Rekomendacje dotyczące bezpieczeństwa płatności internetowych

Wersja ostateczna po konsultacjach publicznych

Polska wersja językowa

1 Część ogólna

Niniejszy raport przedstawia zbiór rekomendacji mających na celu podniesienie poziomu bezpieczeństwa płatności internetowych. Rekomendacje te zostały opracowane przez Europejskie Forum ds. Bezpieczeństwa Płatności Detalicznych (SecuRe Pay – European Forum on the Security of Retail Payments; dalej Forum). Forum zostało utworzone w 2011 r. jako inicjatywa dobrowolnej współpracy pomiędzy władzami nadzorczymi. Jego celem jest szerzenie wiedzy i jednolitego rozumienia – w szczególności pomiędzy nadzorami dostawców usług płatniczych – w zakresie kwestii związanych z bezpieczeństwem elektronicznych usług i instrumentów płatności detalicznych dostarczanych w państwach członkowskich Unii Europejskiej (UE) / Europejskiego Obszaru Gospodarczego (EOG). Prace Forum skupiają się na całościowym łańcuchu przetwarzania usług elektronicznych płatności detalicznych (z wyłączeniem czeków i gotówki), niezależnie od rodzaju kanału elektronicznego. Celem Forum jest odnoszenie się do obszarów, w których stwierdzane są istotne słabości i podatności, oraz – w stosownych przypadkach – wydawanie rekomendacji. Ostatecznym celem jest wspieranie wytworzenia zharmonizowanego minimalnego poziomu bezpieczeństwa w UE / EOG. Organy nadzorcze uczestniczące w pracach Forum wymienione zostały w załączniku.

Biorąc pod uwagę, że płatności dokonywane przez internet są obecnie postrzegane przez regulatorów, ustawodawców, dostawców usług płatniczych oraz przez opinię publiczną jako wiążące się z wyższym udziałem nadużyć w stosunku do tradycyjnych metod płatności[1], Forum zadecydowało o opracowaniu rekomendacji dotyczących bezpieczeństwa płatności internetowych. Stanowią one odzwierciedlenie doświadczenia organów nadzorczych w ich krajach macierzystych, oraz uwzględniają rezultaty konsultacji publicznych.[2]

[1] Obecnie dostępne dane unijne dane dotyczące nadużyć w zakresie płatności są ograniczone. Jednak według brytyjskiej organizacji branżowej, Financial Fraud Action UK oraz francuskiej organizacji Observatoire de la sécurité des cartes de paiement, oszustwa w płatnościach kartowych dokonanych bez fizycznej obecności karty stały się przeważającą grupą nadużyć płatniczych. Patrz też: „Report on card fraud", Europejski Bank Centralny (lipiec 2012 r.).

[2] Konsultacje publiczne rekomendacji przeprowadzone zostały w okresie od połowy kwietnia do czerwca 2012 r.

Oczekuje się, że wypracowanie europejskich zharmonizowanych rekomendacji dotyczących bezpieczeństwa płatności internetowych będzie sprzyjać zwalczaniu nadużyć płatniczych i zwiększeniu zaufania konsumentów do płatności internetowych. Niniejszy raport określa również dobre praktyki, do których wdrożenia zachęcani są dostawcy usług płatniczych, podmioty zarządzające systemami płatności oraz inni uczestnicy rynku (np. akceptanci funkcjonujący w internecie). Powyższe dobre praktyki są istotne, ponieważ bezpieczeństwo płatności internetowych zależy od odpowiedzialnego zachowania wszystkich uczestników rynku.

Zakres i adresaci

O ile nie wskazano inaczej, rekomendacje oraz opisy kluczowych kwestii i dobrych praktyk zawarte w niniejszym raporcie mają zastosowanie do wszystkich dostawców usług płatniczych – zgodnie z definicją zawartą w dyrektywie ws. usług płatniczych[3] – świadczących usługi płatności internetowych, jak również do podmiotów zarządzających systemami płatności[4] (w tym systemów płatności kartowych, systemów przelewów, systemów poleceń zapłaty itp.). Celem niniejszego raportu jest określenie wspólnych, minimalnych wymagań dla usług płatności internetowych wymienionych poniżej, niezależnie od wykorzystywanego urządzenia dostępowego:

- [karty] realizacja płatności kartowych przez internet, w tym z użyciem kart wirtualnych, jak również rejestrowanie danych kart płatniczych w celu ich użycia w „wirtualnych portfelach";
- [polecenia przelewu] realizacja poleceń przelewu przez internet;
- [polecenia zapłaty] wydawanie i modyfikacje elektronicznych poleceń zapłaty;
- [pieniądz elektroniczny] przelewy pieniądza elektronicznego pomiędzy dwoma rachunkami poprzez internet.

Integratorzy płatności[5] oferujący usługi inicjowania płatności są uznawani za agentów rozliczeniowych w zakresie usług płatności internetowych (a zatem za dostawców usług płatniczych), lub za zewnętrznych technicznych dostawców usług odpowiednich systemów płatności. W drugim przypadku, integratorzy płatności powinni być umownie zobowiązani do zachowania zgodności z rekomendacjami.

Z zakresu stosowania rekomendacji, kluczowych kwestii i dobrych praktyk wyłączone są:

- inne usługi internetowe świadczone przez dostawców usług płatniczych przez ich strony internetowe (np. elektroniczne usługi maklerskie i inwestycyjne, kontrakty on-line);
- płatności zlecane za pośrednictwem poczty tradycyjnej, polecenia telefonicznego, poczty głosowej lub przy użyciu technologii opartej o SMS;

[3] Dyrektywa 2007/64/WE Parlamentu Europejskiego i Rady 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.

[4] Podmiot zarządzający systemem płatności jest odpowiedzialny za całościowe funkcjonowanie systemu promującego dany instrument płatniczy oraz za zapewnienie, aby wszystkie strony postępowały zgodnie z zasadami systemu. Ponadto jest on odpowiedzialny za zapewnienie zgodności systemu ze standardami nadzorczymi. „Harmonised oversight approach and oversight standards for payment instruments", Europejski Bank Centralny (luty 2012 r.).

[5] Integratorzy płatności dostarczają odbiorcom płatności (tj. akceptantom) wystandaryzowany interfejs usług inicjacji płatności świadczonych przez dostawców usług płatniczych.

- płatności mobilne inne niż realizowane przy użyciu przeglądarki internetowej[6];
- polecenia przelewu, w przypadku których strona trzecia uzyskuje dostęp do rachunku płatniczego klienta;
- transakcje płatnicze dokonywane przez przedsiębiorstwa poprzez dedykowane sieci;
- płatności kartowe 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.

Zasady przewodnie

Rekomendacje oparte są na czterech zasadach przewodnich.

