Informator
PCI DSS

Jak bezpiecznie i odpowiedzialnie obsługiwać dane właścicieli kart płatniczych?

Worldline

Spis treści

Wstęp

Zdobyć zaufanie

Zdecydowaliście się Państwo zaoferować swoim klientom możliwość dokonywania płatności kartami kredytowymi i debetowymi, co pomoże Państwu zwiększyć sprzedaż. Klienci są skłonni do wydawania większych sum na zakupy, gdy mogą to zrobić w prosty i bezpieczny sposób. Warto zaznaczyć, że bierzecie Państwo na siebie większą odpowiedzialność, ponieważ klienci ufają, że dane ich kart płatniczych są w Państwa rękach bezpieczne.

Akceptując płatności posiadaczy kart jesteście Państwo odpowiedzialni za bezpieczeństwo danych kart płatniczych.

Dla ułatwienia Państwa pracy, pięć największych organizacji płatniczych opracowało standard bezpieczeństwa, zwany „Payment Card Industry Data Security Standard“ (PCI DSS). W związku z tym, firma może przyjmować płatności kartą jedynie wtedy, gdy spełnia wymagania stawiane przez PCI DSS.

Wymagania te powinni spełniać także dostawcy usług (jak na przykład „Payment Service Providers“ (PSPs) oraz dostawcy terminali płatniczych). Dla zachowania bezpieczeństwa podczas akceptacji transakcji płatniczych konieczna jest współpraca wszystkich uczestników obrotu płatniczego. PCI DSS nakłada na Państwa pewne obowiązki.

Korzyścią jest to, że klienci ufają Państwa firmie i kupują w niej bez wahania. Dodatkowo jest to zabezpieczenie dla klientów przed opłatami i karami pieniężnymi, które mogłyby wyniknąć w przypadku kradzieży lub niewłaściwego wykorzystania informacji o kartach.

W broszurze informacyjnej PaySquare znajdują się ważne informacje o PCI DSS. Dowiecie się Państwo, jak zwiększyć zaufanie klientów do Państwa firmy oraz co należy zrobić, aby spełnić wymagania standardu PCI. Dodatkowo otrzymacie Państwo informacje określające zakres odpowiedzialności w ramach PCI DSS.

Definicja

Czym jest „PCI DSS“?

W celu wdrożenia jasnych ogólnych zasad ochrony informacji o kartach płatniczych, główni dostawcy kart płatniczych opracowali zestaw wytycznych dla wszystkich firm uczestniczących w transakcjach dokonywanych kartami płatniczymi. Wytyczne te zostały połączone w standardzie bezpieczeństwa danych dotyczących kart płatniczych (Payment Card Industry Data Security Standard - PCI DSS).

Niezaszyfrowane numery kart

PCI DSS ma zastosowanie tylko w przypadkach, gdy pełne numery kart płatniczych (Primary Account Numbers - PAN) są zapisywane, przetwarzane, przekazywane lub otrzymywane. Inne informacje dotyczące kart (imię i nazwisko posiadacza karty i data ważności karty) należy chronić tylko wtedy, gdy zapisywane są z odpowiednimi numerami kart. Informacje uwierzytelniające, takie jak kod weryfikacji karty (CVC - Card Validation Code) lub wartość weryfikacji karty (CVV - Card Verification Value), znajdujące się na odwrocie każdej karty kredytowej, oraz kod PIN nie mogą być w żadnym wypadku zapisywane.

Zasadniczo należy zapisywać jak najmniej danych kart. Dane, których nie wolno przechowywać i zapisywać, pokazano na poniższym rysunku, przedstawiającym kartę MasterCard, ale odnoszącym się do wszystkich kart płatniczych.

Które dane kart muszą być chronione?

Wrażliwe dane uwierzytelniające: w żadnym wypadku nie wolno przechowywać następujących informacji:

- informacje pozwalające na śledzenie karty (obszerne dane karty, zapisane np. na pasku magnetycznym 1 i/ lub w układzie scalonym 2);
- trzycyfrowa liczba kontrolna [CVC2, CVV2] na pasku podpisu z tyłu karty 3;
- PIN.

Poniższe informacje karty mogą być przechowywane (jeśli spełniają wymagania PCI-DSS), jeśli jest to konieczne do celów biznesowych:

- PAN (Primary Account Number = pełny numer karty 4);
- imię i nazwisko posiadacza karty 5;
- data ważności karty 6.

Poniższe informacje mogą być przechowywane w formie niezaszyfrowanej, jeśli nie są powiązane z innymi informacjami o posiadaczu karty:

- kwota transakcji, data transakcji i kod autoryzacji transakcji.

