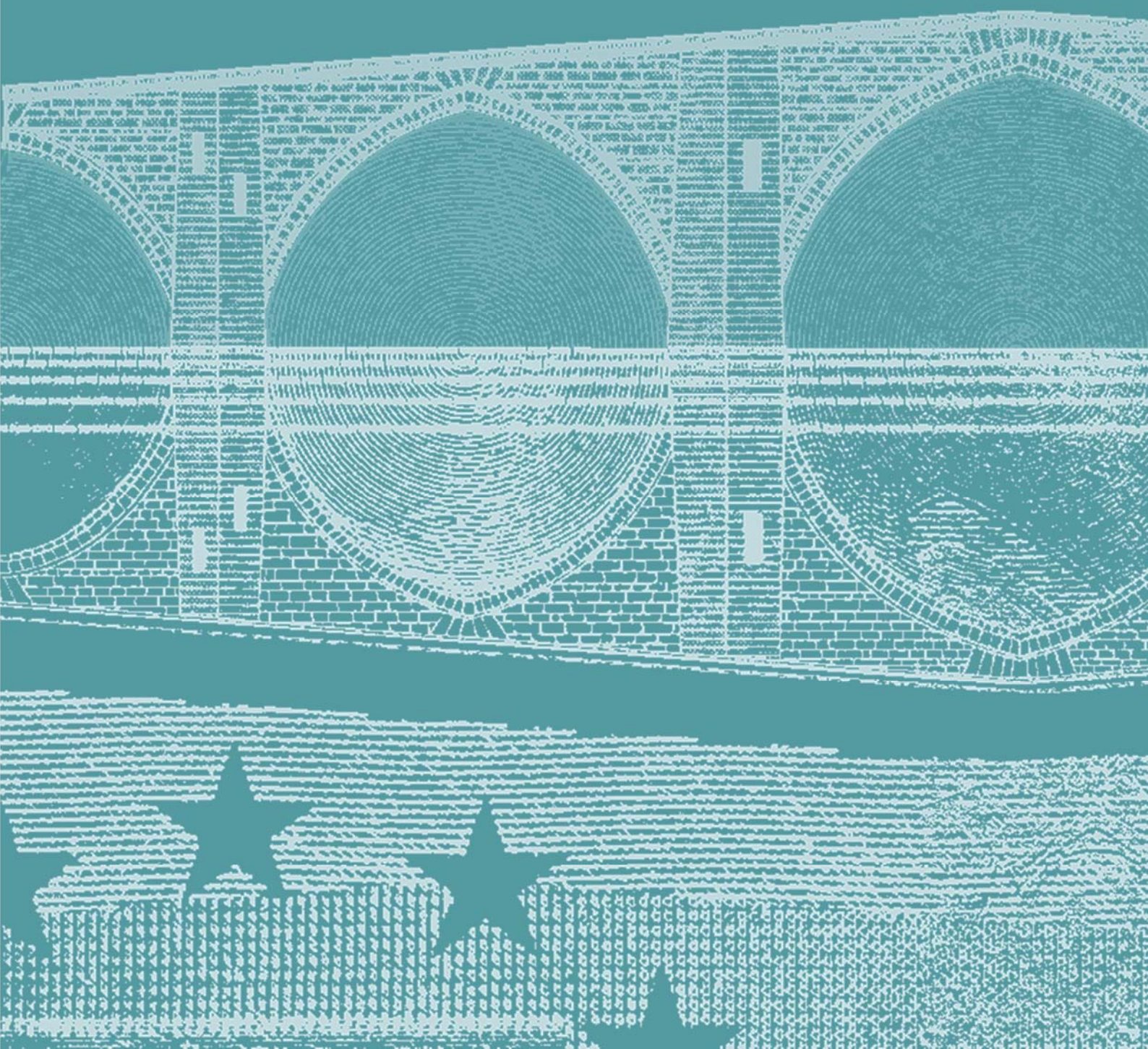
EUROPEAN CENTRAL BANK

EUROSYSTEM

WYTYCZNE W ZAKRESIE OCENY BEZPIECZEŃSTWA PŁATNOŚCI INTERNETOWYCH

LUTY 2014



EUROPEAN CENTRAL BANK

EUROSYSTEM

WYTYCZNE W ZAKRESIE OCENY BEZPIECZEŃSTWA PŁATNOŚCI INTERNETOWYCH
LUTY 2014

W 2014 r. wszystkie publikacje EBC zawierają motyw zapożyczony z banknotu 20 €.

Adres
Kaiserstrasse 29
60311 Frankfurt n. Menem
Niemcy

Adres korespondencyjny
Postfach 16 03 19
60066 Frankfurt n. Menem
Niemcy

Numer telefonu
+49 69 1344 0

Strona internetowa
http://www.ecb.europa.eu

Faks
+49 69 1344 6000

ISBN: 978-92-899-1159-7 (online)
Numer katalogowy UE: QB-04-14-051-EN-N (online)

SPIS TREŚCI

1 WPROWADZENIE

Niniejsze wytyczne oceny zostały opracowane przez Europejskie Forum ds. Bezpieczeństwa Płatności Detalicznych (SecuRe Pay, dalej „Forum“) na podstawie ostatecznej wersji „Rekomendacji dotyczących bezpieczeństwa płatności internetowych“ (dalej „Rekomendacje“) opublikowanych na stronie internetowej EBC 31 stycznia 2013 r.

Wytyczne te przeznaczone są dla członków organów nadzoru i nadzoru systemowego państw członkowskich, którzy odpowiadają za ocenę zgodności z rekomendacjami dotyczącymi płatności internetowych w swoim kraju, i mają zapewnić, aby oceny były zharmonizowane i efektywne na całym obszarze UE/EOG. Ułatwi to organom nadzoru porównywanie i/lub gromadzenie ustaleń z różnych państw członkowskich bez wpływu na kontrole nadzorcze prowadzone zgodnie z ich obowiązkami. Podążając ogólną ścieżką określoną w niniejszych wytycznych, pracownicy organów nadzoru będą wykonywać profesjonalną ocenę, uwzględniając określone cechy w określonym, badanym kontekście, w tym możliwą adaptację i integrację wszelkich wymaganych pytań, punktów kontrolnych lub dokumentacji potwierdzającej/referencyjnej. W celu ułatwienia tych czynności na stronach EBC opublikowane zostaną niniejsze wytyczne.

W założeniu rekomendacje mają przyczynić się do zwalczania nadużyć płatniczych i zapobiegania im, a tym samym zwiększyć zaufanie konsumentów do płatności internetowych. Zostały one sformułowane w możliwie ogólny sposób, aby uwzględnić stały postęp technologiczny. Forum ma świadomość, że w każdej chwili mogą powstać nowe zagrożenia i w związku z tym rekomendacje oraz niniejsze wytyczne będą podlegać okresowym przeglądom. Pewne wytyczne zawarte w niniejszym dokumencie mogą potencjalnie ulec zmianom w wyniku przeglądu dyrektywy ws. usług płatniczych, kiedy uzyska poparcie Parlamentu Europejskiego.

Rekomendacje nie mają na celu wskazania konkretnych rozwiązań w zakresie bezpieczeństwa czy rozwiązań technicznych, nie redefiniują ani nie sugerują zmian do standardów technicznych obowiązujących w branży czy oczekiwań organów w zakresie ochrony danych i ciągłości działania. Oceniając przestrzeganie rekomendacji dotyczących bezpieczeństwa, organy mogą uwzględnić zgodność z odpowiednimi standardami międzynarodowymi. Jeśli rekomendacje wskazują konkretne rozwiązania, należy pamiętać, że takie same rezultaty można osiągnąć za pomocą innych środków. Można zatem powiedzieć, że rekomendacje określają minimalne oczekiwania. Pozostają one bez wpływu na odpowiedzialność dostawców usług płatniczych, podmiotów zarządzających schematami płatniczymi oraz innych uczestników rynku za monitorowanie i ocenę ryzyka związanego z realizowanymi przez nich operacjami płatniczymi, opracowywanie własnych, szczegółowych polityk bezpieczeństwa i wdrażanie odpowiednich środków w zakresie bezpieczeństwa, planowania awaryjnego, zarządzania incydentami oraz ciągłości działania współmiernych do ryzyka związanego ze świadczonymi usługami płatniczymi.

Rekomendacje zawierają kluczowe zagadnienia (KZ) i dobre praktyki (DP), które bardziej szczegółowo określają treść każdej rekomendacji. Niniejsze wytyczne wyszczególnia pytania oceniające dla każdej kluczowego zagadnienia i dobrej praktyki, a jeśli jest to niezbędne, uzupełnia je ilustracyjnymi punktami kontrolnymi, które mają stanowić dalsze wskazówki do zapewnienia, aby na pytanie została udzielona wystarczająco szczegółowa odpowiedź i aby zostało ono zinterpretowane w sposób spójny. Ponadto przedstawiono przykłady potencjalnie istotnych dokumentów potwierdzających (przy czym ich lista nie jest wyczerpująca), z których można skorzystać, aby zyskać wystarczającą pewność podczas oceny zgodności z rekomendacjami.

Pytania oceniające mają pomóc w zapewnieniu zharmonizowanej interpretacji poszczególnych rekomendacji, nie należy jednak uznawać ich formy za obowiązkową. Inne opcje mogą być równie dobre do uzyskania akceptowalnego poziomu zgodności dla każdej rekomendacji. Wytyczne oceny opisują sytuacje ogólne, zatem nie zawsze wszystkie przedstawione w nich aspekty muszą być istotne dla wszystkich dostawców usług płatniczych i podmiotów zarządzających schematami płatniczymi. Powyższe należy mieć na uwadze w trakcie całego procesu oceny.

ZAKRES I ADRESACI

O ile nie wskazano inaczej, rekomendacje oraz opisy kluczowych zagadnień i dobrych praktyk zawarte w niniejszym dokumencie mają zastosowanie do wszystkich dostawców usług płatniczych – zgodnie z definicją zawartą w dyrektywie ws. usług płatniczych[1] – świadczących usługi płatności internetowych, jak również do podmiotów zarządzających schematami płatniczymi[2] (w tym systemami płatności kartowych, systemami przelewów, systemami poleceń zapłaty itp.). Celem niniejszych rekomendacji 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[3] 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 istotnych schematów płatniczych. 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[4]:

– 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;
– płatności mobilne inne niż realizowane przy użyciu przeglądarki internetowej[5];
– 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;
– rozrachunek i rozliczanie transakcji płatniczych.

---

1 Dyrektywa Parlamentu Europejskiego i Rady 2007/64/WE z dnia 13 listopada 2007 r. w sprawie usług płatniczych w ramach rynku wewnętrznego zmieniająca dyrektywy 97/7/WE, 2002/65/WE, 2005/60/WE i 2006/48/WE i uchylająca dyrektywę 97/5/WE, Dz. U. L 319 z dnia 05.12.2007 r., s. 1.

2 Podmiot zarządzający schematem płatniczym 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. Patrz: Europejski Bank Centralny, luty 2009, *Harmonised oversight approach and oversight standards for payment instruments*.

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

4 Niektóre z tych elementów mogą stać się przedmiotem odrębnego raportu na późniejszym etapie.

5 Szczegółowe rekomendacje dotyczące publikowania i utrzymywania aplikacji będą przedmiotem rekomendacji w zakresie płatności mobilnych.

GŁÓWNE DEFINICJE

Inicjacja płatności internetowych oraz dostęp do wrażliwych danych dotyczących płatności powinny być 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[6]. Obejmują one: (i) dane umożliwiające zainicjowanie zlecenia płatniczego, (ii) dane wykorzystywane do uwierzytelniania, (iii) dane wykorzystywane do zamawiania przez klientów instrumentów płatniczych lub narzędzi uwierzytelniających, jak również (iv) 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.

Poniżej przedstawiona została przykładowa lista elementów, które – w zależności od okoliczności, w jakich używane są dane – mogłyby zostać uznane za wrażliwe dane dotyczące płatności. Zgodnie z rekomendacjami, podmiot podlegający nadzorowi powinien przekazać organowi nadzoru listę tych elementów, które uznaje on za dane wrażliwe dotyczące płatności. Na tej podstawie organ nadzoru decyduje o ich wrażliwości dla każdego przypadku osobno, uwzględniając odpowiedni model biznesowy:

a) dane umożliwiające zainicjowanie zlecenia płatniczego, np.:
   - identyfikatory rachunku płatniczego klienta przechowywane przez dostawcę usług płatniczych (IBAN[7] lub jego odpowiednik); kodu BIC nie należy uznawać za daną wrażliwą;
   - dane karty płatniczej (numer rachunku podstawowego, data wygaśnięcia, kod CVx2);

b) dane wykorzystywane do uwierzytelniania (o ile ma to zastosowanie i jest używane w tym kontekście), takie jak:
   - identyfikator klienta (np. numer klienta/login);
   - hasła, kody, osobiste numery identyfikacyjne (numery PIN), pytania pomocnicze, hasła/kody resetujące;
   - numer telefonu (komórkowego lub stacjonarnego, jeżeli zastosowane);
   - certyfikaty;

c) dane wykorzystywane do zamawiania instrumentów płatniczych lub narzędzi uwierzytelniających, które mają być wysłane klientom (jeżeli funkcjonalność ta jest oferowana online w przypadku dostawców usług płatniczych, w przeciwnym razie danych tych nie uznaje się za wrażliwe), np.:
   - adres korespondencyjny klienta;
   - numer telefonu, adres e-mail;

d) dane, parametry i oprogramowanie przechowywane w systemach dostawców usług płatniczych, które w przypadku ich modyfikacji mogą obniżyć bezpieczeństwo dostarczenia instrumentów płatniczych lub narzędzi uwierzytelniających do klienta lub mogą wpłynąć na zdolność klienta do zweryfikowania transakcji płatniczej, autoryzowania poleceń przelewu lub kontroli rachunków, np.:
   - „czarne" i „białe" listy, limity określone przez klienta itp.;
   - dane, o których mowa w punktach a), b) i c), w zależności od zastosowania i używanych metod.

