Komisja Nadzoru Finansowego

Rekomendacja

dotycząca bezpieczeństwa transakcji płatniczych wykonywanych w internecie przez banki, krajowe instytucje płatnicze, krajowe instytucje pieniądza elektronicznego i spółdzielcze kasy oszczędnościowo – kredytowe

Warszawa, listopad 2015 r.

Wstep

Niniejszy dokument wydany jest na podstawie art. 137 pkt 5 ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz. U. z 2015 r. poz. 128 z późn. zm.), art. 102 ust. 2 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych (Dz. U. z 2014 r., poz. 873 z późn. zm.) oraz art. 62 ust. 2 ustawy z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych (Dz. U. z 2013 r. poz. 1450 z późn. zm.).

Postanowienia Rekomendacji mają na celu ujednolicenie zakresu minimalnych wymogów dotyczących zapewnienia bezpieczeństwa płatności internetowych w związku ze świadczeniem usług płatniczych oferowanych przez banki, krajowe instytucje płatnicze, krajowe instytucje pieniądza elektronicznego i spółdzielcze kasy oszczędnościowo-kredytowe (dalej: dostawcy usług płatniczych) przez internet.

Biorąc pod uwagę rozwój technologiczny, którego efektem jest umożliwienie przez dostawców usług płatniczych zaoferowania użytkownikom usług płatniczych dostępu do usług płatniczych z wykorzystaniem elektronicznych kanałów komunikacji i zdalnego korzystania z oferowanych usług oraz szybko zachodzące na rynku płatności internetowych zmiany i związane z nimi zagrożenia dla tych płatności, w szczególności w zakresie bezpieczeństwa i ochrony danych użytkowników, KNF w Rekomendacji zawarła oczekiwania polskiego organu nadzoru wobec dostawców płatniczych świadczących na rzecz swoich klientów (tj. użytkowników w rozumieniu definicji zawartej w ustawie z dnia 19 sierpnia 2011 r. o usługach płatniczych) usługi płatnicze w internecie odnośnie adekwatnych i bezpiecznych zasad (sposobów) oferowania rozwiązań umożliwiających dokonywanie płatności internetowych (w tym także przy użyciu pieniądza elektronicznego) oraz odpowiednich mechanizmów kontrolnych w tym zakresie.

Ryzyka związane z płatnościami internetowymi były identyfikowane w ramach sprawowanego przez KNF nadzoru nad podmiotami rynku finansowego. Mając na uwadze zdefiniowane w art. 2 ustawy z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym cele nadzoru nad rynkiem finansowym, w dniu 18 listopada 2013 r. na stronie internetowej KNF zostało opublikowane „Ostrzeżenie przed dopuszczeniem pośredników do rachunku bankowego w płatnościach internetowych”[1], w związku ze zidentyfikowaną praktyką ujawniania przez klientów banków loginu i hasła podmiotom innym niż ich banki, które prowadzą ich rachunki. Poza tym ze względu na zidentyfikowaną niepokojącą tendencję wśród banków, które oferując możliwość uzyskania szybkiego produktu kredytowego pozyskiwały loginy i hasła aplikujących klientów do ich rachunków bankowych w innych bankach w celu zdalnego pobrania historii obrotów na rachunku, w dniu 14 lipca 2014 r. KNF opublikowała na swojej stronie internetowej komunikat „Ryzyko związane z podawaniem innemu bankowi danych do logowania do rachunku bankowego”[2]. W ramach podejmowanej przez KNF działalności edukacyjnej dotyczącej bezpieczeństwa finansowego w bankowości

[1] http://www.knf.gov.pl/Images/KNF_podawanie_danych_dostepu_do_rachunku_18_11_2013_tcm75-36300.pdf
[2] http://www.knf.gov.pl/Images/KNF_dane_do_logowania_tcm75-38504.pdf

elektronicznej, w dniu 21 września 2015 r. na stronie internetowej KNF opublikowane zostały „Zasady bezpieczeństwa w bankowości elektronicznej”[3].