Po pierwsze, dostawcy usług płatniczych i podmioty zarządzające systemami płatności powinni przeprowadzić szczegółowe oceny ryzyk związanych ze świadczeniem usług płatności internetowych, które powinny być regularnie aktualizowane zgodnie ze zmianami w zakresie zagrożeń bezpieczeństwa w internecie oraz mechanizmów nadużyć. W przeszłości zidentyfikowane zostały pewne ryzyka w tym obszarze, np. przez Bank Rozrachunków Międzynarodowych (Bank for International Settlements) w 2003 r.[7] oraz przez Federalną Radę Badania Instytucji Finansowych (Federal Financial Institutions Examination Council)[8] w latach 2005 i 2011[9]. Jednakże w związku z tempem postępu technologicznego oraz wprowadzania nowych metod płatności internetowych, oraz z faktem, że przestępcy stali się bardziej zorganizowani, zaś ich ataki bardziej wyrafinowane, regularna ocena przedmiotowych ryzyk jest niezmiernie istotna.

Po drugie, zasadą ogólną jest, aby inicjacja płatności internetowych oraz dostęp do wrażliwych danych dotyczących płatności były chronione przez silne uwierzytelnianie klienta. Na potrzeby niniejszego raportu, wrażliwe dane dotyczące płatności zdefiniowane są jako dane, które mogą być wykorzystane w celu dokonania nadużycia, w tym dane umożliwiające zainicjowanie zlecenia płatniczego, dane wykorzystywane do uwierzytelniania, dane wykorzystywane do zamawiania przez klientów instrumentów płatniczych lub narzędzi uwierzytelniających, jak również dane, parametry i oprogramowanie, które – w przypadku modyfikacji – mogą mieć wpływ na zdolność uprawnionej strony do weryfikowania transakcji płatniczych, autoryzowania poleceń przelewu lub kontroli rachunków, takie jak „czarne" lub „białe" listy, limity określone przez klienta itp.

Silne uwierzytelnianie klienta jest procedurą opierającą się na dwóch lub więcej spośród następujących elementów – klasyfikowanych jako wiedza, posiadanie i cechy klienta: i) coś, co jedynie użytkownik wie, np. statyczne hasło, kod, osobisty numer identyfikacyjny; ii) coś, co jedynie użytkownik posiada, np. token, karta smart, telefon komórkowy; iii) coś, czym użytkownik jest, np. w oparciu o cechy biometryczne, takie jak odcisk palca. Dodatkowo,

[6] Niektóre z tych elementów mogą stać się przedmiotem odrębnego raportu na późniejszym etapie.
[7] Szczegółowe rekomendacje dotyczące publikowania i utrzymywania aplikacji będą przedmiotem odrębnych prac w zakresie płatności mobilnych.
[8] „Risk Management Principles for Electronic Banking", Bank Rozrachunków Międzynarodowych (lipiec 2003 r.).
[9] „Authentication in an Internet Banking Environment", Federalna Rada Badania Instytucji Finansowych (październik 2005 r.). Patrz też: suplement do wytycznych z 2005 r. (czerwiec 2011 r.).

wybrane elementy muszą być wzajemnie niezależne, tj. naruszenie bezpieczeństwa jednego nie naraża innego (innych). Co najmniej jeden z elementów musi być niemożliwy do ponownego użycia i niemożliwy do zreplikowana (z wyjątkiem cech klienta), jak również niemożliwy do niejawnego, nieautoryzowanego pozyskania przez internet. Procedura silnego uwierzytelniania powinna być zaprojektowana w sposób zapewniający poufność danych uwierzytelniających.

Z perspektywy Forum, dostawcy usług płatniczych nieposiadający lub posiadający jedynie słabe procedury uwierzytelniania nie mogą – w przypadku wystąpienia spornej transakcji – dostarczyć dowodu, że użytkownik autoryzował transakcję.

Po trzecie, dostawcy usług płatniczych powinni wdrożyć efektywne procesy autoryzowania transakcji, jak również monitorowania transakcji i systemów w celu identyfikowania nietypowych wzorców zachowań płatniczych klientów i przeciwdziałania nadużyciom.

Po czwarte, dostawcy usług płatniczych i podmioty zarządzające systemami płatności powinni angażować się w programy edukowania i zwiększania świadomości klientów w zakresie kwestii bezpieczeństwa związanych z korzystaniem z usług płatności internetowych, mając na względzie umożliwienie klientom[10] korzystania z takich usług w sposób bezpieczny i efektywny.

W celu umożliwienia dostosowania do ciągłych innowacji technologicznych rekomendacje zostały sformułowane w sposób na tyle ogólny, na ile było to możliwe. Jednakże Forum jest świadome, że nowe zagrożenia pojawić mogą się w każdym momencie, w związku z czym rekomendacje co pewien czas będą przedmiotem przeglądu.

Niniejszy raport nie wskazuje konkretnych rozwiązań technicznych czy w zakresie bezpieczeństwa, jak również nie redefiniuje ani nie sugeruje wprowadzania zmian do istniejących technicznych standardów branżowych lub oczekiwań nadzorczych w obszarach ochrony danych i ciągłości działania. Oceniając zgodność z rekomendacjami, organy nadzorcze mogą brać pod uwagę zgodność z odpowiednimi standardami międzynarodowymi. Pomimo tego, że rekomendacje wskazują na pewne rozwiązania, te same rezultaty mogą być osiągane innymi środkami.

Rekomendacje przedstawione w niniejszym raporcie określają oczekiwania minimalne. Nie ograniczają one odpowiedzialności dostawców usług płatniczych, podmiotów zarządzających systemami płatności oraz innych uczestników rynku za monitorowanie i ocenę ryzyk związanych z ich operacjami płatniczymi, opracowywanie własnych szczegółowych polityk bezpieczeństwa oraz wdrażanie odpowiednich środków w zakresie bezpieczeństwa, planowania awaryjnego, zarządzania incydentami oraz ciągłości działania, współmiernych do ryzyk związanych ze świadczonymi usługami płatniczymi.

[10] Klienci oznaczają zarówno konsumentów, jak i przedsiębiorców, dla których świadczone są usługi płatnicze.

Implementacja

Niniejszy raport zawiera 14 rekomendacji mających na celu promowanie bezpieczeństwa płatności internetowych. Każda rekomendacja jest precyzowana poprzez opisy tzw. „kluczowych kwestii" (KK, ang. Key Considerations), które powinny być czytane łącznie z rekomendacjami w celu pełnego zrozumienia minimalnych oczekiwań w zakresie zgodności z rekomendacjami. Oczekuje się, aby adresaci stosowali się zarówno do rekomendacji, jak i kluczowych kwestii, lub byli w stanie wyjaśnić i uzasadnić wszelkie niezgodności na żądanie właściwych organów nadzorczych (tzw. zasada „comply or explain"). Ponadto raport przedstawia dobre praktyki (DP), do stosowania których zachęcani są dostawcy usług płatniczych, podmioty zarządzające systemami płatności i odpowiedni uczestnicy rynku.

