług płatniczych.

Silne uwierzytelnianie klienta

7. Inicjowanie płatności internetowej, a także dostęp do wrażliwych danych płatniczych, powinny być chronione silnym uwierzytelnianiem klienta. Dostawcy usług płatniczych powinni stosować procedurę silnego uwierzytelnienia klienta zgodnie z definicją określoną w niniejszych wytycznych.

7.1 [polecenia przelewu/polecenia zapłaty/pieniądz elektroniczny] Dostawcy usług płatniczych powinni stosować silne uwierzytelnianie klienta na potrzeby autoryzacji przez klienta transakcji płatności internetowych (w tym również pakietów poleceń przelewu) oraz wydawania lub modyfikacji elektronicznych poleceń zapłaty. Dostawcy usług płatniczych mogą jednak rozważyć przyjęcie alternatywnych środków uwierzytelniania klienta na potrzeby:

[13] Zobacz art. 55 dotyczący ograniczeń stosowania instrumentów płatniczych.

- płatności wychodzących na rzecz zaufanych odbiorców wymienionych na uprzednio sporządzonej białej liście klienta;

- transakcji pomiędzy dwoma rachunkami płatniczymi tego samego klienta prowadzonymi przez tego samego dostawcę usług płatniczych;

- przelewów dokonywanych w ramach tego samego dostawcy usług płatniczych uzasadnionych analizą ryzyka transakcji;

- płatności o niskiej wartości, zgodnie z dyrektywą w sprawie usług płatniczych.[14]

7.2 Uzyskanie dostępu do wrażliwych danych płatniczych lub modyfikacja tych danych (w tym tworzenie i modyfikowanie białych list) wymaga silnego uwierzytelnienia klienta. W przypadku gdy dostawca usług płatniczych świadczy wyłącznie usługi doradcze, nie wyświetlając żadnych wrażliwych informacji o kliencie lub płatności, które mogłyby został łatwo wykorzystane do popełnienia oszustwa (takich jak dane kart płatniczych), dostawca usług internetowych może dostosować swoje wymagania w zakresie uwierzytelniania na podstawie oceny ryzyka.

7.3 [karty] W zakresie transakcji kartą wszyscy dostawcy usług płatniczych będący wydawcami kart powinni zapewniać silne uwierzytelnianie posiadacza karty. Wszystkie wydawane karty muszą być przystosowane technicznie (zarejestrowane) do wykorzystywania wraz z silnym uwierzytelnianiem.

7.4 [karty] Dostawcy usług płatniczych świadczący usługi agenta rozliczeniowego powinni posiadać technologie umożliwiające wydawcy karty przeprowadzanie silnego uwierzytelniania posiadacza karty w zakresie systemów płatności kartą, w których uczestniczy agent rozliczeniowy.

7.5 [karty] Dostawcy usług płatniczych świadczący usługi agenta rozliczeniowego powinni wymagać od akceptantów obsługi rozwiązań umożliwiających wydawcy karty przeprowadzanie silnego uwierzytelniania posiadacza karty w zakresie transakcji kartą realizowanych przez internet. Można rozważyć stosowanie alternatywnych metod uwierzytelniania w zakresie uprzednio określonych kategorii transakcji niskiego ryzyka, np. na podstawie analizy ryzyka transakcji, lub płatności o niskiej wartości, zgodnie z dyrektywą w sprawie usług płatniczych.

7.6 [karty] W zakresie systemów płatności kartą akceptowanych w ramach danej usługi, dostawcy „rozwiązań portfelowych” powinni wymagać silnego uwierzytelniania przez wydawcę karty w przypadku, gdy uprawniony posiadacz po raz pierwszy rejestruje dane karty.

[14] Zobacz definicja instrumentów płatniczych obejmujących płatności w art. 34 ust. 1 i 53 ust. 1 dyrektywy w sprawie usług płatniczych.

7.7 Dostawcy „rozwiązań portfelowych" powinni wspierać silne uwierzytelnianie klienta w przypadkach, w których klienci logują się do usług płatności portfelowych lub dokonują transakcji kartą przez internet. Można rozważyć stosowanie alternatywnych metod uwierzytelniania w zakresie uprzednio określonych kategorii transakcji niskiego ryzyka, np. na podstawie analizy ryzyka transakcji, lub płatności o niskiej wartości, zgodnie z dyrektywą w sprawie usług płatniczych.