Kwestie wskazane w niniejszej Rekomendacji są uregulowane także w „Rekomendacjach dotyczących bezpieczeństwa płatności internetowych”[4] wydanych dnia 31 stycznia 2013 r. przez Europejskie Forum ds. Bezpieczeństwa Płatności Detalicznych (SecuRePay – European Forum on the Security of Retail Payments), a obowiązujących od dnia 1 lutego 2015 r. oraz „Wytycznych końcowych w sprawie bezpieczeństwa płatności internetowych”[5] (EBA/GL/2014/12) wydanych dnia 19 grudnia 2014 r. przez Europejski Urząd Nadzoru Bankowego (dalej: EBA), a obowiązujących od dnia 1 sierpnia 2015 r. Rekomendacja nie narusza postanowień zawartych w Rekomendacjach SecuRePay i EBA/GL/2014/12, ale w niektórych obszarach potwierdza i wzmacnia ich postanowienia. Dotyczy to w szczególności zasad bezpiecznego dostępu do rachunku płatniczego przy wykorzystaniu możliwych kanałów dostępu do takiego rachunku. Jednocześnie Rekomendacja wskazuje na konieczność zasadniczego ograniczenia ryzyka wykorzystywania rachunków płatniczych do operacji fraudowych na podstawie skradzionych tożsamości klientów, wynikającego z obecnie możliwej praktyki otwierania kolejnych rachunków w kolejnych instytucjach z wykorzystaniem przelewu jako sposobu potwierdzania tożsamości. Wprowadzenie w szczegółowej Rekomendacji 6.1. (zdanie 2) wymogu, zgodnie z którym rachunek założony zdalnie z wykorzystaniem przelewu potwierdzającego tożsamość klienta nie może służyć do otwarcia tym sposobem kolejnego rachunku płatniczego u innego dostawcy usług płatniczych, nie wpłynie na model funkcjonowania instytucji płatniczych prowadzących rachunki z natury swojej nie dające możliwości dokonywania przelewów w celu otwarcia kolejnego rachunku. Ustalenie i przyjęcie skutecznych metod stosowanych w tym celu pozostawione jest instytucjom otwierającym rachunki. Z tego względu Rekomendacja ma charakter szczególny w stosunku do tych regulacji i w przypadku ewentualnych rozbieżności powinna mieć pierwszeństwo w zastosowaniu.

Poza tym Rekomendacja powinna być traktowana – w stosunku do banków – jako uzupełnienie wydanych przez KNF: „Rekomendacji D dotyczącej zarządzania obszarami technologii informacyjnej i bezpieczeństwa teleinformatycznego w bankach”[6] i „Rekomendacji M dotyczącej zarządzania ryzykiem operacyjnym w bankach”[7].

Należy zwrócić uwagę, iż wskazane oczekiwania nadzoru odnośnie bezpieczeństwa płatności internetowych nie zawierają szczegółowego katalogu sposobów i rodzajów działań, jakie powinny zostać podjęte przez dostawców usług płatniczych świadczących usługi płatnicze w internecie, co oznacza że dostawcy mogą podejmować preferowane przez siebie czynności – w ramach dozwolonych prawem rozwiązań – w celu osiągnięcia rezultatu potwierdzającego spełnienie oczekiwań nadzoru w danym obszarze.

[3] http://www.knf.gov.pl/o_nas/komunikaty/bezpieczenstwo_bankowosc_elektroniczna.html
[4] http://www.knf.gov.pl/Images/Rekomendacje_bezpieczenstwo_platnosci_internetowych_tcm75-37934.pdf
[5] http://www.eba.europa.eu/documents/10180/1004450/EBA-GL-2014-12_PL_rev1+GL+on+Internet+Payments
[6] http://www.knf.gov.pl/Images/Rekomendacja_D_8_01_13_uchwala_7_tcm75-33016.pdf
[7] http://www.knf.gov.pl/Images/Rekomendacja_M_8_01_2013_uchwala_8_tcm75-33017.pdf

Dokument zawiera 14 rekomendacji, które podzielone zostały na następujące obszary:

1) **Zasady i organizacja procesu zarządzania i oceny ryzyka**
   Dostawcy usług płatniczych powinni posiadać formalną politykę bezpieczeństwa i regularnie dokonywać szczegółowych ocen ryzyka w stosunku do płatności internetowych oraz usług powiązanych, a w razie potrzeby dokonywać niezbędnych zmian. Analizy powinny uwzględnić m.in. wykorzystywane rozwiązania technologiczne, środowisko techniczne, w jakim działa klient czy zagadnienia outsourcingu.
2) **Szczególne środki kontroli i bezpieczeństwa w zakresie płatności internetowych**
   Dostawcy usług płatniczych powinni stosować mechanizm silnego uwierzytelniania klienta zawsze, gdy klient inicjuje płatność internetową lub chce uzyskać dostęp do wrażliwych danych płatniczych. Od tej zasady można odstąpić tylko w wyjątkowych przypadkach. Dostawcy powinni udostępniać klientom bezpieczne narzędzia do autoryzacji transakcji internetowych oraz zapewnić ogólną dbałość o bezpieczeństwo całej transakcji, poprzez jasne określenie obowiązków i zakresu odpowiedzialności odpowiednio dostawcy usług płatniczych i klienta w związku z korzystaniem z usług płatności internetowych wynikających m.in. z zakazu udostępniania (ujawniania) podmiotom trzecim danych do logowania. Dostawcy powinni również stosować systemy, które pomogą zidentyfikować i zablokować oszukańcze transakcje.
3) **Świadomość i edukowanie klientów oraz komunikacja z nimi**
   Działania edukacyjne powinny się odbywać zarówno poprzez regularne akcje, jak i poprzez incydentalne ostrzeganie o zagrożeniach oraz bieżący kontakt z klientem za pomocą bezpiecznego kanału komunikacji.