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, 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 zreplikowania (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.

Dalsze wytyczne w zakresie silnego uwierzytelniania można znaleźć w rekomendacji 7. 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.

---

[6] Być może dostawca usług płatniczych / podmiot zarządzający systemem płatności będzie musiał zastosować szerszą definicję w celu stosowania się do innych wymogów, takich jak przepisy prawa z zakresu ochrony danych osobowych lub prywatności.

[7] O ile zostanie to potwierdzone przez Radę Płatności Detalicznych w Euro (Euro Retail Payments Board).

IMPLEMENTACJA

Jak stwierdzono w rekomendacjach, od adresatów oczekuje się, że będą przestrzegać zarówno samych rekomendacji, jak również kluczowych kwestii, bądź będą w stanie wyjaśnić i uzasadnić wszelkie odstępstwa od nich na wniosek właściwych władz (zasada „comply or explain"). Ponadto dostawcy usług płatniczych, podmioty zarządzające systemami płatności i odpowiedni uczestnicy rynku zachęcani są do stosowania dobrych praktyk.

W celu wykazania stosowania się do rekomendacji należy odpowiedzieć na pytania oceniające (wskazane w niniejszych wytycznych). W momencie zapoczątkowania oceny przez odpowiedni organ dostawca usług płatniczych / podmiot zarządzający systemem płatności powinien przekazać wszystkie odpowiedzi oraz dokumentację potwierdzającą w formie elektronicznej, o ile to tylko możliwe. Umowy można przedłożyć w formie skanów, które muszą zawierać strony z datami i podpisami. Informacje właściwe dla danego podmiotu lub spersonalizowane, takie jak dokładna wartość uzgodnionej opłaty lub dane osobowe, można zamazać.

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.

1.1 KK 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.

1.1.1 Czy dostawca usług płatniczych / podmiot zarządzający systemem płatności posiada formalną politykę bezpieczeństwa dotyczącą internetowych usług płatniczych (np. w ramach szerszej polityki bezpieczeństwa informacji podmiotu lub polityki dotyczącej bezpieczeństwa systemów i usług informatycznych)?

- Dostawca usług płatniczych / podmiot zarządzający systemem płatności posiada politykę bezpieczeństwa dotyczącą istotnych obszarów usług płatności internetowych (np. zarządzanie bezpieczeństwem, ochrona danych lub urządzeń wrażliwych, inicjacja i obsługa transakcji oraz outsourcing).
- Polityka bezpieczeństwa określa co najmniej następujące elementy:
  a) *cele i organizację bezpieczeństwa informacji;*
  b) *zasady bezpiecznego używania informacji i zasobów teleinformatycznych i zarządzania nimi;*
  c) *role i obowiązki, działania i procesy w zakresie bezpieczeństwa;*
  d) *bezpieczeństwo zasobów ludzkich;*
  e) *środki kontroli bezpieczeństwa fizycznego/logicznego;*
  f) *ustalenia w zakresie bezpieczeństwa informacji/usług podlegających outsourcingowi;*
  g) *polityka bezpieczeństwa jest udokumentowana oraz istnieje procedura zaznajamiania odpowiednich stron o polityce i procedurach bezpieczeństwa.*
- W odniesieniu do działów polityki bezpieczeństwa podmiotów zarządzających systemami płatności, które dotyczą wszystkich uczestników systemu płatności, podmiot zarządzający posiada określone regulacje i/lub uzgodnienia umowne, które:
  a) *zobowiązują wszystkich uczestników systemu płatności do przestrzegania polityki bezpieczeństwa podmiotu zarządzającego (np. regulamin i przepisy systemu);*
  b) *pozwalają podmiotowi zarządzającemu na sprawdzanie, czy uczestnicy systemu działają zgodnie z polityką (np. oceny, inspekcje na miejscu itp.), a w przypadku braku jej przestrzegania uprawniają go do przywrócenia zgodności (np. plan działania, sankcje i kary, uchylenie licencji).*

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Polityka bezpieczeństwa

1.1.2 Czy polityka określa cele bezpieczeństwa i apetyt na ryzyko w odniesieniu do usług płatności internetowych?

- Polityka bezpieczeństwa dostawcy usług płatniczych / podmiotu zarządzającego systemem płatności określa cele dotyczące usług płatności internetowych.
- Cele bezpieczeństwa są określone na podstawie apetytu na ryzyko dostawcy usług płatniczych / podmiotu zarządzającego systemem płatności wynikającego z jego zdolności do przyjęcia danej straty (np. straty finansowej, utraty reputacji) i predyspozycji do podejmowania ryzyka (ostrożne lub agresywne podejście do ryzyka).

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Polityka bezpieczeństwa

1.1.3 Czy polityka bezpieczeństwa została zatwierdzona przez zarząd lub odpowiadający mu organ zarządzający,

zakomunikowana i udostępniona wszystkim właściwym pracownikom i osobom z zewnątrz na zasadzie dostępu na poziomie niezbędnego minimum?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Zapisy decyzji zarządu (np. okólniki)

1.1.4 Czy dostawca usług płatniczych / podmiot zarządzający systemem płatności udokumentował kryteria aktualizacji polityki? Czy kryteria te zapewniają regularne przeglądy i aktualizacje polityki ?

- Przegląd polityki bezpieczeństwa jest przeprowadzany co najmniej raz w roku na podstawie sformalizowanej i dobrze udokumentowanej procedury, która wyraźnie określa:
  a) *częstotliwość i kryteria jej uruchomienia (np. istotne zmiany w wynikach oceny ryzyka, modelach biznesowych lub przyjętej technologii), rolę i obowiązki podmiotów uczestniczących w procedurze oraz harmonogram jej wykonania;*
  b) *dane wyjściowe na potrzeby przeglądu (np. wyniki oceny ryzyka, wyniki audytu, obowiązujące szacunki i status działań naprawczych, zalecenia organów władzy, wszelkie zmiany, które mogą wpłynąć na usługi płatności internetowych itp.);*
  c) *formę wyników przeglądu (np. plan działań w zakresie ryzyka, potrzeby w zakresie zasobów itp.).*
- Wyniki przeglądu są wyraźnie udokumentowane, a ewidencja jest przechowywana.

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Sprawozdanie z oceny ryzyka

1.2 KK Polityka bezpieczeństwa powinna określać role i zakresy odpowiedzialności, w tym funkcję zarządzania 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 ograniczania ryzyka.

1.2.1 Czy polityka bezpieczeństwa wyraźnie określa wszystkie role i zakresy odpowiedzialności związane z bezpieczeństwem usług płatności internetowych?

- Polityka bezpieczeństwa przypisuje określone role i zakresy odpowiedzialności dotyczące bezpieczeństwa informacji w całej organizacji.
- Role i zakresy odpowiedzialności pracowników, wykonawców i dostawców zewnętrznych w zakresie bezpieczeństwa są określone i udokumentowane zgodnie z obowiązującą w organizacji polityką bezpieczeństwa informacji.
- Role i zakresy odpowiedzialności w zakresie bezpieczeństwa obejmują wymóg:
  a) *wdrożenia polityki bezpieczeństwa i działania zgodnie z tą polityką;*
  b) *ochrony aktywów przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub ingerencją;*
  c) *wykonywania określonych procesów lub czynności w zakresie bezpieczeństwa;*
  d) *zapewnienia, aby odpowiedzialność za działania, które mają zostać podjęte, przypisana była do konkretnej osoby;*
  e) *zgłaszania organizacji faktycznych lub potencjalnych zdarzeń w dziedzinie bezpieczeństwa lub innych ryzyk związanych z bezpieczeństwem;*
  f) *monitorowania rozwoju w dziedzinie technologii i bezpieczeństwa (np. poprzez uczestnictwo w specjalnych forach poświęconych bezpieczeństwu czy stowarzyszeniach zawodowych) oraz przeglądu polityki bezpieczeństwa pod tym kątem.*
- Kierownictwo zapewnia, aby wszyscy pracownicy, którym przypisano odpowiednie zakresy odpowiedzialności określone w polityce bezpieczeństwa, mieli odpowiednie kompetencje do wykonywania wymaganych od nich zadań.

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Polityka bezpieczeństwa, opisy stanowisk pracy i przykładowe CV

1.2.2 Czy te role i zakresy odpowiedzialności obejmują funkcję zarządzania ryzykiem[8]? Czy istnieje bezpośrednia zależność służbowa pomiędzy osobami odpowiedzialnymi za zarządzanie ryzykiem a zarządem?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Polityka bezpieczeństwa

1.2.3 Czy polityka określa wyraźną hierarchię służbową w zakresie usług płatności internetowych?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Polityka bezpieczeństwa

1.2.4 Czy polityka bezpieczeństwa obejmuje postanowienia dotyczące określonych ról i zakresów odpowiedzialności, działań z zakresu oceny, kontroli i minimalizowania ryzyka w zakresie zarządzania wrażliwymi danymi dotyczącymi płatności?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Polityka bezpieczeństwa

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

1.1.1 DP Czy polityka bezpieczeństwa usług płatności internetowych jest opracowana w formie dedykowanego dokumentu? Jeśli nie, czy istnieją łatwe do ustalenia przepisy mające zastosowanie do usług płatności internetowych?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Polityka bezpieczeństwa

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.

2.1 KK 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[9], jak i po stronie klientów[10], a także wyniki procesu monitorowania incydentów dotyczących bezpieczeństwa (patrz: rekomendacja 3).

2.1.1 Czy dostawca usług płatniczych / podmiot zarządzający systemem płatności przeprowadził i udokumentował szczegółową ocenę ryzyka w zakresie płatności internetowych i usług powiązanych, uwzględniając profile ryzyka aktorów uczestniczących w świadczeniu usług (na przykład na podstawie metodologii zarządzania ryzykiem, które są aktualne i uznawane w branży, takich jak te opracowane przez ISO, Project Management Institute i National Institute of Standards)?

---

8 Tj. skoordynowane działania mające na celu kierowanie organizacją i jej kontrolowanie w zakresie ryzyka; zazwyczaj funkcja ta obejmuje ocenę ryzyka, postępowanie z ryzykiem, akceptację ryzyka i komunikację ryzyka.

9 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.

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

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Sprawozdanie z oceny ryzyka / audytu i metodologia oceny ryzyka

2.1.2 Czy ocena ryzyka obejmuje wszystkie potencjalne obszary odpowiedzialności dostawcy usług płatniczych / podmiotu zarządzającego systemem płatności (np. obszar organizacyjny, osobowy, infrastrukturalny i techniczny), potencjalne zagrożenia bezpieczeństwa (wewnętrzne i zewnętrzne) oraz ich wagę (oddziaływanie i prawdopodobieństwo), istniejące lub potencjalne zabezpieczenia (np. środki kontroli i zabezpieczenia technicznego), luki i ryzyko rezydualne?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Sprawozdanie z oceny ryzyka

2.1.3 Czy ocena ryzyka uwzględnia:

- *(po stronie dostawcy usług płatniczych / podmiotu zarządzającego systemem płatności) usługi zlecane wykonawcom zewnętrznym, jak również wyniki monitorowania incydentów w zakresie bezpieczeństwa;*

- *(po stronie dostawcy usług płatniczych / podmiotu zarządzającego systemem płatności i po stronie jego klientów) używane rozwiązania technologiczne i platformy, architekturę aplikacji, techniki programowania i przebieg pracy w zakresie programowania?*

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Sprawozdanie z oceny ryzyka / audytu i metodologia oceny ryzyka

2.1.4 Czy umowy z wykonawcami zewnętrznymi dotyczące zlecanych usług (np. działania urządzeń akceptujących, urządzeń w ramach sieci komunikacyjnej, pozyskiwanie transakcji) obejmują postanowienia, które:

- *wymagają od tych wykonawców zewnętrznych wykonywania oceny ryzyka, podejmowania odpowiednich działań i zgłaszania wyników obu tych procesów podmiotowi zlecającemu;*

- *umożliwiają podmiotowi zlecającemu sprawdzenie – w razie potrzeby w drodze inspekcji na miejscu – skutecznego wprowadzenia w życie oceny ryzyka i powiązanych z nią podjętych działań?*

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Sprawozdanie z oceny ryzyka i umowy

2.2 KK 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 w zakresie bezpieczeństwa i przypadków nadużyć, jak również potencjalnych efektów zakłócających działalność.