Prawną podstawę wdrożenia rekomendacji przez narodowe władze nadzorcze stanowi krajowe prawodawstwo transponujące dyrektywę ws. usług płatniczych i / lub istniejące kompetencje nadzorcze odpowiednich organów. Członkowie Forum poczuwają się do wspierania wdrożenia rekomendacji w swoich krajach i uwzględnią je w ramach sprawowanego nadzoru. Forum będzie również starało się zapewnić efektywne i spójne wdrożenie w poszczególnych krajach i może w tym celu współpracować z odpowiednimi organami.

Rekomendacje powinny zostać wdrożone przez dostawców usług płatniczych i podmioty zarządzające systemami płatności do dnia 1 lutego 2015 r., przy czym organy krajowe mogą w stosownych przypadkach określić krótszy okres przejściowy.

Układ raportu

Rekomendacje zostały podzielone na trzy kategorie:

Kontrola ogólna i środowisko bezpieczeństwa platform wspierających usługi płatności internetowych. W ramach swych procedur zarządzania ryzykiem, dostawcy usług płatniczych powinni oceniać adekwatność wewnętrznych mechanizmów kontrolnych w kontekście scenariuszy wewnętrznych i zewnętrznych ryzyk. Rekomendacje należące do pierwszej kategorii odnoszą się do kwestii związanych z ładem korporacyjnym, identyfikacją i oceną ryzyka, monitorowaniem i raportowaniem, zagadnień kontroli i przeciwdziałania ryzyku oraz zapewnienia możliwości śledzenia (ang. traceability).

Kontrola szczególna i środki bezpieczeństwa w zakresie płatności internetowych. Rekomendacje należące do drugiej kategorii obejmują wszystkie etapy przetwarzania transakcji płatniczych, od uzyskania dostępu do usługi (rozwiązania w zakresie informowania, rejestrowania i uwierzytelniania klientów) po inicjowanie, monitorowanie i autoryzowanie płatności, jak również ochronę wrażliwych danych płatniczych.

Świadomość, edukacja i komunikacja z klientami. Rekomendacje należące do trzeciej kategorii dotyczą ochrony klientów; tego, co klienci powinni robić w przypadku otrzymania niezamawianego żądania podania osobistych danych logowania; tego, w jaki sposób używać bezpiecznie usług płatności internetowych oraz tego, w jaki sposób klienci mogą zweryfikować, czy transakcja została zainicjowana i wykonana.

Raport zawiera ponadto słownik wybranych podstawowych pojęć. W załączniku podana została lista członków Forum.

2 Rekomendacje

Kontrola ogólna i środowisko bezpieczeństwa

Rekomendacja 1: Ład korporacyjny

Dostawcy usług płatniczych i systemy płatności powinni wdrożyć i regularnie przeglądać formalną politykę bezpieczeństwa płatności internetowych.

KK 1.1 Polityka bezpieczeństwa powinna być odpowiednio udokumentowana i regularnie przeglądana (zgodnie z KK 2.4) oraz zatwierdzona przez wyższą kadrę kierowniczą. Powinna ona określać cele w zakresie bezpieczeństwa oraz apetyt na ryzyko.

KK 1.2 Polityka bezpieczeństwa powinna określać role i zakresy odpowiedzialności, w tym funkcję zarzadzania ryzykiem z bezpośrednim raportowaniem do poziomu zarządu, oraz porządek podległości służbowej w zakresie świadczonych usług płatności internetowych, w tym zarządzania wrażliwymi danymi płatniczymi z uwzględnieniem oceny, kontroli i przeciwdziałania ryzyku.

DP 1.1 Polityka bezpieczeństwa może zostać opracowana w formie dedykowanego dokumentu.

Rekomendacja 2: Ocena ryzyka

Dostawcy usług płatniczych i systemy płatności powinni przeprowadzać i dokumentować szczegółowe oceny ryzyka dotyczące płatności internetowych i usług powiązanych, zarówno przed wprowadzeniem tych usług, jak i regularnie po ich prowadzeniu.

KK 2.1 Dostawcy usług płatniczych i systemy płatności powinni – poprzez swoje funkcje zarządzania ryzykiem – przeprowadzać i dokumentować szczegółowe oceny ryzyka w zakresie płatności internetowych i usług powiązanych. Dostawcy usług płatniczych i systemy płatności powinni brać pod uwagę rezultaty bieżącego monitorowania zagrożeń w zakresie bezpieczeństwa oferowanych i planowanych do wprowadzenia usług płatności internetowych, z uwzględnieniem: i) wykorzystywanych rozwiązań technologicznych, ii) usług świadczonych przez dostawców zewnętrznych oraz iii) środowiska technicznego klienta. Dostawcy usług płatniczych i systemy płatności powinni badać ryzyka związane z wybranymi platformami technologicznymi, architekturą aplikacji, technikami programistycznymi oraz procedurami, zarówno po swojej stronie[11], jak i po stronie klientów[12], a także wyniki procesu monitorowania incydentów bezpieczeństwa (patrz: Rekomendacja 3).

[11] Takie jak podatność systemu na przechwycenie sesji płatniczej, „wstrzykiwanie SQL" (ang. SQL injection), „skrypty krzyżowe" (ang. cross-site scripting), przepełnienia bufora (ang. buffer overflow) itd.

[12] Takie jak ryzyka związane z korzystaniem z aplikacji multimedialnych, dodatków do przeglądarek internetowych, ramek (ang. frames), linków zewnętrznych itd.

KK 2.2 Na tej podstawie dostawcy usług płatniczych i systemy płatności powinni określać, czy i w jakim stopniu niezbędne może być wprowadzenie zmian do istniejących środków bezpieczeństwa, wykorzystywanych technologii oraz procedur lub oferowanych usług. Dostawcy usług płatniczych i systemy płatności powinni brać pod uwagę czas niezbędny do wprowadzenia tych zmian (w tym również po stronie klientów) oraz podjąć odpowiednie kroki w okresie przejściowym w celu zminimalizowania incydentów bezpieczeństwa i przypadków nadużyć, jak również potencjalnych efektów zakłócających działalność.

KK 2.3 Ocena ryzyka powinna odnosić się do potrzeb w zakresie ochrony i zabezpieczenia wrażliwych danych płatniczych.

KK 2.4 Dostawcy usług płatniczych i systemy płatności powinni przeprowadzać przegląd scenariuszy ryzyka i istniejących środków bezpieczeństwa po wystąpieniu istotnych incydentów mających wpływ na świadczone przez nich usługi, przed wprowadzeniem istotnych zmian w infrastrukturze lub procedurach oraz po zidentyfikowaniu nowych zagrożeń w ramach monitorowania ryzyka. Dodatkowo, co najmniej raz w roku przeprowadzany powinien być ogólny przegląd oceny ryzyka. Rezultaty oceny ryzyka oraz przeglądów powinny być zatwierdzane przez wyższą kadrę kierowniczą.