Z zakresu zastosowania Rekomendacji **wyłączone** są:

1) inne niż usługi w zakresie płatności internetowych usługi internetowe świadczone przez dostawców usług płatniczych poprzez ich strony internetowe przeznaczone do dokonywania płatności (np. elektroniczne usługi maklerskie, umowy online);
2) płatności zlecane za pośrednictwem poczty tradycyjnej, polecenia telefonicznego, poczty głosowej lub przy użyciu technologii esemesowej;
3) płatności mobilne inne niż realizowane przy użyciu przeglądarki internetowej;
4) transakcje płatnicze dokonywane przez przedsiębiorstwa poprzez dedykowane sieci.

Niniejszy dokument zawiera słownik pojęć, który jednak nie wyczerpuje definicji wszystkich pojęć użytych w Rekomendacji. Z tego względu w odniesieniu do pojęć nie zdefiniowanych w Rekomendacji, zastosowanie będą miały definicje zawarte w przepisach powszechnie obowiązujących.

KNF oczekuje, że Rekomendacja, stanowiąca załącznik do uchwały Nr …./2015 Komisji Nadzoru Finansowego z dnia 17 listopada 2015 r. (Dz. Urz. KNF poz. ….), będzie stosowana począwszy od dnia następującego po dniu opublikowania jej w Dzienniku Urzędowym KNF, z wyjątkiem:

1) obowiązku, o którym mowa w Rekomendacji 6.2. tiret 2 i 7 w odniesieniu do zakazu ujawniania (udostępniania) danych logowania,

który powinien być stosowany nie później niż od dnia 21 grudnia 2015 r. oraz

2) obowiązku, o którym mowa w Rekomendacji 6.1. i
3) obowiązku w zakresie polityki edukacyjnej, o której mowa w Rekomendacji 12,

które powinny być stosowane nie później niż od dnia 1 lipca 2016 r.

Wdrożenie Rekomendacji będzie przedmiotem weryfikacji nadzorczej, w szczególności w trakcie przeprowadzanych czynności kontrolnych. Oczekuje się, że podmioty do których adresowana jest Rekomendacja, na żądanie KNF będą w stanie wyjaśnić i uzasadnić wszelkie przypadki braku zgodności stosowanej w ich działalności praktyki zarówno w odniesieniu do poszczególnych rekomendacji jak i zawartych w dokumencie dobrych praktyk.

Słownik pojęć

- **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.
- **Autoryzacja** – procedura weryfikacji pozwalającej stwierdzić, 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** – 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 element wiedzy/pamięci lub swoistą, indywidualną cechę (np. cechy biometryczne) użytkownika.
- **Karty wirtualne** – karty płatnicze istniejące wyłącznie w postaci cyfrowej, umożliwiające dokonywanie płatności w internecie.
- **Poważny incydent bezpieczeństwa płatności** – 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 pieniężnych. Oceniając istotność incydentu, należy uwzględnić liczbę klientów potencjalnie dotkniętych incydentem, zagrożoną kwotę oraz wpływ na innych dostawców usług płatniczych lub inne infrastruktury płatnicze.
- **Rozwiązania portfelowe** – rozwiązania pozwalające klientom na zarejestrowanie danych związanych z jednym lub większą liczbą instrumentów płatniczych w celu dokonywania płatności u wielu akceptantów.
- **Silne uwierzytelnienie klienta** – procedura obejmująca użycie dwóch lub więcej następujących elementów, klasyfikowanych jako: a) wiedza – coś, co jedynie użytkownik wie (element wiedzy/pamięci użytkownika np. hasło statyczne, kod PIN), b) posiadanie – coś, co jedynie użytkownik posiada (sprzęt/urządzenie będące w posiadaniu użytkownika np. token/generator kodów, karta inteligentna, telefon komórkowy) oraz c) cecha klienta (swoista indywidualna cecha charakteryzująca użytkownika, np. cecha biometryczna, taka jak odcisk palca). Ponadto wybrane elementy muszą być wzajemnie niezależne, w tym znaczeniu, że 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.
- **Uwierzytelnienie** – procedura pozwalająca dostawcom usług płatniczych na potwierdzenie tożsamości klienta.
- **Wrażliwe dane płatnicze** – dane, które w przypadku wejścia w ich posiadanie przez osoby nieuprawnione mogą być wykorzystane w celu dokonania nadużycia, w tym dane umożliwiające zainicjowanie transakcji płatniczej, dane wykorzystywane do uwierzytelnienia, dane wykorzystywane do zamawiania przez klientów instrumentów płatniczych lub narzędzi uwierzytelniających.