7.8 [karty] W zakresie kart wirtualnych początkowa rejestracja powinna odbywać się w bezpiecznym i zaufanym środowisku.[15] Silne uwierzytelnianie klienta powinno być wymagane w procesie generowania danych kart wirtualnych w przypadku, gdy karta wydawana jest w środowisku internetowym.

7.9 Dostawcy usług płatniczych powinni zapewnić właściwe dwustronne uwierzytelniane w przypadkach łączenia się z akceptantami w celu zainicjowania płatności internetowych oraz dostępu do wrażliwych danych płatniczych.

Wnioskowanie o narzędzia uwierzytelniające lub oprogramowanie przez klientów oraz ich dostarczanie klientom

8. Dostawcy usług płatniczych powinni dopilnować, by wnioskowanie przez klientów o narzędzia uwierzytelniające wymagane do korzystania z usług płatności internetowych lub oprogramowanie w tym zakresie, jak również ich dostarczanie klientom, odbywało się w bezpieczny sposób.

8.1 Wnioskowanie przez klientów o narzędzia uwierzytelniające lub oprogramowanie związane z płatnościami oraz ich dostarczanie klientom powinno spełniać następujące wymagania:

- Procedury w tym zakresie powinny być przeprowadzane w bezpiecznym i zaufanym środowisku, z uwzględnieniem potencjalnych ryzyk związanych z użytkowaniem urządzeń znajdujących się poza kontrolą dostawcy usług płatniczych.

- Powinny obowiązywać skuteczne i bezpieczne procedury w zakresie dostarczania spersonalizowanych danych uwierzytelniających, oprogramowania wymaganego do płatności oraz wszelkich spersonalizowanych urządzeń używanych do płatności internetowych. Ponadto oprogramowanie dostarczane przez internet powinno być podpisane cyfrowo przez dostawcę usług płatniczych, tak by umożliwić

[15] Środowiska pozostające w zakresie odpowiedzialności dostawcy usług płatniczych, w których zapewnione jest odpowiednie uwierzytelnienie klienta i dostawcy usług płatniczych świadczącego usługę, jak również ochronę poufnych/wrażliwych informacji, obejmują: i) placówki dostawcy usług płatniczych, ii) bankowość internetową lub inne bezpieczne strony internetowe, np. w przypadku których podmioty zarządzające systemami płatności zapewniają porównywalny poziom bezpieczeństwa, m.in. określony w wytycznej 4; lub iii) usługi bankomatowe. (w przypadku bankomatów wymagane jest silne uwierzytelnianie klienta; takie uwierzytelnianie zwykle zapewniane jest przez chip i kod PIN lub chip i weryfikację biometryczną).

klientowi weryfikację jego autentyczności oraz sprawdzenie, czy nie było ono przedmiotem manipulacji.

- [karty] W przypadku transakcji kartą klient powinien mieć możliwość wyboru silnego uwierzytelniania niezależnie dla poszczególnych zakupów internetowych. Jeżeli oferowana jest możliwość aktywacji podczas zakupów online, aktywacja powinna się odbywać poprzez przekierowanie klienta do bezpiecznego i zaufanego środowiska.

8.2 [karty] Wydawcy karty powinni aktywnie zachęcać posiadaczy kart do wybierania silnego uwierzytelniania oraz pozwalać im na obejście silnego uwierzytelniania jedynie w ograniczonej liczbie wyjątkowych przypadków, gdy jest to uzasadnione ryzykiem związanym z konkretną transakcją kartą.

Próby logowania, wygasanie sesji, ważność uwierzytelniania

9. Dostawcy usług płatniczych powinni ograniczyć liczbę prób logowania lub uwierzytelnienia, określić zasady wygasania sesji usług płatności internetowych oraz ustalić ograniczenia czasowe ważności uwierzytelniania.

9.1 Stosując na potrzeby uwierzytelniania hasła jednorazowe, dostawcy usług płatniczych powinni dopilnować, aby okres ważności haseł był ograniczony do niezbędnego minimum.