Rekomendacja 3: Monitorowanie i raportowanie incydentów

Dostawcy usług płatniczych i systemy płatności powinni posiadać spójne i zintegrowane podejście do monitorowania, obsługi i działań następczych w stosunku do incydentów, w tym skarg klientów związanych z bezpieczeństwem. Dostawcy usług płatniczych i systemy płatności powinni opracować procedurę raportowania takich incydentów do kadry kierowniczej oraz – w przypadku istotnych incydentów bezpieczeństwa dotyczących płatności – organów nadzorczych.

KK 3.1 Dostawcy usług płatniczych i systemy płatności powinni wprowadzić proces monitorowania, obsługi i realizacji działań następczych w stosunku do incydentów bezpieczeństwa oraz skarg klientów związanych z bezpieczeństwem, oraz raportować takie incydenty kadrze zarządzającej.

KK 3.2 Dostawcy usług płatniczych i systemy płatności powinni posiadać procedurę niezwłocznego informowania właściwych organów (tj. organów nadzoru oraz organów ds. ochrony danych), tam gdzie one istnieją, w przypadku wystąpienia istotnych incydentów bezpieczeństwa w zakresie świadczonych usług płatniczych.

KK 3.3 Dostawcy usług płatniczych i systemy płatności powinni posiadać procedurę współpracy z właściwymi organami ścigania w zakresie istotnych incydentów bezpieczeństwa, w tym naruszenia danych.

KK 3.4 Dostawcy usług płatniczych będący agentami rozliczeniowymi powinni wymagać od akceptantów przechowujących, przetwarzających lub przesyłających wrażliwe dane płatnicze, aby współpracowali w zakresie istotnych incydentów bezpieczeństwa płatności (w tym naruszenia danych) zarówno z dostawcami usług płatniczych, jak i z właściwymi organami ścigania. W przypadku, gdy dostawca usług płatniczych uzyska wiedzę o tym, że akceptant

nie współpracuje zgodnie z wymaganiami umownymi, powinien podjąć kroki mające na celu doprowadzenie do wywiązywania się akceptanta ze zobowiązań umownych lub rozwiązać umowę.

Rekomendacja 4: Kontrola i przeciwdziałanie ryzyku

Dostawcy usług płatniczych i systemy płatności powinni wdrożyć środki bezpieczeństwa zgodnie z opracowanymi politykami bezpieczeństwa w celu przeciwdziałania zidentyfikowanym ryzykom. Środki te powinny uwzględniać wiele linii obrony, w przypadku których niepowodzenie jednej linii obrony jest niwelowane przez kolejną linię obrony.

KK 4.1 Projektując, rozwijając i utrzymując usługi płatności internetowych, dostawcy usług płatniczych i systemy płatności powinni przykładać szczególną wagę do odpowiedniego podziału obowiązków w środowiskach teleinformatycznych (np. środowisk rozwojowych, testowych i produkcyjnych) oraz właściwego wdrożenia zasady minimalnych uprawnień[13] jako podstawy poprawnego zarządzania tożsamością i dostępem.

KK 4.2 Dostawcy usług płatniczych i systemy płatności powinni posiadać odpowiednie rozwiązania w zakresie bezpieczeństwa mające na celu zabezpieczenie sieci, stron internetowych, serwerów i łączy komunikacyjnych przed nadużyciami i atakami. Dostawcy usług płatniczych i systemy płatności powinni wyłączać w serwerach wszystkie zbędne funkcje w celu ich ochrony („utwardzenia") i wyeliminowania lub ograniczenia podatności narażonych aplikacji. Dostęp różnych aplikacji do danych i zasobów powinien być ograniczony do niezbędnego minimum, zgodnie z zasadą minimalnych uprawnień. W celu ograniczenia wykorzystania fałszywych stron internetowych (imitujących rzeczywiste strony internetowe dostawców usług płatniczych), transakcyjne strony internetowe udostępniające usługi płatności internetowych powinny być identyfikowane przez rozszerzone certyfikaty walidacyjne dostawców usług internetowych lub zbliżone metody uwierzytelniania.

KK 4.3 Dostawcy usług płatniczych i systemy płatności 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 itd. Dostawcy usług płatniczych powinni tworzyć, przechowywać i analizować odpowiednie dzienniki zdarzeń i ślady audytowe (ang. audit trails).

KK 4.4 Projektując[14], rozwijając i utrzymując usługi płatności internetowych, dostawcy usług płatniczych powinni zapewnić, aby kluczowym elementem podstawowej funkcjonalności była minimalizacja danych[15]: zbieranie, przesyłanie, przetwarzanie, przechowywanie i / lub archiwizowanie oraz wizualizowanie wrażliwych danych płatniczych powinny być utrzymywane na minimalnym poziomie.

---

[13] „Każdy program i każdy użytkownik systemu powinni działać z wykorzystaniem najmniejszej ilości uprawnień niezbędnych do wykonania danego działania". Patrz: J. H. Saltzer, „Protection and the Control of Information Sharing in Multics", „Communications of the ACM", Vol. 17, Nr 7 (1974 r.).

[14] Domyślna ochrona prywatności.

[15] Minimalizacja danych oznacza politykę gromadzenia najmniejszej ilości informacji osobistych niezbędnych do realizacji danej funkcji.

KK 4.5 Środki bezpieczeństwa dla usług płatności internetowych powinny być testowane pod nadzorem funkcji zarządzania ryzykiem w celu zapewnienia ich efektywności i poprawnej konstrukcji. Wszystkie zmiany powinny podlegać formalnemu procesowi zarządzania zmianą zapewniającego poprawne planowanie, testowanie, dokumentowanie i akceptowanie zmian. Na podstawie dokonanych zmian oraz zaobserwowanych zagrożeń, testy powinny być regularnie powtarzane i powinny uwzględniać scenariusze istotnych i znanych potencjalnych ataków.

KK 4.6 Stosowane przez dostawców usług płatniczych środki bezpieczeństwa w zakresie usług płatności internetowych powinny być przedmiotem okresowych audytów w celu zapewnienia ich efektywności i poprawnej konstrukcji. Wdrażanie i funkcjonowanie usług płatności internetowych również powinno być przedmiotem audytów. Częstotliwość i tematyka audytów powinny uwzględniać i być proporcjonalne do ryzyk w zakresie bezpieczeństwa. Audyty powinny być przeprowadzane przez wiarygodnych i niezależnych ekspertów (wewnętrznych lub zewnętrznych), którzy nie powinni być w żaden sposób zaangażowani w rozwój, wdrażanie lub operacyjne zarządzanie świadczonymi usługami płatności internetowych.

KK 4.7 W przypadkach, gdy dostawcy usług płatniczych i systemy płatności zlecają zewnętrznym podmiotom funkcje związane z usługami płatności internetowych, treść umowy powinna określać wymogi dotyczące zapewnienia zgodności z zasadami i rekomendacjami wymienionymi w niniejszym raporcie.