Standard podstawowy

PCI DSS stał się podstawowym standardem ochrony informacji o posiadaczach kart. Jego celem jest pomoc firmom w opracowaniu i wdrożeniu skutecznej polityki bezpieczeństwa. Dlatego, aby akceptować karty płatnicze, musisz spełnić wymagania PCI DSS. W ten sposób chronisz swoich klientów i wzmacniasz fundamenty swojej firmy.

Odpowiedzialność

Jeśli nie będziesz właściwie chronić informacji o kartach swoich klientów, ułatwi to oszustom kradzież, nadużycie i ostatecznie spowoduje znaczne szkody. Jesteś odpowiedzialny za wszystkie bezpośrednie straty, które mogą wyniknąć z użycia podrobionych kart płatniczych i/lub kradzieży danych karty. Ponadto ponosisz odpowiedzialność za wszystkie koszty prawne i wszystkie koszty związane z wymianą kart płatniczych, śledztwami i szkodami reputacyjnymi. Ponadto firma wydająca kartę może nałożyć na Ciebie karę i wykluczyć Cię z transakcji kartą płatniczą. Ze względu na odpowiedzialność, zaleca się przestrzeganie wytycznych PCI DSS.

Cele

Do czego służy PCI DSS?

Wprowadzając PCI DSS, dostawcy kart płatniczych nie tylko opracowali pewne zasady. Standard bezpieczeństwa opiera się na całym zestawie jasno sformułowanych celów dla Twojej firmy. Gdy te cele zostaną osiągnięte, klienci mogą korzystać z międzynarodowych kart płatniczych w punkcie sprzedaży lub w sklepie internetowym, aby płacić łatwo, sprawnie i bezpiecznie.

Cele PCI DSS:

1. Stworzenie bezpiecznej sieci płatniczej;
2. Ochrona informacji o posiadaczu karty (kliencie);
3. Opracowanie, utrzymanie i aktualizacja programu, który pozwala wyeliminować luki bezpieczeństwa w systemie płatności;
4. Ograniczenie dostępu do danych karty swoich klientów do koniecznego minimum;
5. Budowa, utrzymywanie i aktualizacja niezawodnej infrastruktury informatycznej;
6. Realizacja celowej i skutecznej polityki bezpieczeństwa informacji.

W jaki sposób osiągnąć cele PCI DSS?

Każde wymaganie PCI DSS wiąże się z szeregiem praktycznych środków, które można wykorzystać do osiągnięcia celów. Jakie działania należy podjąć, zależy od metody, za pomocą której akceptujesz płatności. Możesz również poprosić dostawców (takich jak PSP, dostawca terminali płatniczych, producent oprogramowania itp.) o podjęcie niezbędnych działań.

Wymagania PCI DSS:

Zapewnij bezpieczną sieć płatności

1. Działanie: zainstaluj zaporę i zapewnij jej pełną funkcjonalność.
2. Działanie: nie używaj domyślnych haseł dostarczonych przez dostawcę systemu.

Ochrona informacji o kartach klientów

1. Działanie: zapisz dane karty tylko wtedy, gdy jest to absolutnie konieczne. Jeśli chcesz przechowywać dane do celów biznesowych, musisz się upewnić, że dane są dobrze chronione.
2. Działanie: jeśli korzystasz z sieci publicznych do przesyłania danych kart swoich klientów, musisz zapewnić odpowiednie szyfrowanie.

Rozpoznanie i usunięcie luk w zabezpieczeniach

1. Działanie: korzystaj z oprogramowania antywirusowego i regularnie aktualizuj.
2. Działanie: chroń swoje systemy i aplikacje oraz regularnie aktualizuj zabezpieczenia.

Ograniczenie dostępu

1. Działanie: daj pracownikom dostęp tylko do informacji o kartach, które naprawdę muszą znać.
2. Działanie: nadaj każdemu pracownikowi, który ma dostęp do danych karty, własną nazwę użytkownika i hasło.
3. Działanie: ogranicz fizyczny dostęp do danych kart.

Monitorowanie infrastruktury informatycznej

1. Działanie: kontroluj dostęp do wszystkich krytycznych komponentów struktury informatycznej i danych posiadaczy kart oraz upewnij się, że są one regularnie monitorowane.
2. Działanie: regularnie testuj wszystkie funkcje i procedury bezpieczeństwa.

Bezpieczeństwo informacji

1. Działanie: opracuj politykę opartą na bezpieczeństwie informacji i regularnie sprawdzaj, czy polityka ta jest przestrzegana na co dzień.

Cztery kategorie Akceptanta

Jak należy dostosować się do standardu PCI DSS?