9.2 Dostawcy usług płatniczych powinni określić maksymalną liczbę nieudanych prób logowania lub uwierzytelnienia, po których dostęp do usługi płatności internetowej jest blokowany (tymczasowo lub na stałe). Dostawcy usług płatniczych powinni stosować bezpieczną procedurę ponownej aktywacji zablokowanych usług płatności internetowych.

9.3 Dostawcy usług płatniczych powinni określić maksymalny okres, po którym nieaktywne sesje usług płatności internetowych są automatycznie zamykane.

Monitorowanie transakcji

10. Należy stosować mechanizmy monitorowania transakcji mające na celu zapobieganie, wykrywanie i blokowanie oszukańczych transakcji płatniczych przed dokonaniem ostatecznej autoryzacji transakcji przez dostawcę usług płatniczych; transakcje podejrzane lub wysokiego ryzyka powinny podlegać szczególnej procedurze kontroli i oceny. Analogiczne mechanizmy monitorowania bezpieczeństwa i autoryzacji powinny funkcjonować również w zakresie wystawiania poleceń zapłaty.

10.1 Dostawcy usług płatniczych powinni stosować systemy wykrywania i zapobiegania oszustwom w celu identyfikacji podejrzanych transakcji przed ostateczną autoryzacją transakcji lub polecenia zapłaty przez dostawcę usług płatniczych. Systemy te powinny

przykładowo funkcjonować w oparciu o sparametryzowane reguły (takie jak czarne listy naruszonych lub skradzionych danych kart) oraz monitorować nietypowe wzorce zachowań klientów lub ich urządzeń dostępowych (takie jak zmiana adresu lub zakresu adresów IP)[16] podczas sesji usług płatności internetowych, czasem identyfikowane przez sprawdzenie geolokalizacji adresu IP,[17] nietypowe kategorie akceptantów dla danego klienta czy nietypowe dane transakcji itp.). Systemy te powinny również być zdolne do wykrywania oznak infekcji sesji przez złośliwe oprogramowanie (np. poprzez sprawdzenie, czy dana czynność realizowana jest przez skrypt, czy przez człowieka) i znanych scenariuszy oszustw. Zakres, stopień złożoności i zdolności adaptacyjne rozwiązań w zakresie monitorowania powinny być – z zastrzeżeniem zgodności z właściwymi przepisami dotyczącymi ochrony danych – współmierne do rezultatów oceny ryzyka.

10.2 Dostawcy usług płatniczych będący agentami rozliczeniowymi powinni posiadać systemy wykrywania i zapobiegania nadużyciom monitorujące działania akceptantów.

10.3 Dostawcy usług płatniczych powinni realizować procedury sprawdzania i oceny przez odpowiedni czas, tak aby nadmiernie nie opóźniać inicjowania lub realizacji danej usługi płatniczej.

10.4 W przypadku, gdy dostawca usług płatniczych w oparciu o politykę ryzyka decyduje o zablokowaniu transakcji płatniczej zidentyfikowanej jako potencjalnie oszukańcza, powinien on utrzymywać blokadę przez możliwie krótki czas do momentu rozwiązania problemów z bezpieczeństwem.

Ochrona wrażliwych danych płatniczych

11. Wrażliwe dane płatnicze powinny podlegać ochronie podczas przechowywania, przetwarzania lub przesyłania.

11.1 Wszelkie dane wykorzystywane do identyfikacji i uwierzytelnienia klientów (np. podczas logowania, w trakcie inicjowania płatności internetowych oraz w trakcie wystawiania, modyfikowania lub anulowania poleceń zapłaty), a także interfejs klienta (strona internetowa dostawcy usług płatniczych lub akceptanta), powinny być odpowiednio zabezpieczone przed kradzieżą i nieautoryzowanym dostępem lub modyfikacją.

11.2 Dostawcy usług płatniczych powinni zapewnić, aby w celu ochrony poufności i integralności danych w trakcie wymiany wrażliwych danych płatniczych przez internet podczas całej sesji komunikacyjnej pomiędzy stronami uczestniczącymi w komunikacji

[16] Adres IP jest unikalnym kodem numerycznym identyfikującym każdy komputer podłączony do internetu.