Wykaz użytych skrótów

GIIF – Generalny Inspektor Informacji Finansowej

GIODO – Generalny Inspektor Ochrony Danych Osobowych

KNF – Komisja Nadzoru Finansowego

NBP – Narodowy Bank Polski

UUP – Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych.

Lista Rekomendacji

I. Zasady i organizacja procesu zarządzania

Rekomendacja 1

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

Rekomendacja 2

Dostawcy usług płatniczych powinni przeprowadzać i dokumentować szczegółowe oceny ryzyka w zakresie bezpieczeństwa płatności internetowych i usług związanych z tymi płatnościami, zarówno przed wprowadzeniem usługi (usług), jak i regularnie po jej (ich) wprowadzeniu.

Rekomendacja 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 opracować i wprowadzić procedurę zgłaszania takich incydentów kierownictwu (stosownie do zakresu kompetencji wynikającego z regulacji wewnętrznych danego dostawcy usług płatniczych), a w przypadku poważnych incydentów bezpieczeństwa płatności – właściwym organom (GIIF, GIODO, KNF, NBP – stosownie do kompetencji tych organów).

Rekomendacja 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 poziomów zabezpieczenia, tak by przełamanie jednego poziomu było niwelowane przez kolejny poziom zabezpieczenia („obrona w głąb”).

Rekomendacja 5

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

II. Szczególne środki kontroli i bezpieczeństwa w zakresie płatności internetowych

Rekomendacja 6

Klienci powinni być odpowiednio identyfikowani – zgodnie z polskimi przepisami dotyczącymi przeciwdziałania praniu pieniędzy – 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.

Rekomendacja 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 Rekomendacji.

Rekomendacja 8

Dostawcy usług płatniczych powinni zapewniać, 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.

Rekomendacja 9

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

Rekomendacja 10

Dostawcy usług płatniczych powinni stosować mechanizmy monitorowania transakcji mające na celu zapobieganie nielegalnym/oszukańczym transakcjom oraz wykrywanie i blokowanie takich transakcji płatniczych przed wykonaniem przez dostawcę usługi płatności internetowej. 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.

Rekomendacja 11

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

III. Świadomość i edukowanie klientów oraz komunikacja z nimi

Rekomendacja 12

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

Rekomendacja 13

Dostawcy usług płatniczych powinni ustalić limity dla usług płatności internetowych oraz mogą udostępniać klientom mechanizmy umożliwiające dalsze ograniczanie ryzyka w ramach tych limitów. Mogą również świadczyć usługi ostrzegania i zarządzania profilem klienta.

Rekomendacja 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.

I. Zasady i organizacja procesu zarządzania i ocena ryzyka

Polityka bezpieczeństwa

1. Rekomendacja 1

Dostawcy usług płatniczych powinni 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 Rekomendacją 2.4.) oraz zatwierdzana przez zarząd lub inny właściwy organ zarządzający, stosownie do zakresu kompetencji wynikającego z regulacji wewnętrznych danego dostawcy usług płatniczych. Polityka bezpieczeństwa powinna określać cele w zakresie bezpieczeństwa i apetyt na ryzyko.

1.2. Polityka 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 wrażliwymi danymi płatniczymi z uwzględnieniem oceny, kontroli i przeciwdziałania ryzyku.

Niezależnie od powyższych Rekomendacji, KNF zachęca dostawców usług płatniczych do wdrażania dobrych praktyk, których stosowanie nie jest obowiązkowe, polegających na określeniu polityki bezpieczeństwa w odrębnym dokumencie.

Ocena ryzyka

2. Rekomendacja 2

Dostawcy usług płatniczych powinni przeprowadzać i dokumentować szczegółowe oceny ryzyka w zakresie bezpieczeństwa płatności internetowych i usług związanych z tymi płatnościami, 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 związanych z tymi płatnościami. Dostawcy usług płatniczych powinni uwzględniać rezultaty bieżącego monitorowania zagrożeń bezpieczeństwa w zakresie usług płatności internetowych, które oferują lub planują oferować, uwzględniając: a) stosowane przez siebie rozwiązania technologiczne, b) usługi zlecane dostawcom zewnętrznym oraz c) środowisko techniczne klientów. Dostawcy usług płatniczych powinni uwzględniać ryzyko związane z wybranymi platformami technologicznymi, architekturą aplikacji, technikami programistycznymi oraz procedurami, zarówno po swojej stronie, jak i po stronie klientów, a także wyniki procesu monitorowania incydentów bezpieczeństwa (Rekomendacja 3).