Podczas dostosowywania standardu PCI DSS do przepisów związanych z przechowywaniem danych, uwzględniono również różnice między firmami. Opracowano tym samym cztery kategorie firm. Kategoria, do której można przyporządkować Państwa firmę zależy od liczby oraz metody akceptacji płatności kartami:

- **POS** (= Point of Sales) – płatność dokonana w miejscu sprzedaży; najczęściej poprzez terminal płatniczy.
- **MOTO** (= Mail Order/Telephone Order) – zamówienia za pomocą listu/faksu/telefonu; klient nie jest obecny podczas płatności, dane karty podaje przez telefon/faks.
- **E-Commerce** – zamówienie dokonywane jest przez Internet (online-shop); klient wprowadza dane karty najczęściej za pomocą formularza online.

Kategoria	Charakterystyka	Konieczne środki PCI-DSS
Poziom 1 Wszystkie kanały sprzedaży (POS, E-Commerce, MOTO)	Wszystkie firmy, które akceptują karty płatnicze i zarejestrowały ponad 6 milionów transakcji Visa lub wszystkie firmy, które akceptują karty płatnicze, a które zostały dotknięte przez szkody lub naruszenia ochrony danych (Account Data Compromise, ADC)	Coroczny audyt zgodności poprzez Qualified Security Assessor (QSA dopuszczony przez PCI SSC). W przypadku Visa audyt może zostać przeprowadzony przez uprawnionego pracownika firmy („Internal Security Assessor", ISA). Kwartalne skany networkingowe ze strony Approved Scanning Vendor (ASV), jeśli systemy Akceptanta dostępne są przez Internet
Poziom 2 Wszystkie kanały sprzedaży (POS, E-Commerce, MOTO)	Wszystkie firmy, które akceptują karty płatnicze i zarejestrowały łącznie od 1 miliona do 6 milionów transakcji Visa/MasterCard i Maestro przez wszystkie kanały sprzedaży	**Visa:** Coroczne wypełnienie formularza samooceny (Self Assessment Questionnaire, SAQ) **Mastercard:** Coroczne wypełnienie formularza SAQ poprzez wyspecjalizowanego pracownika (ISA) lub roczny audyt poprzez Qualified Security Assessor (QSA) Kwartalne skany sieci Approved Scanning Vendor (ASV), jeśli systemy Akceptanta dostępne są przez Internet
Poziom 3 Tylko E-Commerce	Wszystkie firmy, które akceptują karty płatnicze w kanale e-commerce i zarejestrowały ponad 20 000 do 1 miliona transakcji rocznie/marka (Visa/MasterCard)	Coroczne wypełnianie formularza samooceny (Annual Self Assessment Questionnaire, SAQ) Kwartalne skany sieci Approved Scanning Vendor (ASV), jeśli systemy Akceptanta dostępne są przez Internet
Poziom 4	Wszystkie inne firmy akceptujące karty płatnicze do 20.000 transakcji e-commerce rocznie/marka lub do 1 miliona transakcji MOTO/POS-transakcji rocznie/marka	Coroczne wypełnienie formularza samooceny (Self Assessment Questionnaire, SAQ) Kwartalne skany sieci Approved Scanning Vendor (ASV), jeśli systemy Akceptanta dostępne są przez Internet

Praktyka (1)

Jak spełnić wymagania PCI DSS?

Na początku stosowania PCI DSS kieruj się zdrowym rozsądkiem. Zanim przeczytasz regulamin, zastanów się, jaki jest cel standardu bezpieczeństwa. Twoje odpowiedzi na to pytanie często stanowią już solidną podstawę Twojego projektu PCI DSS.

Najlepiej zacząć od kwestionariusza samooceny (SAQ)

Kwestionariusz samooceny (Seif Assessment Questionnaire - SAQ) to świetny sposób na rozpoczęcie procedury PCI DSS. Istnieje 5 różnych kwestionariuszy. To, którą ankietę należy użyć, zależy od tego, w jaki sposób akceptujesz płatności kartą. Po przeczytaniu pytań uzyskasz jasny pogląd, jak zabezpieczyć transakcje kartą płatniczą. Jeżeli spełniasz już wymagania, musisz wypełnić kwestionariusz samooceny i przekazać go swojemu agentowi rozliczeniowemu.

Jeśli PCI DSS jest dla Ciebie nowością możesz skontaktować się bezpośrednio z działem obsługi klienta, aby uzyskać hasło, które pozwoli Ci uzyskać dostęp do strony PCI DSS.

Większość firm nie spełnia na początku wszystkich wymagań PCI DSS. Jeśli tak jest i w Twoim przypadku, możesz zacząć podejmować niezbędne działania w swojej organizacji lub powierzyć zewnętrznemu dostawcy pracę nad projektem PCI-DSS. Na stronie internetowej Rady Bezpieczeństwa PCI (PCI Security Standards Council) znajduje się lista wszystkich firm i narzędzi oprogramowania do płatności, które zostały zatwierdzone przez SCC w celu wsparcia projektów PCI DSS.