2.2.1 Czy dostawca usług płatniczych / podmiot zarządzający systemem płatności posiada procedurę oceny i określania na jej podstawie niezbędnych zmian w istniejących środkach bezpieczeństwa, wykorzystywanych technologiach i wdrożonych procedurach lub oferowanych usługach w oparciu o ocenę ryzyka, w tym wszelkie niezbędne adaptacje samej metodologii oceny ryzyka?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Polityka oceny ryzyka i zarządzania zmianą

2.2.2 Czy ocena zmian prowadzi do sporządzenia formalnego planu wdrożeniowego, w tym w razie potrzeby środków przejściowych, z określonymi kamieniami milowymi, procedurami i środkami awaryjnymi mającymi na celu ułatwienie zmiany usługi, wyeliminowanie wprowadzenia nowych luk w usługach i

zminimalizowania potencjalnych incydentów związanych z dostępnością?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Polityka zarządzania zmianą i plan wdrożeniowy

2.2.3 Czy dostawca usług płatniczych / podmiot zarządzający systemem płatności posiada procedurę monitorowania wdrażania planowanych zmian, która doprowadziła do podjęcia odpowiednich działań?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Polityka oceny ryzyka i zarządzania zmianą

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

2.3.1 Czy dostawca usług płatniczych posiada odpowiednie procedury w zakresie identyfikacji wrażliwych danych płatniczych? Czy obejmują one działania operacyjne związane z ochroną wrażliwych danych płatniczych i określone środki kontroli dotyczące zarządzania nimi?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Sprawozdanie z oceny ryzyka

2.3.2 Czy ocena ryzyka uwzględnia wymogi w zakresie ochrony wrażliwych danych płatniczych (np. szyfrowanie), jak również definicji i wdrożenia polityki dostępu w zakresie wrażliwych działań operacyjnych i danych, których te działania dotyczą?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Sprawozdanie z oceny ryzyka

2.4 KK 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.

2.4.1 Czy dostawca usług płatniczych / podmiot zarządzający systemem płatności dokonuje przeglądów scenariuszy ryzyka, aktualizując odpowiednie wyniki oceny ryzyka, po wystąpieniu istotnych incydentów mających wpływ na ich usługi, a w przypadku istotnych zmian – na ich infrastrukturę lub istotne procedury operacyjne? Czy dostawca usług płatniczych / podmiot zarządzający systemem płatności odpowiednio zdefiniował istotne incydenty i istotne zmiany?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Metodologia oceny ryzyka

2.4.2 Czy dostawca usług płatniczych / podmiot zarządzający systemem płatności, w ramach monitorowania ryzyka, monitoruje zdarzenia i tendencje istotne dla funkcjonowania i bezpieczeństwa usługi płatniczej, w szczególności w stosunku do technologicznych luk bezpieczeństwa i nowych technik oszustwa? Czy nowe zagrożenia, które mogły zostać zidentyfikowane za pomocą monitorowania ryzyka przez dostawcę usług płatniczych / podmiot zarządzający systemem płatności, uruchamiają przegląd scenariuszy ryzyka zgodnie z punktem 2.4.1?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Metodologia oceny ryzyka

2.4.3 Czy dostawca usług płatniczych / podmiot zarządzający systemem płatności wykonuje okresowe przeglądy ogólne oceny ryzyka – co najmniej raz w roku? Czy zapewnia, aby metoda tworzenia oceny ryzyka była zestandaryzowana i możliwa do odtworzenia? Czy wyniki oceny ryzyka są przekazywane do zatwierdzenia przez wyższą kadrę kierowniczą?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Metodologia oceny ryzyka

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 dotyczących bezpieczeństwa dotyczących płatności – organów nadzorczych.

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

3.1.1 Czy dostawca usług płatniczych posiada procedurę monitorowania, obsługi i działań następczych w stosunku do incydentów bezpieczeństwa?

- *Procedura ta obejmuje klasyfikację incydentów w zakresie bezpieczeństwa zgodnie z ich stopniem krytyczności.*
- *Czy procedury monitorowania korzystają z aktualnych informacji np. o statusie systemów, komponentów, funkcji operacyjnych i procedur administracyjnych i technicznych w stosunku do incydentów dotyczących bezpieczeństwa fizycznego i bezpieczeństwa informacji? Czy są one w stanie zidentyfikować wczesne ostrzeżenia o potencjalnych incydentach poprzez wykrywanie zdarzeń nietypowych?*

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Polityka zarządzania incydentami

3.1.2 Czy dostawca usług płatniczych posiada procedurę informowania podmiotu zarządzającego danym systemem o istotnych incydentach w zakresie bezpieczeństwa?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Polityka zarządzania incydentami

3.1.3 Czy dostawca usług płatniczych posiada procedurę monitorowania, obsługi i działań następczych w stosunku do skarg klientów związanych z bezpieczeństwem?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Polityka zarządzania skargami

3.1.4 Czy działania następcze w stosunku do incydentów w zakresie bezpieczeństwa i skarg klientów związanych z bezpieczeństwem uwzględniają proces ewaluacji, zgłaszania zarządowi i wyciągania wniosków z tych incydentów/skarg, uwzględniając je w polityce bezpieczeństwa i zarządzania incydentami dostawcy usług płatniczych / podmiotu zarządzającego systemem płatniczym?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Polityka zarządzania incydentami i skargami

3.2 KK 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 dotyczących bezpieczeństwa płatności w zakresie świadczonych usług płatniczych.

3.2.1 Czy dostawca usług płatniczych / podmiot zarządzający systemem płatności posiada procedurę niezwłocznego informowania właściwych organów o istotnych incydentach dotyczących bezpieczeństwa płatności w zakresie świadczonych usług płatniczych?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Polityka zgodności z przepisami / obsługi incydentów i zarządzania

3.2.2 Czy dostawca usług płatniczych / podmiot zarządzający systemem płatności określił, kto odpowiada za aktualizację odpowiednich umów, w jaki sposób bezpiecznie przekazywane są informacje w tym zakresie i w jaki sposób zapewnia się aktualizację takich umów?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Polityka zgodności z przepisami / obsługi incydentów i zarządzania

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

3.3.1 Czy dostawca usług płatniczych / podmiot zarządzający systemem płatności posiada procedurę współpracy z właściwymi organami ścigania w zakresie istotnych incydentów dotyczących bezpieczeństwa płatności, w tym naruszenia danych?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Polityka zarządzania incydentami

3.3.2 Czy dostawca usług płatniczych / podmiot zarządzający systemem płatności określił, kto odpowiada za aktualizację odpowiednich umów, w jaki sposób bezpiecznie przekazywane są informacje w tym zakresie i w jaki sposób zapewnia się aktualizację takich umów?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Polityka zarządzania incydentami

3.4 KK Dostawcy usług płatniczych będący agentami rozliczeniowymi powinni wymagać od akceptantów przechowujących, przetwarzających lub przesyłających wrażliwe dane płatnicze, aby współpracowali w zakresie istotnych incydentów dotyczących 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.

3.4.1 Czy dostawca usług płatniczych będący agentem rozliczeniowym wymaga na podstawie umowy od akceptanta przechowującego, przetwarzającego lub przesyłającego wrażliwe dane płatnicze współpracy z nim i z właściwymi organami ścigania w zakresie istotnych incydentów dotyczących bezpieczeństwa i wszystkich naruszeń danych?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Umowa z akceptantem

3.4.2 Czy dostawca usług płatniczych będący agentem rozliczeniowym ustanowił procedurę egzekwowania zobowiązań umownych od akceptanta, w przypadku gdy dostawca usług płatniczych dowiaduje się, że akceptant nie współpracuje zgodnie z wymogami umowy?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Listy intencyjne

3.4.3 Czy dostawca usług płatniczych będący agentem rozliczeniowym uwzględnił w postanowieniach dotyczących rozwiązania umowy z danym akceptantem przyczynę „braku współpracy dotyczącej istotnych incydentów bezpieczeństwa płatności“?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Umowa z akceptantem

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.

4.1 KK 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[11] jako podstawy poprawnego zarządzania tożsamością i dostępem.

4.1.1 Czy zapewniono, aby środowiska informatyczne (np. środowiska rozwojowe, testowe i produkcyjne) były odpowiednio rozdzielone zarówno pod względem organizacyjnym, jak i technicznym? W odniesieniu do rozdzielenia środowisk można rozważyć następującą, niewyczerpującą listę zagadnień:

- zasady przenoszenia oprogramowania z fazy rozwojowej do produkcji powinny być określone i udokumentowane;
- oprogramowanie w trakcie fazy rozwojowej, oprogramowanie w trakcie testowania i kod produkcyjny powinny być izolowane od siebie w ramach różnych środowisk pozwalających na odpowiednią separację;
- w środowisku produkcyjnym powinien znajdować się tylko kod wykonywalny; kompilatory, edytory oraz inne narzędzia programistyczne i systemowe nie powinny być dostępne z poziomu systemów produkcyjnych, kiedy nie są potrzebne;
- środowisko testowe powinno zapewniać emulację (faktycznego) środowiska systemu produkcyjnego w najbliższy możliwy sposób;
- użytkownicy powinni używać różnych profili użytkownika do systemu produkcyjnego i testowego, a menu powinny wyświetlać odpowiednie komunikaty identyfikujące system, aby zminimalizować ryzyko błędu;
- należy unikać przenoszenia wrażliwych danych płatniczych do środowiska rozwojowego i testowego lub – jeśli jest to niezbędne – należy na to pozwalać jedynie tymczasowo i z zastrzeżeniem stosowania określonych środków kontroli.

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Polityka bezpieczeństwa, zasady funkcjonowania usługi, specyfikacje zastosowania, specyfikacja rozwiązań architektury i sprawozdania z audytów

4.1.2 Czy zapewniono, aby zarządzanie tożsamością i dostępem było zgodne z zasadą minimalnych uprawnień?

W odniesieniu do uprawnień użytkowników można rozważyć następującą, niewyczerpującą listę zagadnień:

- uprawnienia dostępu (w tym administrator, super user / root, administrator bazy danych itp.) związane z każdym produktem systemu (np. systemem operacyjnym, systemem zarządzania bazami danych i każdą aplikacją) oraz użytkownicy, którym te uprawnienia powinny zostać nadane, powinni być identyfikowani i podlegać regularnej weryfikacji;

[11] „Każdy program i każdy uprawniony użytkownik systemu powinien działać z wykorzystaniem najmniejszej ilości uprawnień niezbędnych do wykonania danego działania.“ Patrz: Saltzer J. H., 1974, *Protection and the Control of Information Sharing in Multics*, *Communications of the ACM,* t. 17, nr 7, str. 388.

- uprawnienia powinny być nadawane użytkownikom na zasadzie dostępu na poziomie niezbędnego minimum oraz – jeżeli jest to możliwe – dla każdego zdarzenia osobno, zgodnie z polityką kontroli dostępu, tj. minimalny zakres dostępu wymagany dla ich funkcji i tylko wtedy, kiedy jest to potrzebne;
- należy utrzymywać procedurę autoryzacji i wykaz wszystkich przydzielonych uprawnień, przy czym uprawnień nie należy nadawać, dopóki procedura autoryzacji nie zostanie ukończona;
- powinna istnieć efektywna procedura recertyfikacji na potrzeby oceny i w razie konieczności także odbierania uprawnień, która powinna być regularnie przeprowadzana;
- należy promować opracowywanie rutynowych procedur systemowych i korzystanie z nich, aby uniknąć konieczności nadawania użytkownikom uprawnień ogólnych;
- uprawniania administratora powinny być przydzielane użytkownikom za pomocą innego ID użytkownika niż ID używane do normalnej działalności;
- zakres i skomplikowanie procesów, architektury i infrastruktury może wymagać kontroli dostępu w oparciu o role lub innych, co najmniej równie mocnych modeli kontroli dostępu.

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Polityka bezpieczeństwa, zasady funkcjonowania usługi, specyfikacje zastosowania, specyfikacja rozwiązań architektury i sprawozdania z audytów

4.2 KK 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[12] dostawców usług internetowych lub zbliżone metody uwierzytelniania.

4.2.1 Czy dostawca usług płatniczych / podmiot zarządzający systemem płatności posiada odpowiednie rozwiązania w zakresie bezpieczeństwa w celu ochrony sieci, stron internetowych, serwerów i łączy komunikacyjnych przed nadużyciami i atakami? Poniżej znajduje się niewyczerpująca lista możliwych środków kontroli, które można rozważyć:

- *Czy dostawca usług płatniczych / podmiot zarządzający systemem płatności posiada skuteczny proces zarządzania aktualizacjami bezpieczeństwa, który zapewnia, że systemy mają wystarczająco aktualne wydania aktualizacji?*
- *Czy wszystkie systemy krytyczne posiadają – zgodnie z wymaganiami – najnowsze i odpowiednie poprawki oprogramowania chroniące przed nadużyciami i naruszaniem bezpieczeństwa danych wrażliwych przez osoby działające w złym zamiarze lub złośliwe oprogramowanie?*
- *Czy dostawca usług płatniczych / podmiot zarządzający systemem płatności ustanowił zapory sieciowe z odpowiednimi regułami pozwalającymi tylko na uprawnione połączenia?*
- *Czy dostawca usług płatniczych / podmiot zarządzający systemem płatności podjął działania zapobiegające atakom typu DoS/DDoS (odmowa usługi / rozproszona odmowa usługi)?*
- *Czy w celu sygnalizacji ataków zidentyfikowanych za pomocą analizy heurystycznej lub znanego i odpowiednio ustalonego modelu dostawca usług płatniczych / podmiot zarządzający systemem płatności używa systemów wykrywania włamań i zapobiegania im?*
- *Czy dostawca usług płatniczych / podmiot zarządzający systemem płatności używa kanałów komunikacji odpornych na manipulację i bezpiecznych metod uwierzytelnienia (takich jak VPN) do zarządzania serwerami?*
- *Czy dostawca usług płatniczych / podmiot zarządzający systemem płatności umożliwił pełne szyfrowanie sesji?*
- *Czy dostawca usług płatniczych / podmiot zarządzający systemem płatności posiada środki kontroli zapewniające odpowiednią jakość architektury danych aplikacji?*
- *Czy dostawca usług płatniczych / podmiot zarządzający systemem płatności posiada politykę dotyczącą bezpiecznych metod tworzenia i modyfikowania aplikacji?*
- *Czy dostawca usług płatniczych / podmiot zarządzający systemem płatności zapewnił, aby dany kod*

[12] Certyfikat rozszerzonej walidacji (EV) to typ certyfikatu klucza publicznego X.509 wydawany według określonego zestawu kryteriów weryfikacji tożsamości. Kryteria te wymagają rozszerzonego zakresu weryfikacji tożsamości podmiotu wnioskującego przez urząd certyfikacji przed wydaniem certyfikatu (źródło: Wikipedia).