[17] Geolokalizacja adresu IP ma na celu określenie miejsca, z którego inicjowana jest transakcja, na podstawie adresu IP.

stosowane było bezpieczne szyfrowanie typu „end-to-end”[18], przy użyciu silnych i powszechnie stosowanych technik szyfrowania.

11.3 Dostawcy usług płatniczych świadczący usługi agenta rozliczeniowego powinni zachęcać akceptantów do nieprzechowywania jakichkolwiek wrażliwych danych płatniczych. W przypadku gdy akceptanci obsługują (tj. przechowują, przetwarzają lub przesyłają) wrażliwe dane płatnicze, dostawcy usług płatniczych powinni wprowadzić w umowach z takimi akceptantami wymóg posiadania niezbędnych środków mających na celu ochronę tych danych. Dostawcy usług płatniczych powinni dokonywać regularnych weryfikacji w tym zakresie, zaś w przypadku stwierdzenia, że akceptant obsługujący wrażliwe dane płatnicze nie posiada wymaganych środków bezpieczeństwa – powinni podjąć kroki mające na celu doprowadzenie do wywiązywania się akceptanta ze zobowiązań umownych lub rozwiązać umowę.

[18] Szyfrowanie typu „end-to-end” występuje wówczas, gdy szyfrowanie danych odbywa się w systemie źródłowym, zaś ich deszyfrowanie odbywa się wyłącznie w systemie docelowym. ETSI EN 302 109 V1.1.1. (2003-06).

Świadomość i edukowanie klientów oraz komunikacja z nimi

Edukowanie klientów i komunikacja z nimi

12. Dostawcy usług płatniczych powinni zapewniać klientom niezbędną pomoc i wsparcie w zakresie bezpiecznego korzystania z usług płatności internetowych. Dostawcy usług płatniczych powinni komunikować się z klientami w sposób umożliwiający im stwierdzenie autentyczności otrzymanych wiadomości.

12.1 Dostawcy usług płatniczych powinni zapewniać funkcjonowanie co najmniej jednego bezpiecznego kanału[19] na potrzeby bieżącej komunikacji z klientami w zakresie poprawnego i bezpiecznego korzystania z usług płatności internetowych. Dostawcy usług płatniczych powinni informować klientów o tym kanale oraz wyjaśniać, że wiadomości dotyczące poprawnego i bezpiecznego korzystania z usług płatności internetowych przesyłane w ich imieniu innym kanałem, np. pocztą elektroniczną, nie są wiarygodne. Dostawcy usług płatniczych powinni wyjaśnić klientom:

- procedury zgłaszania dostawcom usług płatniczych (potencjalnych) transakcji oszukańczych, podejrzanych zdarzeń i nietypowych sytuacji w trakcie sesji usług płatności internetowych lub potencjalnych prób ataków socjotechnicznych[20];
- kolejne kroki, tj. w jaki sposób dostawca usług płatniczych odpowie klientowi;
- w jaki sposób dostawca usług płatniczych będzie powiadamiał klienta o (potencjalnych) transakcjach oszukańczych lub ich niezainicjowaniu, lub ostrzegał klienta o wystąpieniu ataków (np. e-maili phishingowych).

12.2 Dostawcy usług płatniczych powinni informować klientów poprzez bezpieczny kanał o aktualizacjach procedur bezpieczeństwa dotyczących usług płatności internetowych. Bezpiecznym kanałem powinny być również przekazywane wszelkie powiadomienia o pojawiających się poważnych ryzykach (np. ostrzeżenia przed atakami socjotechnicznymi).

12.3 Dostawcy usług płatniczych powinni zapewniać klientom wsparcie w zakresie wszelkich zapytań, skarg, wniosków o wsparcie oraz powiadomień o nietypowych sytuacjach i incydentach w zakresie płatności internetowych i związanych z nimi usług, natomiast klienci powinni być odpowiednio informowani o sposobach uzyskiwania takiego wsparcia.

[19] Takie jak dedykowana skrzynka pocztowa na stronie internetowej dostawcy usług płatniczych lub bezpieczna strona internetowa.

[20] Ataki socjotechniczne w tym kontekście oznaczają techniki manipulacji ludźmi mające na celu pozyskanie informacji (np. poprzez e-mail lub telefon) lub ich wyszukanie w sieciach społecznościowych w celu dokonania oszustwa lub uzyskania nieautoryzowanego dostępu do komputera lub sieci.