Praktyczne wskazówki dla udanego projektu PCI DSS

Nie czekaj dłużej, zacznij już dziś!

Im szybciej zaczniesz, tym bardziej zwiększysz przewagę nad konkurencją i tym więcej zaoszczędzisz.

Zapisuj dane tylko wtedy, gdy jest to naprawdę konieczne

Chociaż PCI DSS jest standardem bezpieczeństwa w zakresie zapisywania, przetwarzania i przesyłania danych kart płatniczych, czasami zapisywanie danych karty nie jest konieczne. Dlatego zalecamy sporządzenie listy danych, które chcesz i/lub musisz zapisywać, oraz sprawdzenie, czy może to nastąpić bez Twojej wiedzy. Zwróć przy tym uwagę na następującą, żelazną regułę: „Czego nie potrzebujemy, nie powinniśmy zapisywać".

Sformułuj jasne wytyczne

Jasna polityka postępowania z danymi kart płatniczych zapewnia solidną podstawę działania. Weź przy tym pod uwagę wszystkie obszary zadań: zapisywanie, przetwarzanie i przesyłanie informacji o kartach.

Porównaj przepisy

Już na etapie zapisu informacji o kartach, możesz być zmuszony do przestrzegania pewnych wymogów prawnych nałożonych przez ustawę o ochronie danych Można jednak bardzo wcześnie określić, czy te przepisy spełniają wymagania PCI DSS.

Przeanalizuj odchylenia (Gap Analysis)

Projekt PCI DSS wymaga specjalnej wiedzy. Oznacza to, że musisz sprawdzić, czy Twoja firma dysponuje informacjami potrzebnymi do wypełnienia poszczególnych przepisów. Jeśli tak nie jest, zalecamy skorzystanie z usług zewnętrznych ekspertów w tej dziedzinie.

Porozmawiaj z dostawcami i uzgodnij warunki na piśmie

Jeśli chcesz spełnić wymagania PCI DSS, dostawcy sprzętu i oprogramowania, którzy przetwarzają lub przesyłają dane kart w Twoim imieniu, muszą również przestrzegać przepisów PCI DSS. Ponieważ nie możesz założyć, że Twoi dostawcy spełniają warunki standardu PCI DSS, powinieneś uzgodnić je z nimi na piśmie.

Powinieneś również zażądać potwierdzenia zgodności ze standardem PCI DSS i zawrzeć uzgodnienia w umowie. Możesz również sprawdzić na stronie internetowej PCI Security Standards Council (PCI SSC), czy dostawcy i/lub sprzęt i oprogramowanie zainstalowane w ich systemach zostały zatwierdzone przez SSC.

Skontaktuj się ze swoimi dostawcami

Pod żadnym pozorem nie należy zapisywać danych karty (tj. pełnych danych karty znajdujących się na pasku magnetycznym lub chipie karty płatniczej), ponieważ dane te można względnie łatwo wykorzystać do nielegalnego kopiowania karty. Ponadto nigdy nie należy przechowywać danych autoryzacji i uwierzytelniania, ponieważ niektóre produkty sprzętowe zapisują te dane automatycznie. Zalecamy skontaktowanie się z dostawcą sprzętu i oprogramowania, aby dowiedzieć się, czy tak jest w przypadku systemu terminali płatniczych lub infrastruktury płatności.

Wyszukaj wszystkie istotne dane

Znajdź wszystkie dane, które mogą być istotne dla PCI DSS. Znajdź wszystkie kanały płatności i strumienie danych i utwórz listę wszystkich miejsc, w których mogą znaleźć się informacje o kartach.

Zaszyfruj wszystkie dane kart

Nigdy nie zapomnij zaszyfrować wszystkich przekazywanych danych kart.

Używaj tylko chronionych sieci Wi-Fi

Niezabezpieczone sieci bezprzewodowe nie są odpowiednie do przesyłania informacji o kartach.

Przeszkol swoich pracowników

Nie wszyscy Twoi pracownicy muszą być kwalifikowanymi audytorami zabezpieczeń (PCI Qualified Security Assessors - QSA), jednak muszą wiedzieć, co jest wymagane do spełnienia wymagań PCI DSS.

Sprawdź swoje systemy POS

Systemy punktów sprzedaży (np. połączenie między kasą, terminalem płatniczym i oprogramowaniem do zarządzania) mogą zawierać luki w zabezpieczeniach danych kart. Upewnij się, że w Twoim systemie POS nie są przechowywane kompletne dane kart, szczególnie wartość/kod weryfikacji karty. Nigdy też nie podawaj całego 16-cyfrowego numeru karty kredytowej na paragonach.

Zapewnij fizyczne bezpieczeństwo swoich systemów

Upewnij się, że tylko Twoi upoważnieni pracownicy mają dostęp do Twoich systemów płatności.