źródłowy podlegał procesowi code review przeprowadzonemu przez niezależną osobę, zanim dane zmiany w kodzie zostaną uruchomione w środowisku produkcyjnym w celu zminimalizowania luk bezpieczeństwa, w tym luk typu backdoor, i możliwości manipulacji?

- *Czy dostawca usług płatniczych / podmiot zarządzający systemem płatności posiada środki kontroli zapewniające, aby wszelkie aplikacje i systemy IT były odpowiednio udokumentowane?*
- *Czy dostawca usług płatniczych / podmiot zarządzający systemem płatności zapewnił, aby zmiany oprogramowania podlegały odpowiednim testom wykonywanym przez testerów niebędących ich programistami, przed uruchomieniem ich w środowisku produkcyjnym?*
- *Czy dostawca usług płatniczych / podmiot zarządzający systemem płatności ustanowił skuteczny proces zarządzania zmianami?*
- *Czy dostawca usług płatniczych / podmiot zarządzający systemem płatności regularnie wykonuje skanowanie pod względem luk bezpieczeństwa?*
- *Czy dostawca usług płatniczych / podmiot zarządzający systemem płatności prowadzi testy penetracyjne wykonywane przez certyfikowanych testerów?*

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Polityka bezpieczeństwa, zasady funkcjonowania usługi, specyfikacje zastosowania, specyfikacja rozwiązań architektury i sprawozdania z audytów

4.2.2 Czy dostawca usług płatniczych / podmiot zarządzający systemem płatności usunął z serwerów wszystkie zbędne funkcje i nieużywane usługi („utwardzenie“)? Dostawca usług płatniczych może rozważyć:

- *przyjęte w branży standardy „utwardzania" systemu (np. CICS, ISP, SANS, NIST itp.);*
- *zmianę domyślnego ID użytkownika i domyślnych danych uwierzytelniających (np. hasła administratorów) przed instalacją produktu;*
- *włączenie tylko niezbędnych usług i protokołów;*
- *usunięcie wszelkich zbędnych elementów, takich jak skrypty, sterowniki, funkcjonalności, podsystemy i systemy plików, jak również niepotrzebnych aplikacji serwerowych.*

Ma zastosowanie do: Wszystkich
Dokumenty potwierdzające: Polityka bezpieczeństwa, specyfikacja rozwiązań architektury i sprawozdania z audytów

4.2.3 Czy dostawca usług płatniczych / podmiot zarządzający systemem płatności zapewnia bezpieczną komunikację zgodnie z aktualnymi dobrymi praktykami, w tym korzystanie z certyfikatów rozszerzonej walidacji (np. długość klucza, wersja TLS, kryptograficzny algorytm szyfrujący itp.) skonfigurowanych dla nazwy dostawcy usług płatniczych lub czy dostawca usług płatniczych używa innych podobnych metod uwierzytelniania?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Polityka bezpieczeństwa i certyfikat rozszerzonej walidacji (lub porównywalna metoda)

4.3 KK 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).

4.3.1 Czy dostawca usług płatniczych / podmiot zarządzający systemem płatności posiada odpowiednie procedury monitorowania, śledzenia i ograniczania dostępu logicznego i fizycznego do wrażliwych danych płatniczych i zasobów krytycznych? Czy zapewnia, aby dostęp był udzielany wyłącznie upoważnionym użytkownikom i programom?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Polityka bezpieczeństwa i specyfikacje aplikacji

4.3.2 Czy dostawca usług płatniczych / podmiot zarządzający systemem płatności tworzy, przechowuje i śledzi

odpowiednie dzienniki zdarzeń i ślady audytowe?

- Aplikacje dostawcy usług płatniczych / podmiotu zarządzającego systemem płatności są w stanie zapewnić ślady audytowe, w tym komunikaty logowania, błędów i ostrzeżeń, jak również innego rodzaju komunikaty w plikach dziennika zdarzeń.
- Dostawca usług płatniczych / podmiot zarządzający systemem płatności zapewnia, aby znaczniki czasu w plikach dziennika zdarzeń i śladach audytowych były dokładne, np. poprzez regularną synchronizację swoich serwerów z co najmniej jednym zaufanym źródłem pomiaru czasu (takim jak serwer czasu lub GPS).
- Dostawca usług płatniczych / podmiot zarządzający systemem płatności regularnie analizuje pliki dziennika zdarzeń i ślady audytowe oraz podejmuje działania naprawcze i/lub zapobiegawcze.

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Specyfikacja aplikacji i sprawozdania z audytu

4.4 KK Projektując[13], rozwijając i utrzymując usługi płatności internetowych, dostawcy usług płatniczych powinni zapewnić, aby kluczowym elementem podstawowej funkcjonalności była minimalizacja danych[14]: zbieranie, przesyłanie, przetwarzanie, przechowywanie i/lub archiwizowanie oraz wizualizowanie wrażliwych danych płatniczych powinny być utrzymywane na minimalnym poziomie.

4.4.1 Czy dostawca usług płatniczych wykonał analizę typów informacji osobistych niezbędnych do funkcjonowania usługi płatniczej i zdefiniował minimalny poziom wymaganych danych?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Sprawozdanie z oceny ryzyka

4.4.2 Czy dostawca usług płatniczych zapewnia, aby minimalizacja danych była istotnym elementem podstawowej funkcjonalności w fazie projektowania, rozwoju i utrzymania? *(Np. dostawca usług płatniczych opisuje stosowane środki zabezpieczenia, jak również określa zarówno zautomatyzowane, jak i ręczne środki kontroli zapewniające, że minimalizację danych uwzględnia się w fazie projektowania, rozwoju i utrzymania, tak aby gromadzenie, przesyłanie, przetwarzanie, przechowywanie i/lub archiwizowanie i wizualizowanie wrażliwych danych płatniczych uzyskiwanych za pośrednictwem aplikacji było utrzymywane na minimalnym poziomie.)*

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Polityka bezpieczeństwa, specyfikacja aplikacji, dokumentacja metodologii projektowania i rozwoju oprogramowania

4.5 KK 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 zapewniającemu 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.

4.5.1 Czy dostawca usług płatniczych / podmiot zarządzający systemem płatności testuje zabezpieczenia usług płatności internetowych pod nadzorem funkcji zarządzania ryzykiem?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Polityka bezpieczeństwa i dokument zatwierdzający funkcję zarządzania ryzykiem

4.5.2 Czy dostawca usług płatniczych / podmiot zarządzający systemem płatności zapewnia, aby wszystkie zmiany podlegały formalnemu procesowi zarządzania zmianą do celów planowania, testowania,

[13] Domyślna ochrona prywatności.
[14] Minimalizacja danych oznacza politykę gromadzenia najmniejszej ilości informacji osobistych niezbędnych do realizacji danej funkcji.

dokumentowania i autoryzowania zmian?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Dokument wnioskowania o zmiany i plan

4.5.3 Czy dostawca usług płatniczych / podmiot zarządzający systemem płatności wykonuje regularne testy pod względem istotnych i znanych potencjalnych ataków, aby zapewnić, że zmiany są wdrażane w sposób prawidłowy i że możliwe punkty narażenia na obserwowane zagrożenia dla bezpieczeństwa są identyfikowane?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Polityka bezpieczeństwa, scenariusze testów i sprawozdania z testów

4.6 KK 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.

4.6.1 Czy wdrażanie i funkcjonowanie usług płatności internetowych, jak również środki bezpieczeństwa stosowane przez dostawcę usług płatniczych / podmiot zarządzający systemem płatności podlegają okresowym audytom, aby zapewnić ich odporność i skuteczność? (Audyt w momencie pierwszego wdrożenia uznaje się za audyt jednorazowy, natomiast dalsze audyty funkcjonalne powinny być wykonywane w przypadku większych zmian.)

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Polityka zarządzania audytem, sprawozdanie z audytu i certyfikacja audytora

4.6.2 Czy dostawca usług płatniczych uwzględnia ryzyka w zakresie bezpieczeństwa, aby ustalić częstotliwość i główne obszary audytu proporcjonalnie do ryzyka w zakresie bezpieczeństwa?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Polityka zarządzania audytem

4.6.3 Czy dostawca usług płatniczych / podmiot zarządzający systemem płatności zapewnia, aby audytorzy byli wiarygodnymi i niezależnymi ekspertami (tj. aby w żaden sposób nie uczestniczyli w fazie opracowania i rozwoju usług płatności internetowych, ich wdrażania i operacyjnego zarządzania nimi)?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Polityka zarządzania audytem

4.6.4 Czy dostawca usług płatniczych / podmiot zarządzający systemem płatności posiada procedury zgłaszania wyników takich audytów zarządowi?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Sprawozdanie dla zarządu / komitetu ds. audytu

4.6.5 Czy dostawca usług płatniczych / podmiot zarządzający systemem płatności zdefiniował pojęcie „istotnej zmiany“ (o której mowa w punkcie 4.6.1)?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Polityka zarządzania audytem

4.7 KK 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.

4.7.1 Czy dostawca usług płatniczych / podmiot zarządzający systemem płatności wymaga w umowie od swoich wykonawców, aby przestrzegali oni zasad i rekomendacji przedstawionych w dokumencie „Rekomendacje dotyczące bezpieczeństwa płatności internetowych" za każdym razem, gdy wykonanie funkcji związanych z bezpieczeństwem płatności internetowych jest powierzane podmiotom zewnętrznym?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Polityka bezpieczeństwa i umowy outsourcingu

4.8 KK 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.

4.8.1 Czy dostawca usług płatniczych świadczący usługi agenta rozliczeniowego wymaga w umowie zawieranej z akceptantami obsługującymi wrażliwe dane płatnicze wdrożenia środków bezpieczeństwa w ich infrastrukturze IT zgodnie z KK 4.1 do 4.7?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Umowa z akceptantem

4.8.2 Czy dostawca usług płatniczych ustanowił procedurę monitorowania przestrzegania tych zobowiązań umownych, szczegółowo określającą kroki, które należy podjąć w przypadku wykrycia naruszeń, włącznie z rozwiązaniem umowy z akceptantem?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Dokument polityki

4.1 DP Dostawcy usług płatniczych mogą dostarczać narzędzia bezpieczeństwa (tj. urządzenia i/lub dostosowane przeglądarki internetowe, odpowiednio zabezpieczone) w celu ochrony interfejsu klienta przed nielegalnym wykorzystaniem lub atakami (np. atakami typu „man-in-the-browser").

4.1.1 DP Czy dostawca usług płatniczych dostarcza narzędzia bezpieczeństwa w celu ochrony interfejsu klienta przed nieuprawnionym wykorzystaniem lub atakami (np. bezpieczny interfejs zapewniany przez specjalnie skonfigurowane oprogramowanie z zabezpieczonego urządzenia USB[15], dedykowane oprogramowanie skanujące komputer klienta)?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Polityka bezpieczeństwa

Rekomendacja 5: Śledzenie

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

5.1 KK Dostawcy usług płatniczych powinni zapewnić, aby świadczone przez nich usługi uwzględniały

[15] Np. przenośna „bezpieczna przeglądarka" dostępna na urządzeniu pamięci USB i pracująca poza systemem operacyjnym komputera.

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.

5.1.1 Czy dostawca usług płatniczych / podmiot zarządzający systemem płatności zapewnia, aby jego usługi uwzględniały mechanizmy bezpieczeństwa pozwalające na szczegółowe rejestrowanie transakcji i danych poleceń zapłaty?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Polityka bezpieczeństwa

5.1.2 Czy rejestry transakcji i poleceń zapłaty zawierają prawidłowe numery porządkowe transakcji i znaczniki czasu?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Specyfikacja aplikacji

5.1.3 Czy zmiany parametryzacji, dostęp i próby dostępu do transakcji i poleceń zapłaty są dokładnie rejestrowane?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Specyfikacja aplikacji

5.1.4 Czy dostawca usług płatniczych / podmiot zarządzający systemem płatności zapewnia, aby pliki dziennika zdarzeń były odporne na manipulację i dostępne wyłącznie dla upoważnionego personelu lub aplikacji?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Specyfikacja aplikacji, sprawozdanie z testowania bezpieczeństwa i sprawozdanie z audytu

5.1.5 Czy dostawca usług płatniczych / podmiot zarządzający systemem płatności zapewnia, aby pliki dziennika zdarzeń były przechowywane za odpowiedni okres, zgodnie z regulacjami lokalnymi?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Polityka bezpieczeństwa

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

5.2.1 Czy dostawca usług płatniczych / podmiot zarządzający systemem płatności ustanowił aplikację do rejestracji plików pozwalającą na śledzenie wszelkich czynności wprowadzania nowych oraz modyfikowania i usuwania danych transakcji lub poleceń zapłaty?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Specyfikacja aplikacji

5.3 KK 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.

5.3.1 Czy dostawca usług płatniczych posiada narzędzia i procesy pozwalające na ocenę plików dziennika zdarzeń?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Polityka bezpieczeństwa

5.3.2 Czy dostawca usług płatniczych posiada politykę kontroli dostępu, która pozwala na dostęp do narzędzi oceny plików dziennika zdarzeń i na ich parametryzację tylko upoważnionemu personelowi?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Polityka bezpieczeństwa

5.3.3 Czy dostawca usług płatniczych okresowo przegląda i analizuje zarejestrowane dane transakcji i poleceń zapłaty pod kątem nieprawidłowości, oznak manipulacji i nieuprawnionego dostępu?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Polityka bezpieczeństwa

5.3.4 Czy poza regularnymi kontrolami istnieją inne zdarzenia, które uruchamiają procedurę przeglądu i analizy operacji?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Polityka bezpieczeństwa

5.1 DP 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.

5.1.1 Czy dostawca usług płatniczych świadczący usługi agenta rozliczeniowego wymaga w umowach zawieranych z akceptantami przechowującymi informacje dotyczące płatności, aby posiadali oni odpowiednie procesy wspomagające śledzenie oraz aby zgłaszali odpowiednie przypadki dostawcy usług płatniczych / podmiotowi zarządzającemu systemem płatności (zgodnie ze wszystkimi KK wymienionymi powyżej)?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Umowa z akceptantem

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 przez 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.