12.4 Dostawcy usług płatniczych powinni prowadzić programy edukowania i uświadamiania klientów mające na celu zapewnienie, aby klienci rozumieli co najmniej potrzebę:

- ochrony haseł, tokenów, danych osobowych i innych poufnych danych;
- właściwego zarządzania bezpieczeństwem urządzeń osobistych (np. komputerów) poprzez instalowanie i aktualizowanie komponentów bezpieczeństwa (programów antywirusowych, zapór sieciowych, poprawek bezpieczeństwa);
- analizowania poważnych zagrożeń i ryzyk związanych z pobieraniem oprogramowania z internetu w przypadku, gdy klienci nie mogą być pewni, że oprogramowanie to jest autentyczne i nie było przedmiotem manipulacji;
- korzystania z autentycznych stron internetowych dostawcy usług płatniczych.

12.5 Dostawcy usług płatniczych będący agentami rozliczeniowymi powinni wymagać od akceptantów jasnego oddzielenia procesów dokonywania płatności od dokonywania zakupów online w celu ułatwienia klientom identyfikowania sytuacji, w których komunikują się oni z dostawcą usług płatniczych, a nie z odbiorcami płatności (np. poprzez przekierowywanie klientów i otwieranie osobnego okna, przez co proces płatności nie będzie widoczny w ramce akceptanta).

Powiadomienia, ustalanie limitów

13. Dostawcy usług płatniczych powinni ustalić limity dla usług płatności internetowych oraz mogą udostępniać klientom możliwość dalszego ograniczania ryzyka w ramach tych limitów. Mogą również świadczyć usługi ostrzegania i zarządzania profilem klienta.

13.1 Przed rozpoczęciem świadczenia klientom usług płatności internetowej dostawcy usług płatniczych powinni ustalić limity[21] mające zastosowanie do tych usług (np. maksymalną wartość indywidualnych transakcji lub łączną wartość transakcji w określonym okresie) i poinformować o tym klientów. Dostawcy usług płatniczych powinni umożliwiać klientom rezygnację z funkcjonalności płatności internetowych.

Dostęp klientów do informacji o statusie inicjacji i realizacji płatności

14. Dostawcy usług płatniczych powinni potwierdzać klientom zainicjowanie płatności oraz dostarczać im we właściwym czasie informacje niezbędne do weryfikacji, czy transakcja płatnicza została poprawnie zainicjowana lub wykonana.

14.1 [polecenia przelewu/polecenia zapłaty] Dostawcy usług płatniczych powinni umożliwiać klientom w niemal rzeczywistym czasie weryfikację statusu wykonania

[21] Takie limity mogą mieć zastosowanie globalne (tj. do wszystkich instrumentów płatniczych umożliwiających dokonywanie płatności internetowych) lub indywidualne.

transakcji oraz salda rachunku w dowolnym momencie[22] w bezpiecznym i zaufanym środowisku.

14.2 Wszelkie szczegółowe wyciągi elektroniczne powinny być udostępniane w bezpiecznym i zaufanym środowisku. W przypadku gdy dostawcy usług płatniczych informują klientów o dostępności wyciągów elektronicznych (np. regularnie w momencie wystawienia okresowego wyciągu elektronicznego lub ad hoc po realizacji transakcji) poprzez alternatywny kanał, taki jak SMS, e-mail lub listownie, wrażliwe dane płatnicze nie powinny być umieszczane w takich wiadomościach lub – jeżeli są umieszczane – powinny być maskowane.

Tytuł III – Przepisy końcowe i wdrożenie

15.Niniejsze wytyczne stosuje się od dnia 01.08.2015.

[22] Z wyłączeniem wyjątkowych przypadków niedostępności takiej funkcjonalności w związku z pracami technicznymi lub poważnymi incydentami.

Załącznik 1: Przykłady najlepszych praktyk

W wytycznych opisano – oprócz powyższych wymogów – przykłady najlepszych praktyk, do których wdrożenia zachęca się dostawców usług płatniczych, lecz których stosowanie nie jest obowiązkowe. Dla ułatwienia orientacji, przykłady najlepszych praktyk przedstawiono według tytułów poszczególnych rozdziałów wytycznych.