2.2. Na podstawie ocen, o których mowa w Rekomendacji 2.1., 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) oraz podjąć odpowiednie kroki w okresie przejściowym w celu zminimalizowania incydentów bezpieczeństwa i przypadków oszustwa/nadużyć, 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 – co najmniej raz w roku – przeprowadzony powinien być ogólny przegląd oceny ryzyka. Rezultaty oceny ryzyka i przeglądów powinny być zatwierdzane przez zarząd lub inny właściwy organ zarządzający dostawcy usług płatniczych, stosownie do zakresu kompetencji wynikającego z regulacji wewnętrznych danego dostawcy.

Monitorowanie i zgłaszanie incydentów

3. Rekomendacja 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 opracować i wprowadzić procedurę zgłaszania takich incydentów kierownictwu (stosownie do zakresu kompetencji wynikającego z regulacji wewnętrznych danego dostawcy usług płatniczych), a w przypadku poważnych incydentów bezpieczeństwa płatności – właściwym organom (GIIF, GIODO, KNF, NBP – stosownie do kompetencji tych organów).

3.1. Dostawcy usług płatniczych powinni stosować proces monitorowania, postępowania w razie wystąpienia incydentów bezpieczeństwa i działań następczych w stosunku do incydentów oraz skarg klientów związanych z bezpieczeństwem, i zgłaszać takie incydenty kierownictwu (stosownie do zakresu kompetencji wynikającego z regulacji wewnętrznych danego dostawcy).

3.2. Dostawcy usług płatniczych powinni posiadać procedurę niezwłocznego informowania GIIF, GIODO, KNF, NBP – stosownie do kompetencji tych organów – o przypadkach wystąpienia poważnych incydentów bezpieczeństwa płatności w zakresie świadczonych usług płatniczych.

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

3.4. W przypadku, gdy akceptanci przechowują, przetwarzają lub przesyłają wrażliwe dane płatnicze, które to czynności są immanentnie związane z daną usługą płatniczą, dostawcy usług płatniczych świadczący usługę acquiringu/agenci rozliczeniowi powinni zapewniać umowne uregulowanie zasad współpracy z tymi akceptantami w zakresie poważnych incydentów bezpieczeństwa płatności, w tym naruszenia danych, zarówno z dostawcami usług płatniczych, jak i właściwymi organami ścigania. Jeżeli dostawca usług płatniczych uzyska wiedzę o tym, że akceptant płatności internetowych nie współpracuje zgodnie z wymaganiami umownymi, powinien podjąć kroki mające na celu wyegzekwowanie tego zobowiązania umownego lub rozwiązać umowę.

Kontrola i przeciwdziałanie ryzyku

4. Rekomendacja 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 poziomów zabezpieczenia, tak by przełamanie jednego poziomu było niwelowane przez kolejny poziom zabezpieczenia („obrona w głąb").

4.1. Projektując i świadcząc (rozwijając/modyfikując) 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.

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 aplikacji na nadużycia i ataki. 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: a) wrażliwych danych płatniczych oraz b) 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 i świadcząc (rozwijając/modyfikując) usługi płatności internetowych, dostawcy usług płatniczych powinni zapewnić, by kluczowym elementem podstawowej

funkcjonalności była minimalizacja danych. Gromadzenie, przesyłanie, przetwarzanie, 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 audytów. Częstotliwość i tematyka audytów powinny uwzględniać i być proporcjonalne do poziomu ryzyka 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 Rekomendacji.

4.8. W przypadku, gdy akceptanci przechowują, przetwarzają lub przesyłają wrażliwe dane płatnicze, które to czynności są immanentnie związane z daną usługą płatniczą, dostawcy usług płatniczych świadczący usługi agenta rozliczeniowego zawierając umowy z takimi akceptantami powinni wymagać wdrożenia przez akceptantów środków bezpieczeństwa w ramach ich infrastruktury IT, zgodnie z Rekomendacjami 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 internetowych nie stosuje wymaganych środków bezpieczeństwa, powinien podjąć kroki mające na celu wyegzekwowanie wspomnianego zobowiązania umownego lub rozwiązać umowę.