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

6.1.1 Jeżeli istnieją oficjalne wytyczne i wymogi prawne w zakresie identyfikacji zdalnej, czy dostawca usług płatniczych ich przestrzega?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Polityka bezpieczeństwa

6.1.2 Czy dostawca usług płatniczych używa odpowiednich procedur identyfikacji w zakresie płatności internetowych?

- Jeżeli klient nie jest identyfikowany w ramach kontaktu osobistego, czy informacje podawane przez klienta są sprawdzane i potwierdzane przez wiarygodne informacje od osoby trzeciej (które, w zależności od prawa danego kraju, mogą stanowić rachunki za telefon lub energię elektryczną lub identyfikację przez osoby trzecie) lub informacje gromadzone na podstawie przelewu niewielkiej kwoty pieniędzy?
- Czy procedury dostawcy usług płatniczych w zakresie analizy due diligence klienta są regularnie weryfikowane przez wewnętrznego/zewnętrznego audytora i zgłaszane zarządowi i właściwemu organowi władzy?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Polityka bezpieczeństwa

6.1.3 Czy proces identyfikacji ma miejsce przed udzieleniem klientowi dostępu do usług płatności internetowych?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Polityka bezpieczeństwa

6.2 KK 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] Przykładowo: Dyrektywa 2005/60/WE Parlamentu Europejskiego i Rady z dnia 26 października 2005 r. w sprawie przeciwdziałania korzystaniu z systemu finansowego w celu prania pieniędzy oraz finansowania terroryzmu, Dz. U. L 309, z dnia 25.11.2005 r., str. 15-36. Patrz także: 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, Dz. U. L 214, z dnia 04.08.2006 r., str. 29-34.

[17] Na przykład 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.

6.2.1 Czy dostawca usług płatniczych przekazuje klientowi z wyprzedzeniem informacje zgodnie z punktami wymienionymi powyżej[20]?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Umowa / warunki świadczenia usługi

6.2.2 Jeżeli kompletność i ważność informacji przekazywanych klientom przez dostawcę usług płatniczych musi zostać (z czasem) poświadczona przez właściwy organ władzy, czy dostawca usług płatniczych przestrzega tego wymogu?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Polityka

6.2.3 Czy dostawca usług płatniczych wymaga od klientów, aby formalnie potwierdzili otrzymanie tych informacji?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Umowa / warunki świadczenia usługi

6.3 KK Dostawcy usług płatniczych powinni zapewnić, aby umowa ramowa z klientem wskazywała, że dostawca usług płatniczych może zablokować określoną transakcję lub instrument płatniczy[21] 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.

6.3.1 Czy umowa ramowa pomiędzy dostawcą usług płatniczych a klientem uwzględnia postanowienia dotyczące płatności internetowych, a w szczególności:

- możliwość zablokowania określonych transakcji lub instrumentów płatniczych przez dostawcę usług płatniczych na podstawie uprzednio zdefiniowanych problemów z bezpieczeństwem;
- metody i warunki powiadamiania klienta przez dostawcę usług płatniczych o zablokowaniu;
- sposoby komunikacji pomiędzy klientem a dostawcą usług płatniczych w celu rozwiązania problemu zablokowania?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Umowa ramowa

[20] Potencjalnie z zastrzeżeniem zmian uwzględniających zrewidowaną wersję dyrektywy ws. usług płatniczych – po jej zatwierdzeniu.
[21] Patrz: art. 55 dyrektywy ws. usług płatniczych dotyczący limitów w zakresie korzystania z instrumentów płatniczych.

6.3.2 Czy blokowanie transakcji opiera się na dobrze zdefiniowanych kryteriach (np. matrycy ryzyka uwzględniającej profil ryzyka i profil ogólny klienta oraz kwotę danej transakcji lub zachowania płatnicze klienta)?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Polityka bezpieczeństwa i sprawozdanie z oceny ryzyka

6.3.3 Czy procedura odblokowania transakcji uwzględnia postanowienia dyrektywy ws. usług płatniczych i informuje klienta o kosztach i jego wkładzie finansowym, jak również o ewentualnych roszczeniach przysługujących klientowi w przypadku nieuzasadnionego zablokowania transakcji?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Umowa / warunki świadczenia usługi

6.4 KK 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.

6.4.1 Czy dostawca usług płatniczych przekazuje klientowi wyraźne instrukcje dotyczące jego odpowiedzialności za bezpieczne korzystanie z usług? Czy te instrukcje są przekazywane za pośrednictwem odpowiednich kanałów komunikacji oraz z akceptowalną częstotliwością?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Umowa / warunki świadczenia usługi

6.4.2 Jeżeli instrukcje te muszą zostać najpierw sprawdzone przez właściwy organ władzy, czy dostawca usług płatniczych przestrzega tego wymogu?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Polityka

6.1 DP 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.

6.1.1 DP Czy dostawca usług płatniczych oferuje dedykowaną umowę o świadczenie usług w zakresie przeprowadzania transakcji płatności internetowych, czy też możliwości wykonywania takich płatności są ujęte w umowie ramowej?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Umowa

6.1.2 DP Jeżeli te dedykowane umowy o świadczenie usług muszą zostać najpierw sprawdzone przez właściwy organ władzy, czy dostawca usług płatniczych przestrzega tego wymogu?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Polityka

Rekomendacja 7: Silne uwierzytelnianie klienta

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

Wyjaśnienie procedury silnego uwierzytelniania klienta.

7.0.1 Czy procedura uwierzytelniania obejmuje co najmniej dwa elementy potwierdzania tożsamości użytkownika?

- Procedura uwierzytelniania wymaga użycia co najmniej dwóch elementów.
- Wybiera się je z co najmniej dwóch zdefiniowanych kategorii (tj. wiedza i posiadanie są dozwolone; posiadanie i posiadanie nie są dozwolone).

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Specyfikacja techniczna

7.0.2 Dotyczy elementów posiadania i cech klienta:

Czy niezależne i kompetentne osoby trzecie poświadczają lub ewaluują, czy poziom bezpieczeństwa tych urządzeń jest solidny i czy są one odporne na manipulację?

- Urządzenia uzyskały poświadczenie od organów certyfikacji na podstawie przyjętych standardów lub metodologii lub zostały co najmniej poddane ewaluacji (np. sprawozdanie nt. bezpieczeństwa) przez np. laboratoria, ekspertów uniwersyteckich lub konsultantów technicznych.
- Odporność jest weryfikowana na podstawie testów penetracyjnych i oceny podatności na zagrożenia.

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Certyfikacja / sprawozdanie z ewaluacji

7.0.3 Czy zabezpieczenia danego rozwiązania zostały odpowiednio określone i wdrożone (np. specyfikacja algorytmu, długość klucza, entropia informacji[22])?

- Zabezpieczenia są zgodne z publicznie dostępnymi i uznawanymi standardami.
- Dotyczy jednorazowych haseł: Czy wartość hasła jest generowana za pomocą bezpiecznych urządzeń i procedur na podstawie publicznie dostępnych i uznawanych standardów? Procedury generują hasła o wystarczającym stopniu skomplikowania; wiedza na temat jednej wartości hasła nie jest wykorzystywana do tworzenia kolejnych wartości.

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Specyfikacja techniczna

7.0.4 Jeżeli w roli elementu posiadania (np. celem uzyskania lub wygenerowania hasła jednorazowego lub zainicjowania mechanizmu kontroli przerwań (ang. drop call mechanism)) używane jest urządzenie wielofunkcyjne (np. telefon komórkowy lub tablet), czy dostawca usług płatniczych stosuje środki mające na celu zminimalizowanie ryzyka wykorzystania tego urządzenia do inicjowania w tym samym czasie płatności internetowych stanowiących oszustwo (np. za pośrednictwem wirusów / ataków internetowych)?

- Czy zabezpieczenia są zgodne z rekomendacjami zawartymi w publicznie dostępnych i uznawanych standardach?
- Czy sama płatność jest inicjowana za pośrednictwem osobnego/niezależnego kanału?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Specyfikacja techniczna

7.0.5 Czy informacje poufne używane w ramach elementu wiedzy są oparte na odpowiedniej polityce bezpieczeństwa?

[22] W tym kontekście termin „entropia" oznacza *miarę wielkości niepewności, z którą atakujący musi się zmierzyć, aby ustalić wartość tajemnicy*. Koncepcja ta jest stosowana w kontekście teorii informacji i kryptografii jako miara trudności odgadnięcia lub ustalenia hasła lub klucza.

- Czy istnieje polityka haseł (entropia informacji, skomplikowanie, długość, okres ważności, liczba znaków, których nie można powtórzyć, niemożliwość łatwego odgadnięcia)? Jeśli tak, czy jest egzekwowana?
- Jeśli przyjęta jest procedura oparta na zabezpieczeniu innym niż hasło, czy zapewnia się, aby prawdopodobieństwo uznania osoby nieupoważnionej za upoważnioną (ang. false positive) było porównywalne lub niższe niż w przypadku (mocnego) hasła?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Polityka bezpieczeństwa, sprawozdanie z certyfikacji/ewaluacji

7.0.6 Czy procedury i wybrane elementy są zaprojektowane tak, aby zapewnić niezależność, np. pod względem używanej technologii, algorytmów i parametrów?

- Naruszenie jednego z elementów uwierzytelniania pozostaje bez wpływu na ochronę zapewnianą przez inne elementy (np. w przypadku wiedzy i posiadania, kradzież/przywłaszczenie jednego elementu wciąż zmusza atakującego do naruszenia/obejścia drugiego elementu).
- Ewentualnie, w przypadku współzależności (np. jeśli numeru PIN używa się do zainicjowania wygenerowania jednorazowego hasła do urządzenia), ryzyka są odpowiednio minimalizowane z uwzględnieniem następujących zagadnień:
  a) określonych środków bezpieczeństwa, aby uniknąć odgadnięcia numeru PIN lub uzyskania go z urządzenia;
  b) właściwości antyklonujących urządzenia (np. karta chip, token, SIM);
  c) szczególnie silnych zabezpieczeń generowanych haseł jednorazowych (długość, entropia informacji, losowe algorytmy).

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Polityka bezpieczeństwa, sprawozdanie z certyfikacji/ewaluacji

7.0.7 Czy procedura silnego uwierzytelniania klienta działa w taki sposób, że:

- klient musi wpisać wszystkie dane uwierzytelniające przed uzyskaniem wyniku pozytywnego lub negatywnego;
- w przypadkach odmowy uwierzytelnienia nie podaje się informacji o tym, który element podanych danych był niewłaściwy (ID użytkownika, pierwszy element, kolejne elementy itd.)?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Specyfikacja techniczna

7.0.8 Czy co najmniej jeden z wybranych elementów należy do kategorii cech charakterystycznych klienta lub czy jest on (lub one) niemożliwy do ponownego użytku i zreplikowania?

- Kody uwierzytelniania są niereplikowalne, ponieważ wartości jednostki uwierzytelniającej[23] są akceptowane tylko raz przez system uwierzytelniania, pozwalając użytkownikowi na wykonanie tylko danej, określonej operacji.
- Niewykonalne jest sfałszowanie/sklonowanie nadającej się do wykorzystania kopii elementu (za wyjątkiem cech charakterystycznych klienta), nawet jeżeli element jest dostępny, a także niewykonalna jest kradzież powiązanych informacji poufnych (np. kluczy kryptograficznych, wrażliwego oprogramowania lub kluczy prywatnych podpisów cyfrowych) za pośrednictwem internetu, włącznie z sytuacją, w której nie wykonuje się transakcji związanych z płatnością (np. z użyciem złośliwego oprogramowania lub tzw. zaawansowane trwałe zagrożenia – ang. advanced persistent threats, APT).

Ma zastosowanie do: Dostawców usług płatniczych

[23] Element uwierzytelniania (np. wiedza, posiadanie, cecha klienta) wytwarza ciąg danych (np. hasło, hasło jednorazowe, wartość biometryczną), który jest przesyłany zdalnie do serwera uwierzytelniającego w trakcie fazy inicjowania płatności. Ten ciąg danych, „wartość jednostki uwierzytelniającej" jest przesyłany protokołem do serwera uwierzytelniającego jako dowód, że użytkownik posiada i kontroluje „element uwierzytelniania" i w konsekwencji jako dowód tożsamości użytkownika.

Dokumenty potwierdzające: Specyfikacja techniczna

7.0.9 Czy poufność wartości uwierzytelnienia jest chroniona od momentu jej wygenerowania do momentu jej weryfikacji przez serwer uwierzytelniający?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Specyfikacja techniczna

7.0.10 Czy bezpieczeństwo całej procedury silnego uwierzytelniania zostało ocenione (np. za pomocą testów penetracyjnych) i podlega regularnym przeglądom?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Sprawozdanie z certyfikacji/ewaluacji i polityka zarządzania ryzykiem

7.1 KK [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;
- 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[24].

7.1.1 Czy dostawca usług płatniczych wdrożył używanie silnego uwierzytelniania klienta do celów autoryzacji transakcji płatności internetowych klienta?

- Obejmuje to inicjowanie polecenia przelewu (pojedynczego lub pakietu poleceń), inicjowanie przelewu pieniądza elektronicznego i wydanie/zmianę poleceń zapłaty.
- Każde zainicjowanie pojedynczej transakcji lub ich pakietu (pojedynczych zleceń płatniczych lub pakietu takich zleceń) wymaga silnego uwierzytelnienia klienta.

