Przewodnik dla firm przyjmujących płatności bezgotówkowe

Standard Bezpieczeństwa Danych w Branży Kart Płatniczych (PCI DSS)

Elavon

secured BY ELAVON

Spis treści

Elavon

01

Naruszenie bezpieczeństwa danych kartowych - realne zagrożenie

Pojedyncza karta płatnicza jest warta na czarnym rynku* ok. 0.50-100 USD – dlatego hakerzy biorą na cel duże bazy danych lub małe firmy, które nie mają odpowiedniego zabezpieczenia przed atakiem

W 2016 r. 40% informacji utraconych wskutek naruszenia bezpieczeństwa danych stanowiły Osobiste Informacje Finansowe, w tym dane z kart kredytowych, debetowych lub bankowe rejestry finansowe.*

*Symantec Internet Security Threat Report, 2017

Hakerzy pragną pozyskać dane posiadaczy kart. Oszust może udawać posiadacza karty, korzystać z jego karty i kraść jego tożsamość.

Przypadki naruszenia bezpieczeństwa danych kartowych lub kradzieży karty i tożsamości mają wpływ na całe środowisko funkcjonowania kart płatniczych. Klienci mogą stracić zaufanie do firm przyjmujących płatności kartowe lub instytucji finansowych. Konsekwencje mogą być jednak dużo poważniejsze:

- Spadek sprzedaży i utrata reputacji
- Straty wynikające z oszustwa
- Koszty prawne, ugody i wyroki
- Kary i grzywny
- Brak możliwości dalszego akceptowania kart płatniczych
- Utrata pracy (dyrektor ds. bezpieczeństwa IT, dyrektor generalny i osoby na podległych im stanowiskach)
- Wycofanie się z biznesu

Elavon

02

O bezpieczeństwie płatności

Aby zapewnić bezpieczeństwo płatności i rozwiązać problem naruszania danych kartowych, organizacja kartowe: Visa, Mastercard, JCB, Amex i Discover opracowały Standard Bezpieczeństwa Danych w Branży Kart Płatniczych (PCI DSS).

Standard ten rekomenduje firmom przyjmującym płatności kartowe najlepsze praktyki w zakresie metod i sposobów zarządzania, przesyłania, przechowywania oraz przetwarzania danych kartowych.

Każda firma przyjmująca płatności kartowe ma obowiązek stosować się do tych standardów i udokumentować, że korzysta z odpowiednich zabezpieczeń, aby zapewnić bezpieczeństwo danych kartowych klientów. Jeśli nie spełnia tych warunków, a dojdzie do naruszenia bezpieczeństwa danych, może podlegać surowym grzywnom.

03

Co to jest PCI DSS?

Standard Bezpieczeństwa Danych w Branży Kart Płatniczych (PCI DSS) jest zbiorem technicznych i operacyjnych wymogów, które opracowała Rada ds. Standardów Bezpieczeństwa w Branży Kart Płatniczych (PCI SSC), aby chronić dane posiadaczy kart.

Standardy te powinny spełniać wszystkie firmy, które przechowują, przetwarzają lub przesyłają dane kartowe oraz firmy, które opracowują oprogramowanie aplikacji, a także producenci urządzeń wykorzystywanych przy transakcjach wykonywanych kartami płatniczymi.

Rada ds. PCI DSS odpowiada za utrzymanie standardu. Zgodność z nim egzekwują jej członkowie-założyciele, tj. American Express, Discover Financial Services, JCB, MasterCard i Visa Inc.

Jeżeli Twoja firma akceptuje lub przetwarza płatności kartowe, powinna uzyskać certyfikat zgodności ze standardem PCI DSS.

Elavon

04

12 wymogów standardu PCI DSS

Standard PCI DSS odnosi się do wszystkich technicznych i operacyjnych elementów transakcji kartowej, które zawierają dane posiadacza karty lub są z nimi powiązane. Oznacza to, że Twoje sklepowe terminale płatnicze, kasy, sieci, procesy płatnicze, a także – jeśli prowadzisz sprzedaż internetową – Twoja lokalna i rozległa sieć komputerowa, linie telefoniczne oraz bramki, podlegają wymogom standardu PCI DSS.