Dokumentuj procedurę

Zapisuj działania, które podejmujesz, aby zachować zgodność z przepisami PCI DSS.

Praktyka (2)

Jak można na stałe sprostać wymaganiom PCI DSS?

Jeśli Twoje transakcje płatnicze spełniają te wymagania, możesz być pewien, że wszystkie transakcje będą obsługiwane w sposób bezpieczny i odpowiedzialny dla Ciebie i Twoich klientów. Następnym krokiem jest upewnienie się, że metoda, której używasz w odniesieniu do danych karty płatniczej, będzie nadal spełniać standardowe wymagania w przyszłości.

Praktyczne wskazówki dotyczące utrzymania zgodności ze standardem PCI DSS

Ciągle przypominaj swoim pracownikom

Regularnie rozmawiaj z pracownikami o PCI DSS. Sformułuj jasne i ukierunkowane wytyczne, które mogą zastosować.

Ograniczaj dostęp

Ogranicz dostęp do danych kart. Tylko pracownicy, którzy naprawdę muszą mieć do nich dostęp w celu wykonania swoich zadań powinni mieć nazwę użytkownika i hasło.

Regularnie usuwaj zbędne dane

Regularnie sprawdzaj, jakich danych klientów już nie potrzebujesz i usuwaj te dane natychmiast.

Przygotuj się na najgorsze

Musisz zapewnić, że dane karty Twojego klienta nie doznają szkody i bądź przygotowany na taką ewentualność. Zastanów się, co ty i Twoi pracownicy musicie zrobić, kiedy taka sytuacja ma miejsce, i opracuj scenariusze kryzysowe.

Przeprowadzaj regularne kontrole

Regularnie sprawdzaj zabezpieczenia systemu i protokoły testowe.

Wspólnie zapobiegajmy oszustwom

Gdzie się zaczyna i kończy Twoja odpowiedzialność?

Korzystanie z kart płatniczych jest łatwe i bezpieczne. Twoi klienci polegają na użyciu zastrzeżonych systemów technicznych i sprzętu oraz współpracują z zaufanymi partnerami i dostawcami w celu obsługi transakcji płatniczych.

Dostawcy kart korzystają z PCI DSS, aby jak najlepiej zabezpieczyć dane kart klientów. Twoja odpowiedzialność za bezpieczeństwo tych informacji dotyczy następujących aspektów transakcji płatniczych:

- sprzęt używany do skanowania kart kredytowych i innych kart płatniczych używanych przez klientów;
- terminale płatnicze używane w Twoich sklepach (lub systemach POS):
- sieci i sprzęt używany w transakcjach płatniczych (np. serwery, routery bezprzewodowe, modemy itd.);
- zapisywanie, przetwarzanie i przesyłanie informacji o karcie płatniczej;
- ochrona sprzętu i oprogramowania wszystkich stron zaangażowanych w Twoje transakcje płatnicze i fizyczny dostęp do ważnych komponentów systemów informatycznych i danych posiadaczy kart.

Twoi dostawcy mają własne standardy bezpieczeństwa

Oczywiście nie jesteś jedyną firmą odpowiedzialną za ochronę transakcji płatniczych. Inne zaangażowane firmy również odgrywają rolę i muszą być zgodne ze standardem PCI DSS. Na przykład potrzebujesz terminala płatniczego lub kasy fiskalnej i oprogramowania do płatności.

Jednak dla producentów i dostawców terminali płatniczych, a także dla dostawców oprogramowania płatniczego, opracowano różne standardy bezpieczeństwa. Zgodnie z wymogami PCI DSS, zawsze należy używać terminala płatniczego lub aplikacji, która spełnia te standardy i wybrać dostawcę oprogramowania, który też je spełnia. Lista zatwierdzonych dostawców, w tym dostawców aplikacji do płatności, znajduje się na stronie pcisecuritystandards.org.

PCI DSS i co dalej?

Jeśli spełniasz wymagania PCI DSS, znacząco przyczynisz się do bezpieczeństwa Twoich danych, które są tak ważne dla Twoich klientów. Fakt, że programy kartowe mają standard bezpieczeństwa nie oznacza, że nie istnieją inne (prawne) regulacje. Na przykład zapisując, przetwarzając i przesyłając informacje o kartach swoich klientów, musisz także przestrzegać wytyczne ustawy o ochronie danych (Mimo że zgodnie z prawem wymagane jest zarządzanie danymi klientów, może być konieczne na przykład nałożenie ograniczeń dotyczących wykorzystywania danych klientów do celów biznesowych.

Jakie przypadki oszustwa mogą wystąpić?