Ma zastosowanie do: Dostawców usług płatniczych [polecenia przelewu / polecenia zapłaty / pieniądz elektroniczny]

Dokumenty potwierdzające: Polityka bezpieczeństwa

7.1.2a Jeżeli dostawca usług płatniczych korzysta z co najmniej jednego z wymienionych wyłączeń, czy ocena bezpieczeństwa wybranych alternatywnych metod uwierzytelniania została wykonana i udokumentowana pod kątem ryzyka powiązanych płatności?

Ma zastosowanie do: Dostawców usług płatniczych [polecenia przelewu / polecenia zapłaty / pieniądz elektroniczny]
Dokumenty potwierdzające: Sprawozdanie z oceny ryzyka (analiza każdej usługi oferowanej klientowi)

7.1.2b Czy dostawca usług płatniczych wymaga silnego uwierzytelniania klienta do celów ustanowienia i/lub modyfikacji białej listy przez klienta przez internet?

[24] Patrz definicja instrumentów przeznaczonych do dokonywania płatności niskokwotowych w art. 34 ust. 1 i art. 53 ust. 1 dyrektywy ws. usług płatniczych.

Ma zastosowanie do: Dostawców usług płatniczych [polecenia przelewu / polecenia zapłaty / pieniądz elektroniczny]

Dokumenty potwierdzające: Polityka bezpieczeństwa

7.1.2c Jeżeli przelewy mają miejsce w ramach tego samego dostawcy usług płatniczych, czy analiza ryzyka transakcji jest używana do określenia płatności niskiego ryzyka według wcześniej zdefiniowanych kategorii i tym samym uzasadnienia użycia alternatywnych metod uwierzytelniania? (Jeżeli ten sam klient posiada dwa rachunki u tego samego dostawcy usług płatniczych, dostawca usług płatniczych nie musi wykonywać analizy ryzyka transakcji dodatkowo do alternatywnego uwierzytelniania klienta.)

Ma zastosowanie do: Dostawców usług płatniczych [polecenia przelewu / polecenia zapłaty / pieniądz elektroniczny]

Dokumenty potwierdzające: Sprawozdanie z oceny ryzyka i polityka bezpieczeństwa

7.1.2d W przypadku kolejnych płatności niskokwotowych[25], czy dostawca usług płatniczych określił limit całkowitej kwoty takich płatności i liczby transakcji niewymagającej silnego uwierzytelnienia klienta?

Ma zastosowanie do: Dostawców usług płatniczych [polecenia przelewu / polecenia zapłaty / pieniądz elektroniczny]

Dokumenty potwierdzające: Sprawozdanie z oceny ryzyka i polityka bezpieczeństwa

7.1.3 Jeśli w wystawieniu lub zmianie elektronicznych poleceń zapłaty nie uczestniczy żaden dostawca usług płatniczych, dostawca usług płatniczych wierzyciela może zachęcać akceptantów do wdrożenia procedury silnego uwierzytelniania klienta.

Ma zastosowanie do: Dostawców usług płatniczych [polecenia przelewu / polecenia zapłaty / pieniądz elektroniczny]

Dokumenty potwierdzające: Umowa dostawcy usług płatniczych wierzyciela z akceptantem

7.2 KK 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.

7.2.1 Czy dostawca usług płatniczych określił wszystkie wrażliwe dane dostępne jego klientom przez internet (np. przez stronę (strony) bankowości online)? Czy dostęp do tych danych i/lub ich zmiana są chronione silnym uwierzytelnieniem klienta? Czy sprawozdanie z oceny ryzyka uwzględnia każdą usługę oferowaną klientowi?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Sprawozdanie z oceny ryzyka

7.2.2 W przypadku usług doradczych niewymagających wyświetlenia wrażliwych informacji dotyczących klienta lub płatności oraz jeżeli przyjęto alternatywne metody uwierzytelniania, czy istnieje analiza ryzyka tych usług, tak aby uzasadnić przyjęcie i odpowiedniość takich rozwiązań uwierzytelniających? Czy sprawozdanie z oceny ryzyka uwzględnia każdą usługę oferowaną klientowi?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Sprawozdanie z oceny ryzyka

7.3 KK [karty] W zakresie transakcji kartowych wszyscy dostawcy usług płatniczych będący wydawcami kart

[25] Zgodnie z definicją zawartą w dyrektywie ws. usług płatniczych.

powinni zapewnić silne uwierzytelnianie posiadacza karty. Wszystkie wydawane karty muszą być przygotowane technicznie (zarejestrowane) do wykorzystywania wraz z silnym uwierzytelnianiem.

7.3.1 Czy dostawca usług płatniczych, wydający karty, wdrożył silne uwierzytelnianie klienta dla wszystkich swoich kart, które mogą być używane w internecie? Czy istnieją znane wyjątki (np. karty korporacyjne) i czy istnieje dla nich analiza ryzyka i odpowiedni monitoring, jeżeli występują jakiekolwiek problemy?

Ma zastosowanie do: Dostawców usług płatniczych [karty]

Dokumenty potwierdzające: Sprawozdanie z oceny ryzyka i polityka bezpieczeństwa

7.3.2 Czy wszystkie karty (które są wydane, aktywowane i możliwe do użycia w internecie) są zarejestrowane w systemie IT dostawcy usług płatniczych, którego używa się do silnego uwierzytelniania klientów?

Ma zastosowanie do: Dostawców usług płatniczych [karty]

Dokumenty potwierdzające: Sprawozdanie z oceny ryzyka, polityka bezpieczeństwa i specyfikacja aplikacji / specyfikacja techniczna

7.3.3 Czy podmiot zarządzający systemem płatności wymaga od dostawcy usług płatniczych wydającego karty silnego uwierzytelniania klienta na żądanie dostawcy usług płatniczych będącego agentem rozliczeniowym lub dostawcy portfela?

Ma zastosowanie do: Dostawców usług płatniczych [karty]

Dokumenty potwierdzające: Polityka

7.4 KK [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.

7.4.1 Czy dostawca usług płatniczych będący agentem rozliczeniowym wdrożył dla wszystkich systemów kartowych, które obsługuje, silne uwierzytelnianie klienta w swoich systemach IT i protokołach używanych podczas komunikacji z wydawcami kart?

Ma zastosowanie do: Dostawców usług płatniczych [karty]

Dokumenty potwierdzające: Sprawozdanie z oceny ryzyka i polityka bezpieczeństwa

7.4.2 Czy te wdrożenia podlegały audytowi lub czy istnieje dla nich proces przeglądu jakości/bezpieczeństwa?

Ma zastosowanie do: Dostawców usług płatniczych [karty]

Dokumenty potwierdzające: Sprawozdanie z audytu / przegląd bezpieczeństwa

7.5 KK [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.

7.5.1 Czy dostawca usług płatniczych będący agentem rozliczeniowym wymaga od swoich akceptantów wspierania silnego uwierzytelnienia klienta przez wystawcę dla transakcji niewymagających fizycznego użycia karty (ang. CNP – card not present) w internecie?

- Czy dostawca usług płatniczych sprawdza, czy akceptant przestrzega tego wymogu?

Ma zastosowanie do: Dostawców usług płatniczych [karty]

Dokumenty potwierdzające: Umowa z akceptantem i sprawozdania z audytu

7.5.2 Czy dostawca usług płatniczych będący agentem rozliczeniowym jest w stanie precyzyjnie monitorować swoją bazę akceptantów w zakresie wdrożenia silnego uwierzytelniania klienta? Na przykład:

- *Czy dostawca usług płatniczych utrzymuje listę swoich akceptantów posiadających skuteczne rozwiązania w zakresie silnego uwierzytelniania klienta?*
- *Czy dostawca usług płatniczych może śledzić transakcje z uwzględnieniem użytej metody uwierzytelnienia (np. silne/alternatywne)?*

Ma zastosowanie do: Dostawców usług płatniczych [karty]

Dokumenty potwierdzające: Umowa z akceptantem, rejestr akceptantów i sprawozdania z monitorowania działalności noszącej znamiona oszustwa

7.5.3 Kiedy dostawca usług płatniczych pozwala akceptantom na korzystanie z alternatywnych metod uwierzytelniania:

- *Czy ten wyjątek jest dozwolony dla płatności niskokwotowej w rozumieniu dyrektywy ws. usług płatniczych lub czy agent rozliczeniowy wymaga od akceptanta wykonania analizy ryzyka w celu uprzedniego zidentyfikowania kategorii transakcji niskiego ryzyka, biorąc pod uwagę charakter sprzedawanych produktów/usług (np. towary i usługi fizyczne/cyfrowe), kanał dostawy, zachowanie klienta, zdolności monitorowania działalności noszącej znamiona oszustwa przez akceptanta itp. oraz czy analiza ryzyka transakcji jest prowadzona w oparciu o te kategorie;*

- *Czy te warunki są uwzględnione w warunkach umownych zapewnionych przez podmiot zarządzający systemem płatności lub w umowach zawartych pomiędzy zainteresowanymi podmiotami (dostawcą usług płatniczych będącym agentem rozliczeniowym, akceptantem)?*

Ma zastosowanie do: Wszystkich [karty]

Dokumenty potwierdzające: Sprawozdanie z oceny ryzyka, polityka bezpieczeństwa i umowa z akceptantem

7.6 KK Wszystkie systemy płatności powinny promować wdrażanie silnego uwierzytelniania klienta poprzez wprowadzenie zasad odpowiedzialności[26] dla uczestniczących dostawców usług płatniczych w ramach rynków europejskich.

7.6.1 Czy podmiot zarządzający systemem płatności wdrożył przeniesienie odpowiedzialności w ramach systemu płatności na dostawcę usług płatniczych niewywiązującego się z obowiązku silnego uwierzytelniania klienta w zakresie płatności internetowych (tj. podczas inicjowania polecenia przelewu, transakcji z użyciem pieniądza elektronicznego lub płatności kartą lub podczas generowania polecenia zapłaty)?

Ma zastosowanie do: Podmiotów zarządzających systemami płatności

Dokumenty potwierdzające: Umowy członkostwa w systemie i regulaminy systemów

7.6.2 Czy zasady odpowiedzialności są transparentne, jasne i egzekwowalne oraz czy uwzględniają mechanizm rozwiązywania sporów?

Ma zastosowanie do: Podmiotów zarządzających systemami płatności

Dokumenty potwierdzające: Umowy członkostwa w systemie i regulaminy systemów

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

[26] 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.

7.7.1 Kiedy prawowity posiadacz po raz pierwszy rejestruje kartę lub co najmniej kiedy inicjowana jest pierwsza transakcja kartą, czy dostawca usług płatniczych zapewnia rozwiązania portfelowe wymagające silnego uwierzytelnienia przez wydawcę?

Ma zastosowanie do: Dostawcy usług płatniczych / Podmiot świadczący usługi portfelowe i [karty]

Dokumenty potwierdzające: Polityka bezpieczeństwa / dokumentacja procesu rejestracji klienta

7.8 KK 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 niskokwotowej, zgodnie z dyrektywą ws. usług płatniczych.

7.8.1 Czy dostawca usług portfelowych zapewnia silne uwierzytelnienie klienta w (co najmniej) jednym z następujących przypadków: i) w przypadku logowania do usługi portfela, ii) podczas inicjowania płatności kartą przez internet?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Polityka bezpieczeństwa / dokumentacja procesu płatności przez klienta

7.8.2 Kiedy dostawca usług płatniczych świadczący usługi portfelowe pozwala akceptantom na korzystanie z alternatywnych metod uwierzytelniania:

- *Czy ten wyjątek jest dozwolony dla płatności niskokwotowych w rozumieniu dyrektywy ws. usług płatniczych lub czy dostawca usług portfelowych wykonał analizę ryzyka w celu uprzedniego zidentyfikowania kategorii transakcji niskiego ryzyka, biorąc pod uwagę charakter sprzedawanych produktów/usług (np. towary i usługi fizyczne/cyfrowe), kanał dostawy, zachowanie klienta, zdolności monitorowania działalności noszącej znamiona oszustwa przez akceptanta itp. oraz czy analiza ryzyka transakcji jest prowadzona w oparciu o te kategorie*;

- *Czy te warunki są uwzględnione w ramach umownych zapewnionych przez podmiot zarządzający systemem płatności lub w umowach zawartych pomiędzy zainteresowanymi podmiotami (dostawcą usług portfelowych, akceptantem)?*

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Sprawozdanie z oceny ryzyka, polityka bezpieczeństwa i umowa z akceptantem

7.9 KK [karty] W zakresie kart wirtualnych wstępna rejestracja powinna odbywać się w bezpiecznym i zaufanym środowisku[27]. Silne uwierzytelnianie klienta powinno być wymagane w procesie generowania danych kart wirtualnych w przypadku, gdy karta wydawana jest w środowisku internetowym.

7.9.1 W przypadku wdrożenia kart wirtualnych, czy wstępna rejestracja ma miejsce w bezpiecznym i zaufanym środowisku zgodnie z przedstawioną definicją?

Ma zastosowanie do: Dostawców usług płatniczych [karty]

Dokumenty potwierdzające: Polityka bezpieczeństwa / proces rejestracji klienta, inne dokumenty na poparcie

[27] 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 podmiot zarządzający systemem płatności zapewnia 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).