Na standard PCI DSS składa się 12 wymogów:

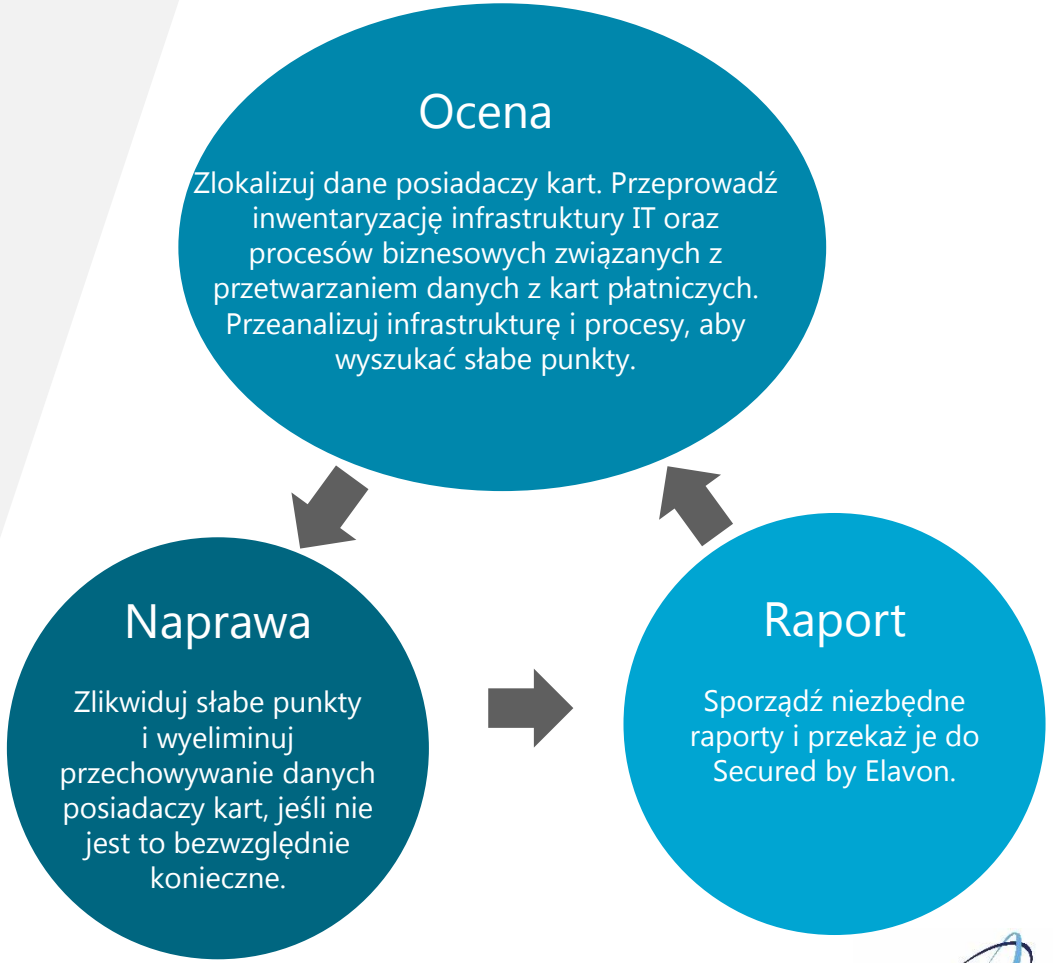
Cele	Wymagania PCI DSS
Budowa i utrzymanie bezpiecznej sieci	1. Instalacja i utrzymanie konfiguracji zapory sieciowej w celu ochrony danych posiadaczy kart płatniczych 2. Zmiana ustawień domyślnych operatora dotyczących haseł systemowych i innych parametrów bezpieczeństwa
Ochrona danych posiadaczy kart płatniczych	3. Ochrona przechowywanych danych posiadaczy kart płatniczych 4. Szyfrowanie transmisji danych posiadaczy kart w otwartych, publicznych sieciach komputerowych
Utrzymywanie programu zarządzającego podatnością na ataki	5. Ochrona wszystkich systemów przed atakiem wirusów oraz regularna aktualizacja oprogramowania antywirusowego 6. Budowa i utrzymanie bezpiecznych systemów i aplikacji
Wdrożenie skutecznych metod kontroli dostępu	7. Ograniczenie dostępu do danych posiadaczy kart płatniczych w zależności od potrzeb związanych z informacją handlową 8. Identyfikacja i autoryzacja dostępu do komponentów systemu 9. Ograniczenie fizycznego dostępu do danych posiadaczy kart płatniczych
Regularne monitorowanie i testowanie sieci komputerowych	10. Śledzenie i nadzorowanie wszystkich prób dostępu do zasobów sieciowych oraz danych posiadaczy kart płatniczych 11. Regularne testowanie systemów i procesów związanych z bezpieczeństwem
Utrzymanie instrukcji dotyczącej bezpieczeństwa informacji	12. Utrzymanie instrukcji dotyczącej bezpieczeństwa informacji dla całego personelu