Niezależnie od powyższych Rekomendacji, KNF zachęca dostawców usług płatniczych do wdrażania dobrych praktyk, których stosowanie nie jest obowiązkowe, polegających na zapewnieniu narzędzi bezpieczeństwa (np. odpowiednio zabezpieczonego urządzenia lub specjalnie zaprojektowanej przeglądarki internetowej) w celu ochrony interfejsu klienta przed bezprawnym wykorzystaniem lub atakami (np. atakami typu „człowiek w przeglądarce").

Śledzenie

5. Rekomendacja 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 zapewniać, 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 analizować dane dotyczące transakcji oraz poleceń zapłaty i posiadać narzędzia do oceny dzienników zdarzeń. Poszczególne aplikacje powinny być wyłącznie dostępne upoważnionym pracownikom.

Niezależnie od powyższych Rekomendacji, KNF zachęca dostawców usług płatniczych świadczących usługi agenta rozliczeniowego do wdrażania dobrych praktyk, których stosowanie nie jest obowiązkowe, polegających na zawieraniu w umowach z akceptantami przechowującymi informacje dotyczące płatności internetowych wymogów dotyczących stosowania odpowiednich procesów umożliwiających śledzenie transakcji.

II. Szczególne środki kontroli i bezpieczeństwa w zakresie płatności internetowych

Wstępna identyfikacja klienta, informacje o kliencie

6. Rekomendacja 6

Klienci powinni być odpowiednio identyfikowani – zgodnie z polskimi przepisami dotyczącymi przeciwdziałania praniu pieniędzy – 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 stosują wobec klientów odpowiednie środki bezpieczeństwa, zwłaszcza skuteczne potwierdzenie ich tożsamości przed udostępnieniem im usług płatności internetowych. Zawieranie umowy rachunku płatniczego z wykorzystaniem przelewu z innego rachunku płatniczego jako sposobu potwierdzenia tożsamości klienta dopuszczalne jest jedynie, gdy kolejne zawarcie umowy rachunku płatniczego u innego dostawcy usług płatniczych z wykorzystaniem przelewu z otwieranego rachunku dla potwierdzania tożsamości u tego dostawcy nie będzie możliwe. Dostawca usługi rachunku płatniczego zapewnia integralność procesu składania wniosku o zawarcie umowy rachunku płatniczego i złożenia dyspozycji wykonania polecenia przelewu wykorzystywanego do otwarcia rachunku płatniczego.

6.2. Dostawcy usług płatniczych powinni zapewniać, by informacje dostarczane klientom przed skorzystaniem przez nich z danej usługi szczegółowo określały kwestie związane z usługami płatności internetowych, w tym dokonywanie płatności pieniądzem elektronicznym. Powinny one, w stosownych przypadkach, uwzględniać:

- 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 (takich jak hasło, login, kod jednorazowy, hasło/kod sms) służących zapewnieniu bezpieczeństwa, mające na celu zapewnienie zachowania wysokiego poziomu ochrony danych użytkowników, w tym odnoszące się m.in. do zakazu ujawniania (udostępniania) komukolwiek spersonalizowanych danych do logowania (login i hasła) oraz ewentualnych dodatkowych informacji potwierdzających tożsamość klienta;
- szczegółowy („krok po kroku") opis procedury inicjowania i autoryzowania przez klienta transakcji płatniczej, w tym dokonywanych pieniądzem elektronicznym lub uzyskiwania informacji, w tym dotyczących zasad akceptacji i rozliczania transakcji przy użyciu pieniądza elektronicznego oraz skutków poszczególnych czynności wykonywanych przez klienta w związku z dokonywaniem transakcji płatniczych;

- 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 dostawcy usług płatniczych i klienta w zakresie korzystania z usług płatności internetowych, obejmujących m.in. zakaz ujawniania (udostępniania) przez klienta komukolwiek danych logowania.

6.3. Dostawcy usług płatniczych powinni zapewniać, aby umowa ramowa z klientem przewidywała możliwość zablokowania przez dostawcę usług płatniczych określonej transakcji lub instrumentu płatniczego ze względów bezpieczeństwa, w szczególności w przypadku posłużenia się instrumentem płatniczym przez osobę nieuprawnioną. 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 przepisami UUP.

Niezależnie od powyższych Rekomendacji, KNF zachęca dostawców usług płatniczych do wdrażania dobrych praktyk, których stosowanie nie jest obowiązkowe, polegających na:

- zapewnieniu możliwości podpisania z klientem, na jego wniosek, 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,
- przekazywaniu klientom na bieżąco, za pomocą odpowiednich środków (np. ulotek, stron internetowych) jasnych i zrozumiałych instrukcji wyjaśniających obowiązki klientów w zakresie bezpiecznego korzystania z danej usługi.