Ogólne środowisko kontroli i bezpieczeństwa

Zarządzanie

NP1: Polityka bezpieczeństwa może być określona w osobnym dokumencie.

Kontrola i przeciwdziałanie ryzyku

NP2: Dostawcy usług płatniczych mogą zapewnić narzędzia bezpieczeństwa (np. odpowiednio zabezpieczone urządzenia lub specjalnie zaprojektowane przeglądarki internetowe) w celu ochrony interfejsu klienta przed bezprawnym wykorzystaniem lub atakami [np. atakami typu „man-in-the-browser" (człowiek w przeglądarce)].

Śledzenie

NP3: Dostawcy usług płatniczych świadczący usługi agenta rozliczeniowego mogą zawrzeć w umowach z akceptantami przechowującymi informacje dotyczące płatności wymóg stosowania odpowiednich procesów umożliwiających śledzenie transakcji.

Szczególne środki kontroli i bezpieczeństwa w zakresie płatności internetowych

Wstępna identyfikacja klienta, informacje o kliencie

NP4: Można wymagać od klienta podpisania osobnej umowy o świadczenie usług w zakresie transakcji płatności internetowych zamiast określania warunków transakcji płatności internetowych w ogólnej umowie o świadczenie usług z dostawcą usług płatniczych.

NP5: Dostawcy usług płatniczych mogą również zapewnić przekazywanie klientom na bieżąco, a w miarę potrzeby – doraźnie, i za pomocą odpowiednich środków (np. ulotek, stron internetowych), jasne i zrozumiałe instrukcje wyjaśniające obowiązki klientów w zakresie bezpiecznego korzystania z usługi.

Silne uwierzytelnianie klienta

NP6: [karty] Akceptanci mogą stosować środki umożliwiające silną autoryzację posiadacza karty przez wydawcę karty podczas dokonywania transakcji kartą przez internet.

NP7: Aby ułatwić klientom korzystanie z usług, dostawcy usług płatniczych mogą rozważyć stosowanie jednego narzędzia silnej autoryzacji w odniesieniu do wszystkich usług płatności internetowych. Może to zwiększyć poziom akceptacji rozwiązania wśród klientów i ułatwić jego właściwe stosowanie.

NP8: Silna autoryzacja klienta może obejmować rozwiązania obejmujące powiązanie autoryzacji z określoną kwotą lub odbiorcą płatności, co może zapewnić klientom większą pewność przy autoryzowaniu płatności. Rozwiązanie techniczne umożliwiające powiązanie silnych danych autoryzacyjnych z danymi transakcyjnymi powinno być odporne na manipulację.

Ochrona wrażliwych danych płatniczych

NP9: Akceptanci obsługujący wrażliwe dane płatnicze powinni odpowiednio przeszkolić swoich pracowników odpowiedzialnych za przeciwdziałanie oszustwom i regularnie aktualizować szkolenia, tak by ich tematyka odpowiadała dynamice zmian warunków bezpieczeństwa.

Edukacja i komunikacja z klientami

NP10: Dostawcy usług płatniczych świadczący usługi agenta rozliczeniowego powinni wprowadzać programy edukowania akceptantów w zakresie zapobiegania oszustwom.

Powiadomienia, określanie limitów

NP11: Z zastrzeżeniem określonych limitów, dostawcy usług płatniczych mogą zapewnić klientom możliwość zarządzania, w bezpiecznym i zaufanym środowisku, limitami odnoszącymi się do usług płatności internetowych.

NP12: Kierując się swoją polityką zarządzania ryzykiem, dostawcy usług płatniczych mogą stosować ostrzeganie klientów, na przykład telefonicznie lub esemesem, w przypadku wystąpienia transakcji podejrzanych lub wysokiego ryzyka.

NP13: Dostawcy usług płatniczych mogą umożliwić klientom określanie ogólnych, spersonalizowanych reguł jako parametrów ich zachowań w zakresie płatności internetowych i powiązanych usług. Reguły mogą przykładowo przewidywać, że klienci będą inicjowali transakcje wyłącznie z określonych krajów i że płatności inicjowane z innych krajów należy blokować, lub możliwość umieszczania określonych odbiorców płatności na białych lub czarnych listach.