Oszustwo ma wiele twarzy, a każda metoda akceptowania kart płatniczych ma swoje własne ryzyka i środki, które je zmniejszają. Broszura informacyjna Worldline o oszustwach przy użyciu kart kredytowych i międzynarodowych kart płatniczych zawiera również informacje o tym, jak wykrywać oszustwa i co można zrobić, aby im zapobiec. W ramach informacji PCI DSS przedstawimy Ci różne możliwe przypadki oszustwa, które mogą wystąpić.

W przypadku niezależnego terminala płatniczego w punkcie sprzedaży

Nawet jeśli kasa i terminal płatniczy nie są połączone w punkcie sprzedaży, istnieje ryzyko, że sam terminal płatniczy lub połączenie transmisji danych zostanie naruszone. Umożliwi to oszustom przechwytywanie danych kart i/lub transakcji Twoich klientów.

Jak możesz temu zapobiec?

Okresowo (najlepiej codziennie rano) sprawdzaj terminal płatniczy i link komunikacyjny pod kątem manipulacji. Jeśli podejrzewasz, że Twój terminal płatniczy i/lub Twoje połączenia i/lub kable zostały naruszone, skontaktuj się z dostawcą, który pomoże Ci rozwiązać problem.

W przypadku terminala płatniczego w punkcie sprzedaży, połączonego z kasą

Jeśli Twój kasa fiskalna i terminal płatniczy są połączone, link komunikacyjny i/lub oprogramowanie do płatności mogą zostać zhakowane. Umożliwiłoby to oszustom uzyskanie dostępu do informacji kart przechowywanych w systemie i dodanie do nich złośliwego oprogramowania.

Jak możesz temu zapobiec?

Zastosuj odpowiedni system bezpieczeństwa i skuteczną metodę szyfrowania transmisji danych.

W przypadku zintegrowanego terminala płatniczego w punkcie sprzedaży

Łącza komunikacyjne mogą zostać zhakowane, nawet jeśli używasz zarówno terminala płatniczego, jak i kasy fiskalnej. Ponieważ te urządzenia są używane głównie przez firmy z wieloma oddziałami, połączenia między oddziałami a główną siedzibą mogą zostać zhakowane.

Jak możesz temu zapobiec?

Ustal szereg jasnych reguł ze swoim dostawcą usług informatycznych i upewnij się, że jego produkty rzeczywiście spełniają wymagania PCI SSC.

W przypadku sklepu internetowego, który korzysta ze strony płatności dostawcy usług płatniczych

Wiele firm e-commerce używa strony płatności dostawcy usług płatniczych do obsługi płatności kartą. Nawet dostawcy usług płatniczych muszą regularnie sprawdzać, czy ich metody spełniają wymagania PCI DSS, ale ostatecznie odpowiadasz za to Ty. Jeśli strona płatności Twojego dostawcy usług płatności nie została poprawnie skonfigurowana i nadal zapisuje dane karty, może to mieć katastrofalne skutki dla Twoich klientów.

Jak możesz temu zapobiec?

Umowa z dostawcą usług płatności musi zawierać postanowienie, że strona płatności zawsze spełnia wymagania PCI DSS. Musisz wdrożyć kompleksowe systemy bezpieczeństwa, takie jak oprogramowanie antywirusowe i zapory; Jeśli tego nie zrobisz, Twój sklep internetowy będzie narażony na ataki hakerskie.

W przypadku sklepu internetowego z własną stroną płatności

Firmy e-commerce z własnymi stronami płatności są narażone na bardzo wysokie ryzyko.

Jak możesz temu zapobiec?

Wielu agentów rozliczeniowych nie akceptuje firm e-commerce z własnymi stronami płatności (tzn. stronami płatności, które nie pochodzą od dostawcy usług płatniczych). Najlepiej zatem skorzystać ze strony płatności dostawcy usług płatności, która spełnia wymagania PCI DSS, aby w ten sposób, w jak największym stopniu zapobiec oszustwom i zagrożeniom bezpieczeństwa.

Akceptacja kart kredytowych w sprzedaży zdalnej (MO/TO)

Jeśli otrzymujesz zamówienia telefonicznie lub drogą pocztową (MO/TO), możesz otrzymać dane karty manualnie przez dostawcę usług płatności wybieranego przez Worldline, ale tylko pod pewnymi, określonymi warunkami. Ryzykujesz dane swoich klientów, przechowując dane kart lub komunikując się z klientami za pośrednictwem poczty e-mail (lub strony internetowej).

Jak możesz temu zapobiec?

Nie zapisuj informacji o kartach kredytowych swoich klientów i odpowiednio szyfruj dane wysyłane w komunikacji z klientami odnośnie zamówień.

Wyjaśnienie

Nieporozumienia dotyczące PCI DSS

Istnieje szereg powszechnych nieporozumień dotyczących bezpieczeństwa danych kart i PCI DSS. Poniżej wyjaśniamy niektóre z nich.