05

Utrzymanie zgodności ze standardem PCI DSS to ciągły proces

Standard PCI DSS został stworzony po to, by zmniejszyć liczbę oszustw dotyczących kart kredytowych. Jest to możliwe dzięki zabezpieczeniu danych posiadacza karty metodą 360°.

Zakłada ona, że dane posiadacza karty są monitorowane przez cały czas. Dlatego ich ochrona jest ciągłym procesem i nie sprowadza się tylko do corocznego testu sprawdzającego. Realizacja standardu obejmuje następujące procedury kontrolne:



Elavon

06

PCI DSS - jakiej walidacji podlega Twoja firma?

W zależności od tego, ile transakcji wykonywanych kartami Visa lub Mastercard przyjmuje i przetwarza w ciągu 12 miesięcy Twoja firma, zostaje ona zakwalifikowana do jednego z czterech poziomów. Firmy należące do danego poziomu obowiązuje określona walidacja: na czym ona polega i jakiego rodzaju raportowanie jest konieczne przedstawia tabela obok.

Poziom	Jakie kryteria kwalifikacji powinna spełnić Twoja firma	Na czym polega walidacja na danym poziomie
Poziom 1	Ponad 6 milionów transakcji wykonanych kartami Visa lub MasterCard przetworzonych w danym roku.	Coroczna weryfikacja na terenie klienta, którą przeprowadza Qualified Security Assessor, oraz pozytywny wynik skanu sieci, który wykonuje approved scanning vendor (ASV), jeżeli skanowanie jest konieczne.
Poziom 2	Od miliona do 6 milionów transakcji wykonanych kartami Visa lub MasterCard przetworzonych w danym roku.	Coroczne wypełnienie Kwestionariusza Samooceny (SAQ) oraz pozytywny wynik skanu sieci, który wykonuje ASV, jeżeli skanowanie jest konieczne.
Poziom 3	Od 20.000 do miliona transakcji e-commerce wykonanych kartami Visa lub MasterCard przetworzonych w danym roku.	Coroczne wypełnienie SAQ oraz skan sieci za pomocą skanu zatwierdzonego przez ASV, jeżeli jest to konieczne.
Poziom 4	Mniej niż milion transakcji kartami Visa lub MasterCard przetworzonych w danym roku oraz poniżej 20.000 transakcji e-commerce.	Coroczne wypełnienie SAQ oraz skan sieci za pomocą skanu zatwierdzonego przez ASV.

Elavon

07

Jakie wsparcie w zakresie PCI DSS oferujemy klientom?

Wspieramy wszystkich naszych klientów w uzyskaniu zgodności ze standardem PCI DSS, niezależnie od poziomu, do którego została zakwalifikowana Twoja firma, i jej wielkości; bez względu na to, czy jesteś naszym nowym klientem: dostawcą usług płatniczych, bramek płatności lub przetwarzasz dane, czy też dopiero zaczynasz swoją przygodę z akceptowaniem kart.
Jako autoryzowany usługodawca w zakresie PCI DSS pomagamy na kilka sposobów:

Śledzenie i monitorowanie programów zgodności z PCI DSS dla klientów poziomów 1-4 – jako dostawca usług płatniczych mamy obowiązek zapewnić, że nasi klienci utrzymują zgodność ze standardem PCI DSS, a także składać Organizacjom Kartowym stosowne raporty.