KK 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 ich infrastrukturach IT, zgodnie z KK 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 nie stosuje wymaganych środków bezpieczeństwa, powinien podjąć kroki mające na celu doprowadzenie do wywiązywania się akceptanta ze zobowiązań umownych lub rozwiązać umowę.

DP 4.1 Dostawcy usług płatniczych mogą dostarczać narzędzi bezpieczeństwa (tj. urządzeń i / lub dostosowanych przeglądarek internetowych, odpowiednio zabezpieczonych) w celu ochrony interfejsu klienta przed nielegalnym wykorzystaniem lub atakami (np. atakami typu „Man-in-the-Browser").

Rekomendacja 5: Śledzenie (ang. traceability)

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

KK 5.1 Dostawcy usług płatniczych powinni zapewnić, aby świadczone przez nich usługi uwzględniały mechanizmy bezpieczeństwa w zakresie szczegółowego rejestrowania transakcji i danych dotyczących poleceń zapłaty, w tym numerów porządkowych transakcji, znaczników czasowych danych transakcji, zmian parametryzacji oraz dostępu do danych transakcji i poleceń zapłaty.

KK 5.2 Dostawcy usług płatniczych powinni wdrożyć dzienniki zdarzeń pozwalające na śledzenie wprowadzania nowych oraz modyfikowania i usuwania istniejących danych transakcji i poleceń zapłaty.

KK 5.3 Dostawcy usług płatniczych powinni analizować dane transakcji i poleceń zapłaty oraz posiadać narzędzia do oceny dzienników zdarzeń. Odpowiednie aplikacje powinny być dostępne jedynie dla upoważnionych pracowników.

DP 5.1 Dostawcy usług płatniczych świadczący usługi agenta rozliczeniowego mogą wymagać w umowach zawieranych z akceptantami przechowującymi informacje dotyczące płatności, aby wdrożyli oni odpowiednie procesy wspierające możliwość śledzenia.

Kontrola szczególna i środki bezpieczeństwa w zakresie płatności internetowych

Rekomendacja 6: Wstępna identyfikacja klienta, informacje

Klienci powinni być odpowiednio identyfikowani – zgodnie z europejskim prawodawstwem w zakresie przeciwdziałania praniu pieniędzy[16] – oraz 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 przed nich z danej usługi, regularnie, lub – o ile ma to zastosowanie – ad hoc) dotyczące wymagań (np. sprzętu, procedur) w zakresie bezpiecznego przeprowadzania transakcji płatności internetowych i dotyczące ryzyk inherentnych.

KK 6.1 Dostawcy usług płatniczych powinni zapewnić, aby klienci podlegali procedurom due dilligence oraz dostarczali odpowiednie dokumenty identyfikacyjne[17] oraz powiązane informacje przed udzieleniem im dostępu do usług płatności internetowych[18].

KK 6.2 Dostawcy usług płatniczych powinni zapewnić, aby informacje dostarczane klientom przed skorzystaniem przez nich z danej usługi[19] określały kwestie związane z usługami płatności internetowych. Powinny one – w stosownych przypadkach – uwzględniać:

[16] 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. Patrz też: Dyrektywa Komisji 2006/70/WE z dnia 1 sierpnia 2006 r. ustanawiająca 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.

[17] Np. paszport, krajowa karta identyfikacyjna lub zaawansowany podpis elektroniczny.

[18] Proces identyfikacji klienta nie narusza jakichkolwiek wyłączeń przewidzianych w regulacjach w zakresie przeciwdziałania praniu pieniędzy. Dostawcy usług płatniczych nie muszą przeprowadzać odrębnego procesu identyfikacji klienta w odniesieniu do usług płatności internetowych, pod warunkiem, że taka identyfikacja klienta została już przeprowadzona, np. w zakresie istniejących usług związanych z płatnościami czy też otwieraniem rachunku.

[19] Ta informacja stanowi uzupełnienie Art. 42 dyrektywy ws. usług płatniczych, w którym określono informacje, jakie dostawcy usług płatniczych muszą dostarczać użytkownikom usług płatniczych przed zawarciem umowy w zakresie świadczenia usług płatniczych.

- jasne informacje dotyczące wymagań w zakresie sprzętu klienta, jego oprogramowania lub innych niezbędnych narzędzi (np. oprogramowania antywirusowego, zapór ogniowych);
- wytyczne dotyczące właściwego i bezpiecznego korzystania z danych logowania;
- opis (krok po kroku) procedury przesyłania i autoryzowania przez klienta transakcji płatniczej i / lub uzyskiwania informacji, w tym dotyczących konsekwencji każdego działania;
- wytyczne dotyczące właściwego i bezpiecznego korzystania ze sprzętu i oprogramowania dostarczanego klientowi;
- procedury postępowania w przypadku utraty lub kradzieży danych logowania lub sprzętu lub oprogramowania klienta wykorzystywanego do logowania lub przeprowadzania transakcji;
- procedury postępowania w przypadku wystąpienia lub podejrzenia wystąpienia nadużycia;
- opis obowiązków dostawcy usług płatniczych i klienta w zakresie korzystania z usług płatności internetowych.

KK 6.3 dostawcy usług płatniczych powinni zapewnić, aby umowa ramowa z klientem wskazywała, że dostawca usług płatniczych może zablokować określoną transakcję lub instrument płatniczy[20] ze względów bezpieczeństwa. Powinna ona określać metody i terminy powiadamiania klienta oraz sposób, w jaki klient może skontaktować się z dostawcą usług płatniczych w celu odblokowania transakcji lub usługi płatności internetowych, zgodnie z dyrektywą ws. usług płatniczych.

KK 6.4 Dostawcy usług płatniczych powinni również zapewnić, aby klientom na bieżąco lub – w stosownych przypadkach – ad hoc, odpowiednimi kanałami (np. w postaci ulotek czy na stronach internetowych) dostarczane były jasne i zrozumiałe instrukcje wyjaśniające ich odpowiedzialność w zakresie bezpiecznego korzystania z usług.

DP 6.1 Klient może podpisać dedykowaną umowę na świadczenie usług w zakresie przeprowadzania transakcji płatności internetowych zamiast wyrażenia zgody na warunki ujęte w szerszej, ogólnej umowie o świadczenie usług zawartej z dostawcą usług płatniczych.

Rekomendacja 7: Silne uwierzytelnianie klienta

Inicjowanie płatności internetowej, jak również dostęp do wrażliwych danych płatniczych, powinny być chronione silnym uwierzytelnianiem klienta.

KK 7.1 [polecenia przelewu / polecenia zapłaty / pieniądz elektroniczny] dostawcy usług płatniczych powinni dokonywać silnego uwierzytelniania klienta na potrzeby autoryzacji przez klienta transakcji płatności internetowych (w tym również pakietów poleceń przelewu) oraz wystawiania lub modyfikacji elektronicznych poleceń zapłaty. Jednakże, dostawcy usług płatniczych mogą rozważyć alternatywne środki uwierzytelniania klienta na potrzeby:

- płatności wychodzących do zaufanych odbiorców wymienionych na uprzednio opracowanej białej liście klienta;
- transakcji pomiędzy dwoma rachunkami płatniczymi tego samego klienta prowadzonymi przez tego samego dostawcę usług płatniczych;

[20] Patrz: Art. 55 dyrektywy ws. usług płatniczych dotyczący limitów w zakresie korzystania z instrumentów płatniczych.