Nieporozumienie 1

PCI DSS to zalecenie, a nie wymóg.

Dostawcy kart płatniczych mogą decydować, w jaki sposób, powinieneś przetwarzać dane karty jako firma. Oznacza to, że musisz spełniać wymagania PCI DSS, aby mieć możliwość akceptowania płatności kartą.

Nieporozumienie 2

Kontrola przeprowadzana przez ASV to jedyny wymóg zgodności PCI DSS.

Kontrola bezpieczeństwa, przeprowadzana przez uprawnioną firmę kontrolującą jest tylko częścią procesu PCI DSS. Jednak jako firma zazwyczaj musisz również przesłać wypełniony roczny kwestionariusz samooceny (Seif Assessment Questionnaire). Na stronie www.paysquare.pl dowiesz się, jakie warunki Worldline nakłada na akceptantów.

Nieporozumienie 3

Akceptuję tak mało płatności kartą, że nie muszę spełniać wymagań PCI DSS.

Nawet jeśli otrzymasz tylko jedną płatność kartą, Twoja firma musi spełniać przepisy PCI DSS.

Nieporozumienie 4

Ponieważ nie zapisuję danych kart moich klientów, przepisy PCI DSS nie dotyczą mnie.

PCI DSS to standard bezpieczeństwa zapisywania, przetwarzania i przesyłania danych kart: oznacza to, że musisz spełnić większość wymagań PCI DSS. Jesteś absolutnie pewien, że nie zapisujesz żadnych danych kart?

Nieporozumienie 5

Małe firmy nigdy nie są karane przez dostawców kart płatniczych.

Gdy dane karty zostaną skradzione z Twojej firmy, musisz być w stanie udowodnić, że spełniałeś wymagania PCI DSS w momencie kradzieży. Jeśli się nie uda, zostaniesz pociągnięty do odpowiedzialności za wszelkie poniesione straty, niezależnie od wielkości firmy. Ponadto możesz zostać wykluczony z przyjmowania płatności kartą, a nawet przypisany do wyższej kategorii handlowców (patrz tabela na stronie 8) z bardziej rygorystycznymi wymaganiami i wyższymi opłatami kontrolnymi.

Nieporozumienie 6

PCI DSS dotyczy tylko e-commerce.

Wszystkie firmy, które zapisują, przetwarzają i/lub przesyłają dane kart, muszą spełniać wymagania PCI DSS. Dotyczy to również punktów sprzedaży (tj. sklepów) oraz firm, które przyjmują zamówienia pocztą lub telefonicznie (MO/TO).

Nieporozumienie 7

Wypełnienie i złożenie kwestionariusza samooceny (Seif Assessment Questionnaire) kończy procedurę PCI-DSS.

Ponieważ informacje, które podajesz w kwestionariuszu SAQ, mogą się zmieniać z czasem, musisz spełnić wymagania PCI DSS także po przesłaniu kwestionariusza. W przypadku problemu z danymi kart płatniczych, musisz być w stanie udowodnić zgodność z PCI DSS w danym okresie.

Nieporozumienie 8

PCI DSS daje dużą swobodę interpretacji.

PCI DSS to najbardziej precyzyjny zbiór wymagań bezpieczeństwa, które do tej pory wydała branża. W przeciwieństwie do innych standardów związanych z bezpieczeństwem (takich jak SOX, ISO i ISO 27002), PCI DSS to więcej niż struktura szkieletowa, ponieważ zawiera również szczegółowy opis powiązanych wymagań i procedur.

Nieporozumienie 9

Wystarczy mieć aplikację z certyfikatem PA-DSS, aby spełnić wymagania PCI DSS.

Korzystanie z certyfikowanej aplikacji PA-DSS to tylko pierwszy krok. Potem musisz przestrzegać wszystkich przepisów i wdrożyć systemy kontroli, które zapewniają, że wszystkie Twoje sieci i serwery spełniają wymagania PCI DSS. Jeśli powierzyłeś innym firmom administrowanie systemem, ich administratorzy muszą spełnić te wymagania.

Terminologia

Pojęcia PCI DSS

Agent rozliczeniowy („Acquirer“)

Agenci rozliczeniowi odpowiadają za uregulowanie płatności kartami dla danej firmy. W tym celu zawierają umowę licencyjną z międzynarodowym dostawcą kart.

Poświadczanie zgodności (AoC)

Ten dokument jest dowodem, że wypełniłeś kwestionariusz SAQ poprawnie i zgodnie z prawdą.

Uprawniona firma kontrolująca (ASV)

ASV przeprowadzają kontrole w firmach, które akceptują karty płatnicze w celu sprawdzenia ich systemów i sieci informatycznych. ASV muszą być certyfikowane przez Radę Bezpieczeństwa PCI.