Wparcie – jeśli jesteś klientem korporacyjnym, korzystasz z osobistych konsultacji i doradztwa: współpracujemy, aby zrozumieć działalność Twojej firmy i wypracować dla niej indywidualne plany w zakresie zgodności ze standardami PCI DSS. Jeśli należysz do małych i średnich klientów biznesowych, korzystasz ze specjalnego portalu, za pomocą którego samodzielnie uzyskujesz certyfikat zgodności ze standardem PCI DSS.

Wiedza branżowa i ekspercka – jako klient Elavon masz dostęp do ogromnych zasobów produktów zabezpieczających i PCI Qualified Security Assessors oraz możesz kontaktować się z ekspertami, którzy są na bieżąco z najnowszymi trendami w branży płatności.

Elavon

08

Kto jest kim w procesie PCI DSS i jakie ma obowiązki?

PCI SSC jest organem, który opracowuje i utrzymuje PCI DSS.

Jeśli Twoja firma akceptuje płatności kartowe, masz obowiązek co roku dostarczać Twojemu dostawcy usług płatniczych jeden Raport dot. Zgodności (ROC) lub Kwestionariusz Samooceny (SAQ) oraz przez cały czas utrzymywać zgodność ze standardami PCI DSS.

Dostawcy usług płatniczych informują firmy akceptujące płatności o standardzie PCI DSS i obowiązkach z nim związanych. Zbierają oni również informacje na temat statusu tych firm w zakresie PCI DSS i przekazują je Organizacjom Kartowym.

Organizacje Kartowe odpowiadają za programy, których muszą przestrzegać firmy akceptujące płatności. Dane kartowe otrzymują bezpośrednio od dostawców usług płatniczych, a nie od firm akceptujących płatności.

Qualified Security Assessors (QSA) zapewniając techniczne wytyczne i instrukcje, pomagają klientom poziomu 1 i 2 uzyskać pełną zgodność ze standardem PCI DSS, tak aby mogli oni wypełnić SAQ. **QSA** mogą także tworzyć ROC, aby potwierdzić status danej firmy w zakresie zgodności ze standardem PCI DSS.

Approved Scanning Vendors (ASV) przeprowadzają skany bezpieczeństwa PCI przez Internet – pomagają one zidentyfikować słabe punkty stron internetowych, aplikacji i infrastruktury IT.

Elavon

09

Ogólne rozporządzenie o ochronie danych (RODO)

Więcej informacji dotyczących RODO:
http://ec.europa.eu/justice/data-protection/index_en.htm

Rozporządzenie o ochronie danych osobowych (RODO) wchodzi w życie we wszystkich krajach Unii Europejskiej w maju 2018 roku. Tak więc, niezależnie od wielkości Twojej firmy, jeżeli przeprowadzasz transakcje z klientami na terytorium UE lub część Twojej działalności jest prowadzona na terenie UE, postanowienia tego rozporządzenia będą Cię dotyczyć.

PCI DSS może zapewnić ramowe informacje pomocne w realizacji celów RODO. Standard PCI DSS dotyczy danych posiadaczy kart, natomiast RODO reguluje kwestie dotyczące wszystkich danych osobowych.

Miej na uwadze, że naruszenie bezpieczeństwa danych lub brak jego zgłoszenia w ciągu 72 godzin podlega karze grzywny w wysokości do 20 milionów euro lub 4% Twoich obrotów (w zależności od tego, która z tych kwot jest wyższa). Jeżeli naruszenie dotyczy danych posiadacza karty, Rada PCI może nałożyć dodatkowe grzywny.

Elavon

10

Podstawowe informacje do realizacji celów RODO

Dzięki zmianie jednego słowa w zapisie 12 głównych wymagań standardu PCI DSS możesz zobaczyć, co trzeba zrobić, aby zapewnić zgodność z RODO.