7.9.2 Czy silne uwierzytelnianie klienta jest wymagane podczas generowania danych karty wirtualnej przez internet?

Ma zastosowanie do: Dostawców usług płatniczych [karty]

Dokumenty potwierdzające: Specyfikacja aplikacji

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

7.10.1 Czy dwustronne (wzajemne) uwierzytelnianie jest wymagane przez dostawcę usług płatniczych podczas komunikowania się z akceptantami na potrzeby inicjowania płatności internetowych i uzyskiwania dostępu do wrażliwych danych płatniczych, np. z użyciem bezpiecznych protokołów (takich jak TLS), pozwalających na wzajemne uwierzytelnienie zgodnie z aktualnymi dobrymi praktykami (dotyczącymi między innymi długości klucza, wersji TLS, kryptograficznego algorytmu szyfrującego itp.)?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Umowa dostawcy usług płatniczych i akceptanta oraz specyfikacja techniczna

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

7.1.1 DP Uwzględniona w punkcie KK 7.5.1

Ma zastosowanie do: Akceptantów [karty]

Dokumenty potwierdzające: Umowa z akceptantem

7.2 DP 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 7.2.1 Czy dostawca usług płatniczych oferuje to samo rozwiązanie w zakresie silnego uwierzytelniania klienta wobec wszystkich swoich klientów i wszystkich usług płatności internetowych, w tym np. usług płatności w ramach bankowości online i płatności kartą przez internet?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Polityka bezpieczeństwa i specyfikacja techniczna

DP 7.2.2 Czy dostawca usług płatniczych określił rozwiązania awaryjne obejmujące ryzyko punktów podatności na uszkodzenie (ang. single point of compromise) (w zakresie narzędzia SCA)?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Polityka bezpieczeństwa i specyfikacje techniczna

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

7.3.1 DP Czy dostawca usług płatniczych zapewnia rozwiązania w zakresie silnego uwierzytelniania klienta, dla których jeden (lub kilka) z wybranych elementów pociąga za sobą oznaczenie danych transakcji (określających kwotę i płatnika, jak również znacznik czasu i zapewnienie, że transakcja nie może zostać zmodyfikowana)?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Polityka bezpieczeństwa i specyfikacja techniczna

7.3.2 DP Czy wybrane rozwiązania zostały poddane audytowi/przeglądowi, w tym pod względem odporności na manipulowanie?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Certyfikacja / sprawozdanie z ewaluacji

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.

8.1 KK 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.

– [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.

8.1.1 Czy dostawca usług płatniczych wdrożył procedurę zapewniającą, że wnioskowanie o narzędzia uwierzytelniające i/lub oprogramowanie związane z płatnościami dostarczane klientowi oraz ich dostarczanie odbywa się w bezpiecznym i zaufanym środowisku?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Polityka bezpieczeństwa i specyfikacja techniczna

8.1.2 Czy dostawca usług płatniczych uwzględnił możliwe ryzyka związane z przekazywanymi narzędziami uwierzytelniania i/lub oprogramowaniem dostarczanym klientowi wynikające z używania urządzeń, które nie znajdują się pod kontrolą dostawcy usług płatniczych?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Sprawozdanie z oceny ryzyka i specyfikacja techniczna

8.1.3 Czy dostawca usług płatniczych posiada skuteczne i bezpieczne procedury dostarczania spersonalizowanych danych uwierzytelniających (np. osobne dostarczenie urządzeń i danych uwierzytelniających, osobne kanały dostawy)?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Polityka bezpieczeństwa

8.1.4 Czy dostawca usług płatniczych posiada skuteczne i bezpieczne procedury dostarczania

spersonalizowanego oprogramowania związanego z płatnościami?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Polityka bezpieczeństwa

8.1.5 Czy dostawca usług płatniczych posiada skuteczne i bezpieczne procedury dostarczania wszystkich spersonalizowanych urządzeń związanych z płatnościami internetowymi?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Polityka bezpieczeństwa

8.1.6 Czy dostawca usług płatniczych posiada procedurę monitorowania liczby incydentów związanych z dostarczaniem narzędzi uwierzytelniania i oprogramowania?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Polityka zarządzania incydentami

8.1.7 Jeżeli oprogramowanie jest dostarczane przez internet, czy zapewnia się, aby było ono podpisane cyfrowo przez dostawcę usług płatniczych, w celu umożliwienia klientom dokonania weryfikacji jego autentyczności oraz sprawdzenia, czy nie podlegało ono manipulacji?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Polityka bezpieczeństwa

8.1.8 Czy dostawca usług płatniczych określa w swoich umowach lub polityce, że klient (w przypadku transakcji dokonywanych kartą) ma możliwość wyboru uwierzytelniania niezależnie dla poszczególnych zakupów internetowych?

Ma zastosowanie do: Dostawców usług płatniczych [karty]

Dokumenty potwierdzające: Polityka bezpieczeństwa i umowy z klientami

8.1.9 Jeżeli dostawca usług płatniczych oferuje aktywację silnego uwierzytelniania klienta podczas zakupów internetowych, czy ma to miejsce poprzez przekierowanie klienta do bezpiecznego i zaufanego środowiska?

Ma zastosowanie do: Dostawców usług płatniczych [karty]

Dokumenty potwierdzające: Specyfikacja techniczna

8.2 KK [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.

8.2.1 Czy wystawcy aktywnie zachęcają posiadaczy kart do wybierania silnego uwierzytelniania?

Ma zastosowanie do: Dostawców usług płatniczych [karty]

Dokumenty potwierdzające: Materiały informacyjne dla klientów i umowy z klientami

8.2.2 Czy dostawca usług płatniczych wyraźnie określił – w oparciu o analizę ryzyka – ograniczoną liczbę wyjątkowych przypadków, w których dozwolone jest pominięcie silnego uwierzytelnienia?

Ma zastosowanie do: Dostawców usług płatniczych [karty]

Dokumenty potwierdzające: Sprawozdanie z oceny ryzyka

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.

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

9.1.1 Czy dostawca usług płatniczych zdefiniował okres ważności hasła jednorazowego zgodnie z analizą ryzyka? Jeśli tak, czy skutkuje on ograniczoną żywotnością hasła?

- Zdefiniowany okres ważności skutkuje ograniczoną żywotnością hasła, która jest odpowiednia do zapobiegania atakom (np. w niektórych przypadkach odpowiedni może być okres ważności poniżej 120 sekund).

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Ocena ryzyka, polityka bezpieczeństwa i specyfikacja techniczna

9.2 KK 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.

9.2.1 Czy dostawca usług płatniczych określił maksymalną liczbę nieudanych prób logowania i uwierzytelniania (ang. retry limits) zgodnie z analizą ryzyka (patrz Rekomendacja 2), po której dostęp do usług płatności internetowych jest blokowany (tymczasowo lub na stałe)?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Sprawozdanie z oceny ryzyka, polityka bezpieczeństwa i specyfikacja techniczna

9.2.2 Czy dostawca usług płatniczych określił konkretne procedury w celu umożliwienia sobie zablokowania (tymczasowo lub na stałe) usługi płatności internetowych w przypadku wyczerpania dozwolonej liczby prób? Czy klient został poinformowany o ograniczeniu liczby prób i o procedurze przywracania usług płatności internetowych? Czy klientom niezwłocznie dostarcza się wyraźne powiadomienie o zablokowaniu usługi i informację o procedurze przywracania usługi płatności internetowych?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Polityka bezpieczeństwa i specyfikacja techniczna

9.2.3 Czy dostawca usług płatniczych określił konkretne, bezpieczne procedury przywracania zablokowanych usług płatności internetowych?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Polityka bezpieczeństwa

9.2.4 Czy dostawca usług płatniczych wdrożył mechanizm zapobiegający podwójnemu logowaniu?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Polityka bezpieczeństwa

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

9.3.1 Czy dostawca usług płatniczych określił maksymalny okres, po którym nieaktywne sesje usług płatności internetowych są automatycznie zamykane (poprzez zamknięcie zarówno sesji w ramach aplikacji, jak również w ramach sieci po zdefiniowanym okresie braku aktywności) zgodnie z analizą ryzyka (Rekomendacja 2)?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Sprawozdanie z oceny ryzyka i polityka bezpieczeństwa

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.

10.1 KK 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 sparametryzowanych regułach (takich jak czarne listy naruszonych lub skradzionych danych kart) oraz monitorować nietypowe wzorce zachowań klientów lub ich urządzeń dostępowych (takie jak zmiana w trakcie sesji płatniczej adresu lub zakresu adresów IP[28], czasem identyfikowane przez sprawdzenie geolokalizacji adresu IP[29], 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 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.

10.1.1 Czy dostawca usług płatniczych / podmiot zarządzający systemem płatności posiada rozwiązania w zakresie wykrywania oszustw i zapobiegania im w celu identyfikowania podejrzanych transakcji przed ich ostateczną autoryzacją?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Polityka bezpieczeństwa i specyfikacja techniczna

10.1.2 Jeżeli system monitorowania jest oparty na sparametryzowanych regułach (takich jak czarne listy naruszonych lub skradzionych danych kart), czy zostały one w wystarczającym stopniu zdefiniowane i są regularnie aktualizowane?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Specyfikacja techniczna

10.1.3 Czy systemy wykrywania oszustw i zapobiegania im, z których korzysta dostawca usług płatniczych / podmiot zarządzający systemem płatności, identyfikują nietypowe wzorce zachowań klientów (takie jak zmiana adresu lub zakresu adresów IP w trakcie sesji internetowej)?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Specyfikacja techniczna

10.1.4 Czy geolokalizacja i/lub kategorie akceptantów są używane/sprawdzane podczas monitorowania (potencjalnie nietypowych) zachowań klientów? Jeżeli nie, czy używane są odpowiednie parametry alternatywne?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Specyfikacja techniczna

10.1.5 Czy dostawca usług płatniczych / podmiot zarządzający systemem płatności posiada rozwiązania

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

w zakresie wykrywania oszustw i zapobiegania im w celu wykrywania oznak infekcji sesji przez szkodliwe oprogramowanie i ostrzegania o podejrzanych transakcjach?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Specyfikacja techniczna

10.1.6 Czy reguły objęte rozwiązaniami monitorującymi zostały przyjęte przez dostawcę usług płatniczych / podmiot zarządzający systemem płatności zgodnie z oceną ryzyka, o której mowa w Rekomendacji 2, oraz są z nią powiązane?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Ocena ryzyka i specyfikacja techniczna

10.2 KK 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[30].

10.2.1 Czy podmiot zarządzający systemem płatności kartowych opracował lub przyjął zharmonizowane definicje kategorii akceptantów?

- Czy definicje te zostały uzgodnione z dostawcami usług płatniczych będącymi agentami rozliczeniowymi?
- Czy definicje te są zgodne ze standardami ustanowionymi dla akceptantów tradycyjnych/fizycznych?
- Czy definicje te są regularnie aktualizowane i ogłaszane[31]?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Plan wdrożenia projektu i zharmonizowane kategorie akceptantów

10.2.2 Czy istnieją procedury zapewniające, aby agenci rozliczeniowi stosowali te definicje w komunikatach autoryzacyjnych przekazywanym wystawcom transakcji płatniczych?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Umowy i regulaminy biznesowe

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

10.3.1 Czy dostawcy usług płatniczych będący agentami rozliczeniowymi posiadają systemy wykrywania nadużyć wdrożone w sposób, który pozwala na monitorowanie działań akceptantów na podstawie na przykład:

10.3.1.1 wzorców transakcji (rodzajów nabywanych produktów/usług, powiązanych z nimi kwot);
10.3.1.2 kategorii akceptantów;
10.3.1.3 geolokalizacji?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Polityka bezpieczeństwa i specyfikacja techniczna

10.4 KK Dostawcy usług płatniczych powinni realizować procedury sprawdzania i oceny przez odpowiedni czas,

[30] Kategorie akceptantów odnoszą się do klasyfikacji akceptantów w odniesieniu do sektora 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.

[31] Biorąc pod uwagę stosunkowo młody wiek rynku sprzedaży internetowej w ujęciu ogólnym oraz jego dynamikę w zakresie nowych rodzajów świadczonych/oferowanych usług.

tak aby nadmiernie nie opóźniać inicjowania i/lub wykonania danej usługi płatniczej.

10.4.1 Czy dostawca usług płatniczych stosuje odpowiednie ramy czasowe dla procedur sprawdzania transakcji (i oceny potencjalnego nadużycia), które zapewniają, aby inicjowanie i/lub wykonanie transakcji nie było nadmiernie opóźnione (zgodnie z przepisami dyrektywy ws. usług płatniczych)?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Polityka bezpieczeństwa i specyfikacja techniczna

10.5 KK 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.

10.5.1 Czy dostawca usług płatniczych określił i udokumentował procedury (techniczne lub inne) mające na celu utrzymywanie statusu zablokowania transakcji przez najkrótszy możliwy czas?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Sprawozdanie z oceny ryzyka, polityka bezpieczeństwa i specyfikacja techniczna

Rekomendacja 11: Ochrona wrażliwych danych płatniczych

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

11.1 KK 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.

11.1.1 Czy dostawca usług płatniczych odpowiednio zidentyfikował i podzielił wszystkie wrażliwe dane dotyczące płatności według potrzeb w zakresie ochrony?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Polityka bezpieczeństwa

11.1.2 Czy powyższe obejmuje 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)?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Ocena ryzyka i polityka bezpieczeństwa

11.1.3 Czy dostawca usług płatniczych ustanowił określone procedury i środki techniczne (np. korzystanie z kryptografii, środków kontroli dostępu lub ścieżki audytu), aby zapewnić, że wszelkie wrażliwe dane płatnicze są odpowiednio chronione przed kradzieżą i nieautoryzowanym dostępem lub modyfikacją?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Polityka bezpieczeństwa

11.2 KK 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”[32], przy użyciu

[32] 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. (2003-06)).

silnych i powszechnie stosowanych technik szyfrowania.

11.2.1 Czy dostawca usług płatniczych zapewnia, 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", przy użyciu silnych i powszechnie stosowanych technik szyfrowania? (Szyfrowanie powinno obejmować całą sesję komunikacyjną – „pełne szyfrowanie sesji".)