Silne uwierzytelnianie klienta

7. Rekomendacja 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 Rekomendacji.

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 przy użyciu pieniądza elektronicznego i pakietów poleceń przelewu) oraz wydawania lub modyfikacji elektronicznych poleceń zapłaty. Dostawcy usług płatniczych mogą jednak rozważyć przyjęcie alternatywnych środków uwierzytelniania klienta na potrzeby:
   - 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 przepisami UUP.

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 zostać łatwo wykorzystane do popełnienia oszustwa (takich jak dane kart płatniczych), dostawca usług płatności internetowych może dostosować swoje wymagania w zakresie uwierzytelniania na podstawie oceny ryzyka.

7.3. [karty] W zakresie transakcji kartą płatniczą wszyscy dostawcy usług płatniczych będący wydawcami kart płatniczych 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 płatniczej przeprowadzanie silnego uwierzytelniania posiadacza karty płatniczej w zakresie systemów płatności kartą płatniczą, w których uczestniczy agent rozliczeniowy.

7.5. [karty] Dostawcy usług płatniczych świadczący usługi agenta rozliczeniowego powinni wymagać od akceptantów obsługi rozwiązań umożliwiających wydawcy karty płatniczej przeprowadzanie silnego uwierzytelniania posiadacza karty płatniczej w zakresie transakcji kartą płatniczą 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 przepisami UUP.

7.6. [karty] W przypadku płatności internetowych przy użyciu karty płatniczej, dostawcy „rozwiązań portfelowych” powinni wymagać silnego uwierzytelniania przez wydawcę karty płatniczej w przypadku, gdy uprawniony posiadacz po raz pierwszy rejestruje dane tej karty.

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 płatniczą 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 przepisami UUP.

7.8. [karty] W zakresie wirtualnych kart płatniczych wstępna rejestracja powinna odbywać się w bezpiecznym i zaufanym środowisku. Silne uwierzytelnianie klienta powinno być

wymagane w procesie generowania danych takich kart w przypadku, gdy karta ta wydawana jest w środowisku internetowym.

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

Niezależnie od powyższych Rekomendacji, KNF zachęca dostawców usług płatniczych do wdrażania dobrych praktyk, których stosowanie nie jest obowiązkowe, polegających na:

- [karty] stosowaniu przez akceptantów w ramach współpracy z dostawcą usług płatniczych środków umożliwiających silne uwierzytelnienie posiadacza karty płatniczej przez wydawcę tej karty podczas dokonywania transakcji tą kartą przez internet,
- stosowaniu (w celu ułatwienia klientom korzystania z usług płatniczych) jednego narzędzia silnego uwierzytelnienia w odniesieniu do wszystkich usług płatności internetowych, co może zwiększyć poziom akceptacji rozwiązania wśród klientów i ułatwić jego właściwe stosowanie,
- stosowaniu rozwiązań obejmujących powiązanie autoryzacji z określoną kwotą lub odbiorcą płatności, co może zapewnić klientom większą pewność przy autoryzowaniu płatności, przy czym rozwiązanie techniczne umożliwiające powiązanie silnych danych uwierzytelniających z danymi transakcyjnymi powinno być odporne na manipulację.

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

8. Rekomendacja 8

Dostawcy usług płatniczych powinni zapewniać, 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 i/lub oprogramowanie związane z płatnościami oraz ich dostarczanie klientom powinno spełniać następujące wymagania:
   - Procesy 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 (danych logowania), 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 klientowi weryfikację jego autentyczności oraz sprawdzenie, czy nie było ono przedmiotem manipulacji.

– [karty] W przypadku transakcji przy użyciu karty, klient powinien mieć możliwość wyboru silnego uwierzytelniania niezależnie od konkretnego zakupu internetowego. Jeżeli oferowana jest możliwość aktywacji podczas zakupów online, aktywacja powinna się odbywać poprzez przekierowanie klienta do bezpiecznego i zaufanego środowiska.

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 przy użyciu karty.

Próby logowania, wygaszanie sesji, ważność uwierzytelniania

9. Rekomendacja 9

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

9.1. Stosując na potrzeby uwierzytelniania hasła jednorazowe, dostawcy usług płatniczych powinni zapewnić, 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. Rekomendacja 10

Dostawcy usług płatniczych powinni stosować mechanizmy monitorowania transakcji mające na celu zapobieganie nielegalnym/oszukańczym transakcjom oraz wykrywanie i blokowanie takich transakcji płatniczych przed wykonaniem przez dostawcę usługi płatności internetowej. 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 wykonaniem przez dostawcę usługi płatności internetowej. 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)

podczas sesji usług płatności internetowych, czasem identyfikowane przez sprawdzenie geolokalizacji adresu IP, 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 w odpowiednim czasie, tak aby nadmiernie nie opóźniać inicjowania i/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. Rekomendacja 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 stosowane było bezpieczne szyfrowanie typu „end-to-end”[8], 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 przechowują, przetwarzają lub przesyłają wrażliwe dane płatnicze, które to czynności są immanentnie związane z daną usługą

[8] Szyfrowanie typu „end-to-end” występuje wówczas, gdy szyfrowanie danych odbywa się w systemie źródłowym, zaś ich deszyfrowanie odbywa się wyłącznie w systemie docelowym.

płatniczą, 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.