- przelewów dokonywanych w ramach tego samego dostawcy usług płatniczych, w przypadkach uzasadnionych analizą ryzyka transakcji;
- płatności o niskiej wartości, zgodnie z dyrektywą ws. usług płatniczych[21].

KK 7.2 Uzyskanie dostępu do wrażliwych danych płatniczych lub modyfikacja tych danych (w tym tworzenie i modyfikowanie białych list) wymaga silnego uwierzytelniania klienta. W przypadku, gdy dostawca usług płatniczych oferuje jedynie usługi doradcze, nie wyświetlając wrażliwych informacji dotyczących klienta lub płatności, które mogłyby być łatwo wykorzystane w celu popełnienia oszustwa (takich jak dane kart płatniczych), dostawca usług płatniczych może dobierać wymagania w zakresie uwierzytelniania na podstawie oceny ryzyka.

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

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

KK 7.5 [karty] Dostawcy usług płatniczych świadczący usługi agenta rozliczeniowego powinni wymagać od akceptantów wsparcia dla rozwiązań pozwalających wydawcy karty na przeprowadzenie silnego uwierzytelniania posiadacza karty w zakresie transakcji kartowych realizowanych przez internet. Można rozważyć wykorzystanie alternatywnych środków uwierzytelniania w zakresie uprzednio określonych kategorii transakcji niskiego ryzyka, np. w oparciu o analizę ryzyka transakcji, lub płatności o niskiej wartości, zgodnie z dyrektywą ws. usług płatniczych.

KK 7.6 Wszystkie systemy płatności powinny promować wdrażanie silnego uwierzytelniania klienta poprzez wprowadzenie zasad odpowiedzialności[22] dla uczestniczących dostawców usług płatniczych w ramach rynków europejskich.

KK 7.7 [karty] W zakresie systemów płatności akceptowanych przez daną usługę, dostawcy rozwiązań portfelowych powinni wymagać silnego uwierzytelniania przez wydawcę karty w przypadkach, gdy prawowity / legalny posiadacz po raz pierwszy rejestruje dane karty.

KK 7.8 Dostawcy rozwiązań portfelowych powinni wspierać silne uwierzytelnianie klienta w przypadkach, w których klienci logują się do usług płatności portfelowych lub dokonują transakcji kartowych przez internet. Można rozważyć wykorzystanie alternatywnych środków uwierzytelniania w zakresie uprzednio określonych kategorii transakcji niskiego ryzyka, np. w oparciu o analizę ryzyka transakcji, lub płatności o niskiej wartości, zgodnie z dyrektywą ws. usług płatniczych.

[21] Patrz: definicja płatności o niskiej wartości w Art. 34(1) i 53(1) dyrektywy ws. usług płatniczych.

[22] Zasady odpowiedzialności powinny zapewniać, aby dostawca usług płatniczych był zobowiązany zwrócić innym dostawcom usług płatniczych kwoty związane z jakimikolwiek oszustwami wynikającymi ze słabego uwierzytelniania klienta.

KK 7.9 [karty] W zakresie kart wirtualnych, wstępna rejestracja powinna odbywać się w bezpiecznym i zaufanym środowisku[23]. Silne uwierzytelnianie klienta powinno być wymagane w procesie generowania danych kart wirtualnych w przypadku, gdy karta wydawana jest w środowisku internetowym.

KK 7.10 Dostawcy usług płatniczych powinni zapewniać właściwe dwustronne uwierzytelnianie w przypadkach komunikacji z akceptantami w celu zainicjowania płatności internetowych oraz dostępu do wrażliwych danych płatniczych.

DP 7.1 [karty] Akceptanci mogą wspierać silne uwierzytelnianie posiadacza karty przez wydawcę w przypadku transakcji realizowanych przez internet.

DP 7.2 W celu zapewnienia wygody klientom, dostawcy usług płatniczych mogą rozważyć wykorzystanie pojedynczego narzędzia silnego uwierzytelniania klienta dla wszystkich usług płatności internetowych. Mogłoby to podnieść poziom akceptacji rozwiązania wśród klientów i przyczynić się do poprawy jego prawidłowego wykorzystywania.

DP 7.3 Silne uwierzytelnianie klienta może uwzględniać elementy łączące uwierzytelnianie z konkretną kwotą i odbiorcą płatności. Może to zwiększyć stopień pewności klientów w ramach autoryzowania płatności. Rozwiązanie techniczne pozwalające na powiązanie danych wykorzystywanych do silnego uwierzytelniania z danymi transakcji powinno być odporne na manipulację.

Rekomendacja 8: Wnioskowanie o narzędzia uwierzytelniające i/lub oprogramowanie oraz ich dostarczanie

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

KK 8.1 Wnioskowanie przez klientów o narzędzia uwierzytelniające i / lub oprogramowanie oraz ich dostarczanie klientom powinno spełniać następujące wymagania:

- Procedury w tym zakresie powinny być realizowane w bezpiecznym i zaufanym środowisku, z uwzględnieniem potencjalnych ryzyk wynikających z urządzeń znajdujących się poza kontrolą dostawcy usług płatniczych.
- Powinny obowiązywać efektywne i bezpieczne procedury w zakresie dostarczania spersonalizowanych danych logowania, oprogramowania wymaganego do płatności oraz wszelkich spersonalizowanych urządzeń wymaganych do płatności internetowych. Oprogramowanie dostarczane przez internet powinno być podpisane cyfrowo przez dostawcę usług płatniczych, w celu umożliwienia klientom dokonania weryfikacji jego autentyczności oraz sprawdzenia, czy nie podlegało ono manipulacji.

[23] 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) siedzibę 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 Rekomendacji 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).

- [karty] W przypadku transakcji kartowych, klient powinien mieć możliwość wyboru silnego uwierzytelniania niezależnie dla poszczególnych zakupów internetowych. Jeżeli oferowana jest możliwość aktywacji podczas zakupów online, powinno to być dokonywane poprzez przekierowanie klienta do bezpiecznego i zaufanego środowiska.

KK 8.2 [karty] Wydawcy kart 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 kartową.

Rekomendacja 9: Próby logowania, wygasanie sesji, ważność uwierzytelnienia

Dostawcy usług płatniczych powinni ograniczać liczbę prób logowania i uwierzytelniania, określić zasady wygasania sesji usług płatności internetowych oraz ustalić ograniczenia ważności uwierzytelnienia.

KK 9.1 Jeżeli na potrzeby uwierzytelniania wykorzystywane są hasła jednorazowe, dostawcy usług płatniczych powinni zapewnić, aby okres ważności takich haseł był ograniczony do niezbędnego minimum.