Cele	Wymagania standardu PCI DSS
Budowa i utrzymanie bezpiecznej sieci	1. Instalacja i utrzymanie konfiguracji zapory sieciowej w celu ochrony danych **OSOBOWYCH** 2. Zmiana ustawień domyślnych operatora dotyczących haseł systemowych i innych parametrów bezpieczeństwa
Ochrona danych posiadaczy kart płatniczych	3. Ochrona przechowywanych danych **OSOBOWYCH** 4. Szyfrowanie transmisji danych **OSOBOWYCH** w otwartych, publicznych sieciach komputerowych
Utrzymywanie programu zarządzającego podatnością na ataki	5. Ochrona wszystkich systemów przed atakiem wirusów oraz regularna aktualizacja oprogramowania antywirusowego 6. Budowa i utrzymanie bezpiecznych systemów i aplikacji
Implementacja skutecznych metod kontroli dostępu	7. Ograniczenie dostępu do danych **OSOBOWYCH** płatniczych w zależności od potrzeb związanych z informacją handlową 8. Identyfikacja i autoryzacja dostępu do komponentów systemu 9. Ograniczenie fizycznego dostępu do danych **OSOBOWYCH**
Regularne monitorowanie i testowanie sieci komputerowych	10. Śledzenie i nadzorowanie wszystkich prób dostępu do zasobów sieciowych oraz danych **OSOBOWYCH** 11. Regularne testowanie systemów i procesów związanych z bezpieczeństwem
Utrzymanie instrukcji dotyczącej bezpieczeństwa informacji	12. Utrzymanie instrukcji dotyczącej bezpieczeństwa informacji dla całego personelu

11

Dalsze kroki

Twoja firma ma obowiązek uzyskać zgodność ze standardem PCI DSS, a my mamy obowiązek pomóc Ci w tym, zawsze gdy jest to możliwe.

Niezależnie od tego, czy Twoja firma ma już pełną zgodność ze standardem PCI DSS, pracujesz nad jej uzyskaniem, czy też słyszysz o tym standardzie po raz pierwszy, pomożemy Ci podjąć dalsze kroki.

Co muszę zrobić jako firma akceptująca płatności, jeśli...	Dalsze kroki Poziomy 1-3	Dalsze kroki Poziom 4
"Nigdy nie słyszałem o zgodności ze standardem PCI i nie wiem jakie wiążą się z tym obowiązki."	Skontaktuj się z Konsultantem Elavon ds. Bezpieczeństwa Danych – przeprowadzi Cię on przez cały proces.	Skontaktuj się z Przedstawicielem ds. Sprzedaży w Elavon lub wyślij email na adres: elavonpci@elavon.com
"Pracuję/pracujemy nad zapewnieniem zgodności z PCI"	Prześlij dokumentację swoich postępów do Konsultanta Elavon ds. Bezpieczeństwa Danych.	Zaloguj się do portalu Secured by Elavon i zaktualizuj swoje dane, aby odzwierciedlały Twój obecny status.
"Moja firma uzyskała zgodność ze standardem PCI"	Prześlij do Konsultanta Elavon ds. Bezpieczeństwa Danych dowód statusu zgodności Twojej firmy, który spełnia wymogi walidacji na danym poziomie.	Załaduj Certyfikat zgodności do portalu Secured by Elavon.

Elavon

Masz pytania?

Skontaktuj się z nami, by uzyskać dalsze informacje na temat zgodności ze standardem PCI DSS oraz bezpieczeństwa danych:

Klienci poziomu 4

Obsługa klienta
+48 22 306 0316

Secured by Elavon
+48 22 307 1833
helpdesk@elavonsecuritymanager.com

Klienci korporacyjni poziomu 1-2 oraz 3

PCIEurope@elavon.com

Zgłoś przypadek naruszenia:

ADCqueries-EU@elavon.com

Elavon Financial Services Designated Activity Company (Spółka z Ograniczoną Odpowiedzialnością o Wyznaczonym Przedmiocie Działalności) Oddział w Polsce z siedzibą w Warszawie, ul. Puławska 17, 02-515 Warszawa, zarejestrowany w rejestrze przedsiębiorców Krajowego Rejestru Sądowego prowadzonym przez Sąd Rejonowy dla m.st. Warszawy w Warszawie, XIII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 287836, numer REGON 300649197, NIP 2090000825, kapitał zakładowy Elavon Financial Services Designated Activity Company 6.400.001,00 euro.
Elavon Financial Services DAC prowadzi działalność gospodarczą pod nazwą Elavon Merchant Services i podlega nadzorowi Centralnego Banku Irlandii.