Niezależnie od powyższych Rekomendacji, w przypadku gdy akceptanci przechowują, przetwarzają lub przesyłają wrażliwe dane płatnicze, które to czynności są immanentnie związane z daną usługą płatniczą, KNF zachęca dostawców usług płatniczych do wdrażania dobrych praktyk, których stosowanie nie jest obowiązkowe, polegających na zapewnieniu przez tych akceptantów odpowiedniego przeszkolenia swoich pracowników odpowiedzialnych za przeciwdziałanie oszustwom i regularnego aktualizowania zakresu szkoleń, tak by ich tematyka odpowiadała dynamice zmian warunków bezpieczeństwa.

III. Świadomość i edukowanie klientów oraz komunikacja z nimi

Edukowanie klientów i komunikacja z nimi

12. Rekomendacja 12

Dostawcy usług płatniczych powinni zapewniać klientom niezbędną pomoc i wsparcie w zakresie bezpiecznego korzystania z usług płatności internetowych i stosować w tym zakresie przyjętą politykę edukacyjną. 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 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 zastosowania technik manipulacji ludźmi mającymi na celu pozyskanie informacji (np. poprzez e-mail lub telefon) lub ich wyszukiwanie w sieciach społecznościowych w celu dokonania oszustwa lub uzyskania nieautoryzowanego dostępu do komputera lub sieci (ataki socjotechniczne);
- 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 istotnych 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. Klienci powinni być odpowiednio informowani o sposobach uzyskiwania takiego wsparcia.

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 przed dostępem osób nieuprawnionych, w celu ograniczenia nieakceptowalnego ryzyka naruszenia zasady nieujawniania spersonalizowanych danych do logowania;
- 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).

Niezależnie od powyższych Rekomendacji, KNF zachęca dostawców usług płatniczych świadczących usługi agenta rozliczeniowego do wdrażania dobrych praktyk, których stosowanie nie jest obowiązkowe, polegających na wprowadzaniu programów edukowania akceptantów w zakresie zapobiegania oszustwom.

Powiadomienia, ustalanie limitów

13. Rekomendacja 13

Dostawcy usług płatniczych powinni ustalić limity dla usług płatności internetowych oraz mogą udostępniać klientom mechanizmy umożliwiające dalsze ograniczanie ryzyka w ramach tych limitów. Mogą również świadczyć usługi ostrzegania i zarządzania profilem klienta.

13.1. Przed rozpoczęciem świadczenia klientom usług płatności internetowych dostawcy usług płatniczych powinni ustalić limity 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.

Niezależnie od powyższych Rekomendacji, KNF zachęca dostawców usług płatniczych do wdrażania dobrych praktyk, których stosowanie nie jest obowiązkowe, polegających na:

- zapewnieniu klientom, z zastrzeżeniem określonych limitów, możliwości zarządzania, w bezpiecznym i zaufanym środowisku, limitami odnoszącymi się do usług płatności internetowych,
- stosowaniu (kierując się własną polityką zarządzania ryzykiem) systemu ostrzegania klientów, na przykład telefonicznie lub poprzez SMS, w przypadku wystąpienia transakcji podejrzanych lub wysokiego ryzyka,

- umożliwieniu klientom określenia ogólnych, spersonalizowanych reguł jako parametrów ich zachowań w zakresie płatności internetowych i usług związanych z tymi płatnościami (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).

Dostęp klientów do informacji o statusie inicjacji i realizacji płatności

14. Rekomendacja 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 transakcji oraz salda rachunku w dowolnym momencie (z wyłączeniem wyjątkowych przypadków niedostępności tej funkcjonalności w związku z procesami technicznymi lub poważnymi incydentami) 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.

Spis treści

Wstęp……..2
Słownik pojęć…….6
Wykaz użytych skrótów…….7
Lista rekomendacji……..8
I. Zasady i organizacja procesu zarządzania i ocena ryzyka……11
II. Szczególne środki kontroli i bezpieczeństwa w zakresie płatności internetowych…..16
III. Świadomość i edukowanie klientów oraz komunikacja z nimi……23