KK 9.2 Dostawcy usług płatniczych powinni określić maksymalną liczbę nieudanych prób logowania i uwierzytelniania, po której dostęp do usług płatności internetowych jest blokowany (tymczasowo lub na stałe). Powinni również posiadać bezpieczne procedury reaktywowania zablokowanych usług płatności internetowych.

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

Rekomendacja 10: Monitorowanie transakcji

Mechanizmy monitorowania transakcji mające na celu zapobieganie, wykrywanie i blokowanie oszukańczych transakcji płatniczych powinny być uruchamiane przed ostateczną autoryzacją płatności przez dostawcę usług płatniczych; podejrzane transakcje i transakcje wysokiego ryzyka powinny podlegać procedurze sprawdzenia i oceny. Analogiczne mechanizmy monitorowania bezpieczeństwa i autoryzacji powinny funkcjonować również w zakresie wystawiania poleceń zapłaty.

KK 10.1 Dostawcy usług płatniczych powinni wykorzystywać systemy wykrywania i zapobiegania oszustwom w celu identyfikacji transakcji podejrzanych przed ostateczną autoryzacją transakcji lub poleceń zapłaty. Systemy te powinny być oparte np. na parametryzowanych regułach (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[24], czasem identyfikowane przez sprawdzenie geolokalizacji adresu IP[25], nietypowe kategorie akceptantów dla danego klienta czy nietypowe dane transakcji itd.). Systemy te powinny również być zdolne do wykrywania symptomów infekcji sesji przez szkodliwe oprogramowanie (np. poprzez sprawdzenie, czy dana czynność realizowana jest przez skrypt, czy przez człowieka) oraz znanych scenariuszy

[24] Adres IP to unikalny kod numeryczny identyfikujący każdy komputer podłączony do internetu.
[25] Geolokalizacja adresu IP ma na celu określenie miejsca, z którego inicjowana jest transakcja, na podstawie adresu IP.

oszustw. Zakres, stopień złożoności oraz zdolności adaptacyjne rozwiązań monitorujących, przy zapewnieniu zgodności ze stosownym prawodawstwem w zakresie ochrony danych, powinny być współmierne do rezultatów oceny ryzyka.

KK 10.2 Systemy płatności kartowych we współpracy z agentami rozliczeniowymi powinny wypracować zharmonizowane definicje kategorii akceptantów oraz wymagać od agentów rozliczeniowych wdrożenia tych definicji w komunikatach autoryzacyjnych przekazywanych wydawcom kart przez dostawców usług płatniczych[26].

KK 10.3 Dostawcy usług płatniczych będący agentami rozliczeniowymi powinni posiadać systemy wykrywania i zapobiegania nadużyciom monitorujące działania akceptantów.

KK 10.4 Dostawcy usług płatniczych powinni realizować procedury sprawdzania i oceny przez odpowiedni czas, tak aby nadmiernie nie opóźniać inicjowania i / lub wykonania danej usługi płatniczej.

KK 10.5 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.

Rekomendacja 11: Ochrona wrażliwych danych płatniczych

Wrażliwe dane płatnicze powinny podlegać ochronie w zakresie ich przechowywania, przetwarzania i przesyłania.

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

KK 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 stosowane było bezpieczne szyfrowanie „end-to-end”[27], przy użyciu silnych i powszechnie stosowanych technik szyfrowania.

KK 11.3 Dostawcy usług płatniczych świadczący usługi agenta rozliczeniowego powinni zachęcać akceptantów do nieprzechowywania jakichkolwiek wrażliwych danych płatniczych. W przypadkach, gdy akceptanci obsługują (tj. przechowują, przetwarzają lub przesyłają) wrażliwe dane płatnicze, dostawcy usług płatniczych powinni wprowadzić w umowach z

[26] Kategorie akceptantów odnoszą się do klasyfikacji akceptantów w odniesieniu do sektorów lub działalności biznesowej. Obecnie kategorie akceptantów nie są zestandaryzowane w systemach kart płatniczych i nie zawsze są przekazywane w komunikacie autoryzacyjnym. Zharmonizowana klasyfikacja kategorii akceptantów (oparta np. na europejskiej klasyfikacji NACE) mogłaby wspomóc dostawców usług płatniczych w zakresie analizy ryzyka nadużycia dla transakcji.

[27] Szyfrowanie „end-to-end” odnosi się do sytuacji, w których szyfrowanie odbywa się w systemie źródłowym, zaś odpowiednie deszyfrowanie odbywa się jedynie w systemie docelowym (ETSI EN 302 109 V1.1.1).

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.

DP 11.1 Pożądane jest, aby akceptanci obsługujący wrażliwe dane płatnicze odpowiednio szkolili swoje kadry odpowiedzialne za zarządzanie ryzykiem oraz regularnie aktualizowali te szkolenia w celu zapewnienia, aby ich treść odpowiadała dynamicznie rozwijającemu się środowisku bezpieczeństwa.

Świadomość, edukacja i komunikacja z klientami

Rekomendacja 12: Edukacja i komunikacja z klientami

Dostawcy usług płatniczych powinni zapewniać klientom wsparcie w odniesieniu do bezpiecznego korzystania z usług płatności internetowych. Dostawcy usług płatniczych powinni komunikować się z klientami w sposób umożliwiający im stwierdzenie autentyczności otrzymanych wiadomości.

KK 12.1 Dostawcy usług płatniczych powinni zapewniać funkcjonowanie co najmniej jednego bezpiecznego kanału[28] 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 wskazywać, że jakakolwiek wiadomość przekazana w ich imieniu innym kanałem (jak np. poczta elektroniczna) dotycząca poprawnego i bezpiecznego korzystania z usług płatności internetowych nie jest wiarygodna. Dostawcy usług płatniczych powinni wyjaśniać klientom:

- procedury raportowania dostawcom usług płatniczych (potencjalnych) transakcji oszukańczych, podejrzanych zdarzeń i nietypowych sytuacji w trakcie sesji usług płatności internetowych i / lub potencjalnych prób ataków socjotechnicznych[29];
- 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).

KK 12.2 Dostawcy usług płatniczych powinni informować klientów poprzez bezpieczny kanał o zmianach w procedurach bezpieczeństwa dotyczących usług płatności internetowych. Wszelkie powiadomienia o pojawiających się istotnych ryzykach (np. ostrzeżenia przed atakami socjotechnicznymi) również powinny być przekazywane bezpiecznym kanałem.

KK 12.3 Dostawcy usług płatniczych powinni zapewniać klientom wsparcie w zakresie wszelkich zapytań, skarg, wniosków o wsparcie oraz powiadomień o nietypowych sytuacjach

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

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

i incydentach w zakresie płatności internetowych i związanych z nimi usług, natomiast klienci powinni być odpowiednio informowani o sposobach uzyskiwania takiego wsparcia.