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Specyfikacja techniczna

11.3 KK 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 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.

11.3.1 Czy dostawca usług płatniczych zachęca akceptantów do nieprzechowywania jakichkolwiek wrażliwych danych płatniczych, np. oferując usługi agenta rozliczeniowego, który przejmuje odpowiedzialność za wrażliwe dane płatnicze?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Specyfikacja techniczna

11.3.2 W przypadkach gdy akceptanci obsługują (tj. przechowują, przetwarzają lub przesyłają) wrażliwe dane płatnicze, czy dostawca usług płatniczych wprowadza w umowach z takimi akceptantami wymóg posiadania niezbędnych środków mających na celu ochronę tych danych?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Umowa z akceptantem

11.3.3 Czy dostawca usług płatniczych dokonuje regularnych weryfikacji akceptantów, którzy obsługują wrażliwe dane płatnicze (np. w drodze audytu lub wymagając przedstawienia przez akceptanta odpowiednich sprawozdań z audytów)?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Sprawozdania z audytów

11.3.4 W przypadku niewywiązywania się z tych zobowiązań przez akceptantów, czy dostawca usług płatniczych podejmuje kroki mające na celu doprowadzenie do wywiązania się ze zobowiązań umownych lub rozwiązuje umowę?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Sprawozdania z audytów

11.1 DP 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.

11.1 DP Czy dostawca usług płatniczych wymaga w umowach, 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?

Ma zastosowanie do: Akceptantów

Dokumenty potwierdzające: Umowa z akceptantem

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.

12.1 KK Dostawcy usług płatniczych powinni zapewniać funkcjonowanie co najmniej jednego bezpiecznego kanału[33] 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[34];
- 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).

12.1.1 Czy dostawca usług płatniczych zdefiniował co najmniej jeden bezpieczny kanał (np. bankowość elektroniczna, szyfrowane wiadomości e-mail z podpisem cyfrowym, dedykowana, bezpieczna strona internetowa, bankomat) na potrzeby bieżącej komunikacji z klientami w zakresie poprawnego i bezpiecznego korzystania z usług płatności internetowych?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Polityka bezpieczeństwa

12.1.2 Czy dostawca usług płatniczych poinformował klientów o tym kanale oraz wskazał, że jakakolwiek wiadomość przekazana w jego imieniu innym kanałem (jak np. poczta elektroniczna) dotycząca poprawnego i bezpiecznego korzystania z usług płatności internetowych nie jest wiarygodna?

- Procedura ta jest wdrażana w praktyce np. w umowach z klientami, w ulotkach informacyjnych dla klientów, kampaniach informacyjnych lub na stronach internetowych.

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Dokument polityki, umowa z klientem i strona internetowa dostawcy usług płatniczych

12.1.3 Czy dostawca usług płatniczych wyjaśnił klientom: (i) procedury raportowania przez klientów dostawcy usług płatniczych (potencjalnych) transakcji oszukańczych, podejrzanych zdarzeń i nietypowych sytuacji w trakcie sesji usług płatności internetowych i/lub potencjalnych prób ataków socjotechnicznych, (ii) kolejne kroki, tj. w jaki sposób dostawca usług płatniczych odpowie klientowi, (iii) 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)?

- Procedury te są bezpieczne, skuteczne i zrozumiałe dla klienta.

Ma zastosowanie do: Dostawców usług płatniczych

---

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

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

Dokumenty potwierdzające: Dokument polityki i umowy z klientami

12.2 KK 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.

12.2.1 Czy dostawca usług płatniczych posiada procedurę mającą na celu zapewnienie, aby klienci byli informowani poprzez bezpieczny kanał o zmianach w procedurach bezpieczeństwa dotyczących usług płatności internetowych oraz o wszelkich powiadomieniach o pojawiających się istotnych ryzykach (np. ostrzeżenia przed atakami socjotechnicznymi)?

- Procedura jest wyraźnie określona.
- Procedura jest bezpieczna, skuteczna i zrozumiała dla klienta.

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Dokument polityki

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

12.3.1 Czy wsparcie klienta w zakresie zgłaszania nietypowych sytuacji i incydentów dotyczących płatności internetowych i związanych z nimi usług jest dostępne przez całą dobę, a w zakresie wszelkich zapytań, skarg lub wniosków o wsparcie dotyczących płatności internetowych oraz związanych z nimi usług w zwyczajowych godzinach pracy?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Polityka wsparcia klienta

12.3.2 Czy dostawca usług płatniczych posiada procedurę mającą na celu zapewnienie, aby w przypadku poważnego incydentu klientom zostały przesłane odpowiednie informacje?

- Personel wsparcia klienta ma odpowiednie umiejętności.
- Personel wsparcia klienta dysponuje odpowiednimi środkami i wystarczającymi zasobami.

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Polityka HR oraz polityka wsparcia klienta

12.3.3 Czy dostawca usług płatniczych posiada procedurę informowania klientów o sposobach uzyskania wsparcia?

- Może ona obejmować wstępną informację podczas podpisywania umowy z klientem, wskazówki na stronie internetowej dostawcy usług płatniczych, numery alarmowe na instrumentach płatniczych lub narzędziach uwierzytelniania.

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Polityka wsparcia dla klientów, umowa z klientem i strona internetowa dostawcy usług płatniczych

12.4 KK 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.

12.4.1 Czy dostawca usług płatniczych prowadzi programy edukowania i uświadamiania klientów mające na celu zapewnienie, aby klienci rozumieli co najmniej potrzebę:

- ochrony haseł, tokenów, danych osobowych i innych poufnych danych;
- właściwego zarządzania bezpieczeństwem urządzeń osobistych (np. komputerów) poprzez instalowanie i aktualizowanie komponentów bezpieczeństwa (programów antywirusowych, zapór sieciowych, poprawek bezpieczeństwa);
- analizowania 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?

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Dokument polityki oraz materiały programu uświadamiania klientów

12.4.2 Czy dostawca usług płatniczych posiada procedurę mającą na celu zapewnienie, aby treści i dokumentacja dotyczyły danego problemu, były kompletne, zrozumiałe i dostępne?

- Procedura powinna obejmować mechanizm pozyskiwania informacji zwrotnych od klientów w celu pomiaru skuteczności (tj. sprawdzania, czy odbiorcy rozumieją ważne komunikaty) oraz zasięgu programów (np. pomiar liczby klientów).

Ma zastosowanie do: Wszystkich

Dokumenty potwierdzające: Dokument polityki, program uświadamiania klientów oraz statystyki / sprawozdanie z oceny

12.5 KK 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.

12.5.1 Czy dostawcy usług płatniczych będący agentami rozliczeniowymi wymagają od akceptantów w ramach umów 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 akceptanta?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Umowa z akceptantem, specyfikacja techniczna i sprawozdania z audytu

12.5.2 Czy dostawcy usług płatniczych będący agentami rozliczeniowymi monitorują i egzekwują realizację powyższego?

- Dostawca usług płatniczych będący agentem rozliczeniowym ma prawo do przeprowadzenia audytu u akceptanta w zakresie przestrzegania regulaminów i umów.
- Dostawca usług płatniczych będący agentem rozliczeniowym podnosi świadomość akceptantów w tym

zakresie i posiada procedurę mającą na celu zapewnienie przestrzegania tych zasad (np. kary finansowe, rozwiązanie umowy).

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Sprawozdania z audytów

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

12.1.1 DP Czy dostawca usług płatniczych ustanowił/oferuje dla akceptantów fizyczne lub wirtualne programy edukacyjne w zakresie przeciwdziałania oszustwom?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Materiały programów edukacyjnych

12.1.2 DP Czy treści i dokumentacja dotyczą danego problemu oraz czy akceptanci mają łatwy dostęp do tych informacji (np. poprzez chronione strony internetowe, regularne okólniki)?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Materiały programów edukacyjnych

12.1.3 DP Czy dostawca usług płatniczych jest w stanie wykazać, że istotna liczba akceptantów regularnie uczestniczy w programach szkoleniowych?

- Dostawca usług płatniczych posiada procedurę śledzenia liczby akceptantów, którzy uczestniczą w szkoleniach i ukończyli programy edukacyjne.
- Dostawca usług płatniczych określił kategorie ryzyka dla akceptantów i zapewnia, aby zwłaszcza akceptanci wysokiego ryzyka brali udział w programach szkoleniowych.

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Statystyki / sprawozdania z oceny programów edukacyjnych

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.

13.1 KK Przed rozpoczęciem świadczenia klientom usług płatności internetowej dostawcy usług płatniczych powinni ustalić limity[35] 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.

13.1.1 Czy limity dostawcy usług płatniczych zostały wyraźnie określone (np. maksymalna wartość każdej transakcji lub łączna wartość transakcji w określonym czasie)?

- Dostawca usług płatniczych określił limity właściwe dla świadczonych przez siebie usług płatności internetowych lub w inny sposób znajdujące zastosowanie ogólnie do wszystkich instrumentów płatniczych. Limity uwzględniające inne zdalne formy płatności (np. zlecenia przez e-mail lub telefon) także będą akceptowalne.
- Czy limity są proporcjonalne do ryzyka związanego ze świadczonymi usługami (np. dostawca usług płatniczych dokonał analizy powiązanego ryzyka i posiada procedurę mającą na celu zapewnienie, aby limity były proporcjonalne do tego ryzyka)?

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

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Sprawozdanie z analizy ryzyka i dokument polityki

13.1.2 Czy dostawca usług płatniczych posiada procedurę wyraźnego informowania klientów o tych limitach i ich obsłudze w drodze zrozumiałego i transparentnego procesu? Czy proces informowania ma miejsce przed rozpoczęciem świadczenia usług płatności internetowych na rzecz klienta?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Polityka bezpieczeństwa i materiały informacyjne dla klientów

13.1.3 Czy dostawca usług płatniczych poinformował klienta w transparentny sposób o sposobie, w jaki klient może zrezygnować z funkcjonalności płatności internetowych? Czy odpowiednia procedura jest skuteczna i została zrozumiale wyjaśniona?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Polityka bezpieczeństwa i specyfikacja techniczna

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

13.1.1 DP Czy dostawca usług płatniczych udostępnia klientom funkcjonalność zarządzania limitami w zakresie usług płatności internetowych w bezpiecznym i zaufanym środowisku?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Dokument polityki i specyfikacja techniczna

13.1.2 DP Czy dostawca usług płatniczych ustanowił procedurę, która jest odpowiednia, bezpieczna i nie wprowadza w błąd?

- *Procedura została zrozumiale wyjaśniona klientom, włącznie ze wszystkimi istotnymi aspektami (np. kiedy zmiany limitów wchodzą w życie).*
- *Zmiany w limitach użytkownika są rejestrowane i udostępniane klientowi.*

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Dokument polityki i specyfikacja techniczna

13.2 DP 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.

13.2.1 DP Czy dostawca usług płatniczych wdrożył ostrzeżenia dla klientów (np. przez telefon lub SMS) o transakcjach podejrzanych lub wysokiego ryzyka?

- W ramach procedury ustala się wartość domyślną, która uruchamia ostrzeżenie, przy czym możliwe jest obniżenie tej wartości.

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Dokument polityki i specyfikacja techniczna

13.2.2 DP Czy ostrzeżenia są bezpieczne, jasne i zgodne z polityką zarządzania ryzykiem dostawcy usług płatniczych?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Dokument polityki, specyfikacja techniczna

13.3 DP 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.

13.3.1 DP Czy dostawca usług płatniczych umożliwia klientom określenie – w bezpiecznym i zaufanym środowisku – 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?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Dokument polityki i specyfikacja techniczna

13.2.2 DP Czy klient może zmienić spersonalizowane reguły i parametry, o których mowa powyżej, w sposób bezpieczny i wygodny?

- Prowadzona jest historia zmian w spersonalizowanych regułach, która jest udostępniania klientowi za pośrednictwem kanału bankowości elektronicznej.
- Klienci są informowani przez dostawcę usług płatniczych o zmianach limitów dokonanych za pośrednictwem niestandardowych kanałów, np. ostrzeżenia SMS.

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Dokument polityki i specyfikacja techniczna

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.

14.1 KK [polecenia przelewu / polecenia zapłaty] Dostawcy usług płatniczych powinni umożliwiać klientom w niemal rzeczywistym czasie weryfikację statusu wykonania transakcji oraz salda rachunku w dowolnym momencie[36] w bezpiecznym i zaufanym środowisku.

14.1.1 Czy dostawca usług płatniczych umożliwia klientom w niemal rzeczywistym czasie oraz przez całą dobę weryfikację statusu wykonania transakcji oraz salda rachunku w dowolnym momencie?

Ma zastosowanie do: Dostawców usług płatniczych [polecenia przelewu / polecenia zapłaty]

Dokumenty potwierdzające: Dokument polityki

14.1.2 Czy ta funkcjonalność jest udostępniana w bezpiecznym i zaufanym środowisku?

Ma zastosowanie do: Dostawców usług płatniczych [polecenia przelewu / polecenia zapłaty]

Dokumenty potwierdzające: Dokument polityki

14.2 KK 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.

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

14.2.1 Czy dostawca usług płatniczych posiada procedurę zapewniającą, aby wszelkie szczegółowe wyciągi elektroniczne były udostępniane w bezpiecznym i zaufanym środowisku?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Kodeks praktyki biznesowej

14.2.2 Czy dostawca usług płatniczych posiada procedurę zapewniającą, aby w przypadku informowania klienta 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 były umieszczane w takich wiadomościach lub aby były maskowane?

Ma zastosowanie do: Dostawców usług płatniczych

Dokumenty potwierdzające: Podręcznik praktyki biznesowej

SŁOWNIK POJĘĆ

Poniższe pojęcia zostały zdefiniowane na potrzeby niniejszych Wytycznych oceny.

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 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.