Listę zatwierdzonych firm można znaleźć na stronie internetowej Rady Bezpieczeństwa PCI pod adresem www.pcisecuritystandards.com.org. Większość systemów i sieci informatycznych musi być sprawdzana co trzy miesiące, co zwykle można wykonać zdalnie. Ta procedura jest podobna do skanowania antywirusowego.

Certyfikacja

W ramach procesu certyfikacji, jednostka certyfikująca sprawdza, czy firma spełnia określone przepisy i wymagania w momencie certyfikacji.

Zgodność

Jest to spełnienie i/lub postępowanie zgodnie z niektórymi ustawami i/lub przepisami.

Manipulacja

Są to manipulacja, kradzież i utrata danych i/lub systemów lub wpływ na nie w celu ich niewłaściwego użycia.

Dostawca usług płatności (PSP)

Dostawcy usług płatności mają za zadanie ułatwienie technicznego połączenia między firmą a agentem rozliczeniowym oraz przeprowadzanie transakcji kartowych. Ponadto dostawcy usług płatniczych oferują inne produkty i usługi w zakresie rozliczania całej gamy płatności elektronicznych.

PCI DSS

Jest to zbiór przepisów wydanych przez głównych dostawców kart płatniczych (w tym Visa i MasterCard), których celem jest zapobieganie niewłaściwemu użyciu kart płatniczych. Wszystkie strony uczestniczące w łańcuchu transakcji kart płatniczych (takie jak firmy, agenci rozliczeniowi, dostawcy usług płatniczych i dostawcy usług informatycznych) muszą spełniać wymagania PCI.

Kwalifikowany audytor zabezpieczeń (QSA)

To ekspert ds. bezpieczeństwa informatycznego, upoważniony przez PCI SCC do przeprowadzania kontroli bezpieczeństwa (OnSite Assessments) w firmach akceptujących karty i przetwarzających dane kart.

Rozwiązanie „bezpieczna przystań“

Jeśli detalista pada ofiarą kradzieży/oszustwa, mimo zgodności z PCI DSS, wystawca karty płatniczej może w pewnych okolicznościach obniżyć karę pieniężną, którą nałożył by w przeciwnym razie zapłacić, lub zupełnie z niej zrezygnować.

Kontrola bezpieczeństwa

Jest to audyt bezpieczeństwa fizycznego przeprowadzany na terenie firmy, który obejmuje inspekcję pomieszczeń serwerowych i rozmowy z pracownikami.

Skan bezpieczeństwa

Jest to badanie mające na celu ujawnienie słabych punktów infrastruktury informatycznej lub konfiguracji systemu. Skany bezpieczeństwa są zwykle wykonywane online.

Kwestionariusz samooceny (SAQ)

Kwestionariusze samooceny (SAQ) to ankiety, za pomocą których firmy przekazują swoim agentom rozliczeniowym informacje o wdrożeniu przepisów PCI DSS w firmie. Każda kategoria firmy ma swój własny kwestionariusz. Ankiety zawierają informacje o przyjętej przez firmę metodzie akceptowania i przetwarzania transakcji płatności kartą, przetwarzania ogólnych informacji biznesowych, relacjach (w tym stosunkach umownych) z innymi firmami oraz szczegółach technicznych. Jeżeli należą one do odpowiedniej kategorii handlowców (informacje na temat każdej kategorii znajdują się na stronie 9), firmy muszą raz w roku wypełnić i przekazać SAQ agentowi rozliczeniowemu.

Więcej informacji na stronie

www.paysquare.pl

lub na którejkolwiek z poniższych stron.

www.visa.com

www.mastercard.com

www.pcisecuritystandards.org

Dane kontaktowe

Chcesz dowiedzieć się więcej? Skontaktuj się z nami! Chętnie odpowiemy na każde pytanie.

Tel.: +48 22 646 11 99

Email: info@pl.paysquare.eu

Treść niniejszej broszury ma charakter wyłącznie informacyjny i nie ponosimy żadnej odpowiedzialności za błędy lub pominięcia. Informacje pochodzą ze źródeł udostępnianych publicznie. Zastrzega się błędy w druku.

Jako profesjonalny partner w transakcjach płatniczych, informujemy niezależnie i obiektywnie o transakcjach płatniczych za pomocą publikowanych broszur informacyjnych. W broszurach tych przedstawiamy rozwiązania szeregu problemów związanych z określonymi wymaganiami rynkowymi. Wszystkie nasze broszury informacyjne i inne materiały można pobrać na stronie www.paysquare.

PaySquare SE
a Worldline Company
Oddział w Polsce
ul. Puławska 182
02-670 Warszawa

Telefon: +48 22 646 11 99
Fax: +48 22 646 11 98
E-mail: info@pl.paysquare.eu
www.paysquare.pl