WORLDLINE

Payments to grow your world

Wskazówki dla akceptantów dot. przestrzegania zasad bezpieczeństwa zgodnie ze standardem PCI DSS.

Na całym świecie wszyscy akceptanci, którzy przesyłają, przetwarzają lub przechowują dane kart płatniczych, zobowiązani są do przestrzegania dyrektyw bezpieczeństwa zdefiniowanych w standardzie PCI DSS (Payment Card Industry Data Security Standard – Standard bezpieczeństwa przetwarzania danych posiadaczy kart płatniczych). W przypadku nieprzestrzegania tych zasad firma Worldline jest uprawniona do rozwiązania umowy ze skutkiem natychmiastowym i może dochodzić odszkodowania za ewentualne kary i roszczenia.

Następujące wskazówki stanowią techniczne i organizacyjne dyrektywy, które są wiążące dla każdej części umowy z firmą Worldline.

Co zawiera standard PCI DSS?

Standard PCI DSS obejmuje 12 wiążących wymogów, które pomagają zapewnić ochronę informacji pochodzących z kart płatniczych podczas przetwarzania, przechowywania i przesyłania. Wdrożenie standardu PCI DSS jest sterowane za pomocą programów bezpieczeństwa organizacji kart płatniczych. Do tych programów zaliczamy program AIS organizacji Visa, SDP organizacji Mastercard, jak i odpowiednie programy takich organizacji jak American Express, Discover (Diners Club) i JCB.

Dlaczego wprowadzono standard PCI DSS?

W ostatnich latach zwiększyła się liczba kradzieży danych kart płatniczych. Bezprawne użycie skradzionych informacji pochodzących z kart płatniczych wyrządza znaczące szkody u wszystkich zainteresowanych stron.

Czemu służy standard PCI DSS?

Organizacje kart płatniczych za pomocą standardu PCI DSS zwiększają bezpieczeństwo płatności dokonywanych kartami płatniczymi, aby jeszcze skuteczniej chronić akceptantów, posiadaczy kart i całą branżę przed kradzieżą i bezprawnym użyciem danych pochodzących z kart.

Kto jest zobowiązany do przestrzegania standardu PCI DSS?

Standard PCI DSS zobowiązuje akceptantów na całym świecie przesyłających, przetwarzających, lub przechowujących dane kart płatniczych, do implementacji i skutecznego przestrzegania wymaganych środków bezpieczeństwa. Dodatkowo akceptanci są odpowiedzialni za przestrzeganie dyrektyw dot. bezpieczeństwa przez inne upoważnione podmioty niebędące stroną, takie jak firmy hostingowe lub Payment Service Provider (PSP), których usługi są przez nich wykorzystywane lub które działają w ich imieniu, a których działanie może wpłynąć na bezpieczeństwo danych posiadacza karty. Prosimy o zapoznanie się z zawartymi w Ogólnych Warunkach Handlowych punktach „Ochrona danych" i „Odpowiedzialność", znajdującymi zastosowanie do akceptacji kart.

Kto jest odpowiedzialny za przestrzeganie standardu PCI DSS?

Przestrzeganie zasad dotyczących bezpieczeństwa należy do odpowiedzialności osobistej każdego akceptanta. Organizacje kart płatniczych wymagają jednak, aby akceptanci zadeklarowali (poddali weryfikacji zgodności) podjęte przez nich środki bezpieczeństwa. Zakres deklaracji (weryfikacji zgodności) zależy od liczby transakcji.

Jakie rodzaje sposobów weryfikacji zgodności można wyróżnić?

- **Self Assessment Questionnaire (SAQ)**
  Polega na samodzielnym wypełnieniu kwestionariusza.
- **On-Site Audit**
  Akceptanci realizujący dużą liczbę transakcji i ewentualnie tacy, którzy padli ofiarą kradzieży danych kart płatniczych, mają obowiązek skompletować raport dotyczący zapewnienia zgodności z przepisami (ROC – Report on Compliance).
  Wymagany raport i atest są wystawione przez certyfikowanego audytora bezpieczeństwa (QSA – Qualified Security Assessor) lub wewnętrznego audytora bezpieczeństwa (ISA – Internal Security Assessor).
- **Network Scan**
  Akredytowana jednostka weryfikująca (Approved Scanning Vendor) przeprowadza raz na kwartał po uzgodnieniu z akceptantem odpowiedni audyt w celu wskazania potencjalnie istniejących słabych punktów.

Jeżeli któryś z akceptantów nie spełnia wszystkich kryteriów weryfikacyjnych, jest zobowiązany niezwłocznie zwiększyć środki bezpieczeństwa w odpowiednich obszarach i może podlegać karom finansowym dopóki nie są one spełnione.

Kto ponosi koszty weryfikacji zgodności?

Koszty związane z działaniami certyfikacyjnymi pokrywane są w całości przez akceptantów, podobnie jak koszty poniesione w celu usunięcia braków, które zostały stwierdzone w wyniku kontroli.

Co się stanie, gdy akceptant nie podda się weryfikacji zgodności?

Jeżeli akceptant, który jest do tego zobowiązany, nie podda się certyfikacji, wówczas firma Worldline jest upoważniona do rozwiązania umowy ze skutkiem natychmiastowym i może żądać odszkodowania za możliwe kary nałożone przez organizacje kart płatniczych i roszczenia banku, który wydał kartę.

Kto ma wgląd do danych podlegających weryfikacji zgodności?

Wgląd do danych, które są zbierane podczas weryfikacji, ma jedynie akceptant i upoważniona jednostka certyfikująca. Jednakże akceptant jest zobowiązany do przesłania firmie Worldline podsumowania wyników z weryfikacji zgodności. Firma Worldline ma także wgląd do Self Assessment Questionnaire. Natomiast organizacje kart płatniczych przechowują tylko analizy statystyczne.

Jak często należy odnawiać weryfikację zgodności?

Wszystkie podmioty podlegają corocznej ocenie, a podmioty korzystające z adresów IP z dostępem do Internetu (e-commerce itp.) podlegają również kwartalnej ocenie ASV (potencjalne słabe punkty). Wszystkie znaczące zmiany w środowisku akceptanta muszą być niezwłocznie zgłoszone firmie Worldline w celu przeprowadzenia oceny ich wpływu na wymagania handlowe oraz w zakresie zgodności z przepisami.

Przez jakie firmy musi być przeprowadzana certyfikacja zgodności?

Spis wszystkich akredytowanych jednostek certyfikacyjnych znajduje się w Internecie.

- Dla przeprowadzania OnSiteAudits:
  pcisecuritystandards.org/pdfs/pci_qsa_list.pdf
- Dla przeprowadzania Network Scans:
  pcisecuritystandards.org/pdfs/asv_report.html

Gdzie znajdę więcej informacji na temat standardu PCI DSS?

Dalsze informacje na temat standardu PCI DSS znajdują się na następujących stronach internetowych:

- Worldline: worldline.com/merchant-services/pci
- PCI Security Standards Council: pcisecuritystandards.org

Osobę do kontaktu w Państwa kraju znaleźć można pod adresem: worldline.com/merchant-services/contacts

110.00110.05 INT_PL/08.2023