KK 12.4 Dostawcy usług płatniczych i – w stosownych przypadkach – systemy płatności 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 ogniowych, poprawek bezpieczeństwa);
- analizowania istotnych zagrożeń i ryzyk związanych z pobieraniem oprogramowania z internetu w przypadkach, gdy klienci nie mogą być pewni, że oprogramowanie to jest autentyczne i nie podlegało manipulacji;
- korzystania z autentycznych stron internetowych dostawców usług płatniczych.

KK 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 zidentyfikowania sytuacji, w których komunikują się oni z dostawcami usług płatniczych, a nie z odbiorcami płatności, np. poprzez przekierowywanie klientów i otwieranie osobnego okna, przez co proces płatności nie będzie widoczny w ramce (ang. frame) akceptanta.

DP 12.1 Pożądane jest, aby dostawcy usług płatniczych będący agentami rozliczeniowymi organizowali dla akceptantów programy szkoleniowe w zakresie przeciwdziałania oszustwom.

Rekomendacja 13: Powiadomienia, ustalanie limitów

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.

KK 13.1 Przed rozpoczęciem świadczenia klientom usług płatności internetowej dostawcy usług płatniczych powinni ustalić limity[30] odnoszące się do tych usług (np. maksymalną wartość poszczególnych transakcji lub łączną wartość transakcji w określonym okresie) i poinformować o tym klientów. Dostawcy usług płatniczych powinni umożliwiać klientom rezygnację z funkcjonalności płatności internetowych.

DP 13.1 W ramach ustalonych limitów dostawcy usług płatniczych mogą udostępniać klientom funkcjonalność zarządzania limitami w zakresie usług płatności internetowych w bezpiecznym i zaufanym środowisku.

DP 13.2 Dostawcy usług płatniczych mogą wdrożyć ostrzeżenia dla klientów (np. przez telefon lub SMS) o transakcjach podejrzanych lub wysokiego ryzyka, w oparciu o polityki zarządzania ryzykiem.

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

DP 13.3 Dostawcy usług płatniczych mogą umożliwić klientom określenie ogólnych, spersonalizowanych reguł jako parametrów ich zachowania w odniesieniu do płatności internetowych i związanych z nimi usług, np. dotyczących inicjowania płatności jedynie z określonych państw (w przypadku płatności inicjowanych z innych miejsc powinny być one w takim przypadku blokowane) lub dotyczące umieszczenia określonych odbiorców płatności na białych lub czarnych listach.

Rekomendacja 14: Dostęp dla klientów do informacji o statusie inicjacji i wykonania płatności

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

KK 14.1 [polecenia przelewu / polecenia zapłaty] Dostawcy usług płatniczych powinni umożliwiać klientom w niemal rzeczywistym czasie weryfikację statusu wykonania transakcji oraz salda rachunku w dowolnym momencie[31] w bezpiecznym i zaufanym środowisku.

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

Słownik pojęć:

Pojęcie	Definicja
Uwierzytelnienie	Procedura pozwalająca dostawcy usług płatniczych na potwierdzenie tożsamości klienta.
Autoryzacja	Procedura weryfikacji, czy klient lub dostawca usług płatniczych ma prawo do wykonania określonego działania, np. prawo do przelewu środków czy prawo dostępu do danych wrażliwych.
Dane logowania	Informacje – co do zasady poufne – wprowadzane przez klienta lub dostawcę usług płatniczych na potrzeby uwierzytelnienia. Dane logowania mogą oznaczać również fizyczne narzędzie zawierające te informacje (np. generator haseł jednorazowych, karta smart) czy też coś, co użytkownik pamięta lub czym jest (np. w oparciu o jego cechy biometryczne).
Istotny incydent bezpieczeństwa płatności	Incydent, który ma lub może mieć znaczący wpływ na bezpieczeństwo, integralność lub ciągłość działania systemów wykorzystywanych przez dostawcę usług płatniczych w zakresie płatności i / lub bezpieczeństwo

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

	wrażliwych danych płatniczych lub środków pieniężnych. Ocena wpływu incydentu powinna uwzględniać liczbę potencjalnie dotkniętych nim klientów, zagrożoną kwotę oraz wpływ na innych dostawców usług płatniczych lub inne infrastruktury płatnicze.
Analiza ryzyka transakcji	Ocena 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	Kartowe rozwiązanie płatnicze, w którym 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	Rozwiązania pozwalające klientom na zarejestrowanie danych związanych z jednym lub większą liczbą instrumentów płatniczych w celu dokonywania płatności u wielu akceptantów.

Załącznik: lista uczestników prac Europejskiego Forum ds. Bezpieczeństwa Płatności Detalicznych

	Członkowie
BE	Nationale Bank van België/Banque Nationale de Belgique
BG	Българска народна банка (Bulgarian National Bank)
CZ	Česká národní banka
DK	Danmarks Nationalbank Finanstilsynet
DE	Deutsche Bundesbank Bundesanstalt für Finanzdienstleistungsaufsicht
EE	Eesti Pank Finantsinspektsioon
IE	Central Bank of Ireland
GR	Bank of Greece
ES	Banco de España
FR	Banque de France Autorité de Contrôle Prudentiel
IT	Banca d'Italia
CY	Central Bank of Cyprus
LV	Latvijas Banka Finanšu un kapitāla tirgus komisija
LT	Lietuvos bankas
LU	Banque centrale du Luxembourg Commission de Surveillance du Secteur Financier
HU	Magyar Nemzeti Bank Pénzügyi Szervezetek Állami Felügyelete
MT	Central Bank of Malta
NL	De Nederlandsche Bank
AT	Oesterreichische Nationalbank Österreichische Finanzmarktaufsicht
PL	Narodowy Bank Polski Komisja Nadzoru Finansowego
PT	Banco de Portugal

RO	Banca Naţională a României
SI	Banka Slovenije
SK	Národná banka Slovenska
FI	Suomen Pankki – Finlands Bank Finanssivalvonta
SE	Sveriges Riksbank Finansinspektionen
UK	Financial Services Authority
	European Banking Authority European Central Bank
	Obserwatorzy
IS	Central Bank of Iceland Fjármálaeftirlitið
LI	Liechtensteinische Landesbank 1861 Finanzmarktaufsicht Liechtenstein
NO	Norges Bank
	Finanstilsynet – The Financial Supervisory Authority of Norway
	European Commission
	Europol

© Europejski Bank Centralny, 2013

Adres: Kaiserstrasse 29, 60311 Frankfurt am Main, Germany

Adres korespondencyjny: Postfach 16 03 19, 60066 Frankfurt am Main, Germany

Nr telefonu: +49 69 1344 0; Strona www: http://www.ecb.europa.eu; Faks: +49 69 1344 6000

Wszelkie prawa zastrzeżone. Powielanie do celów edukacyjnych i niekomercyjnych dozwolone pod warunkiem podania źródła.

ISSN 978-92-899-0866-5 (online)

Numer katalogowy UE QB-30-13-188-EN-N (online)