Payment Services

Wskazówki dla akceptantów na temat 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 informacji dla kart płatniczych). W przypadku nieprzestrzegania tych zasad firma SIX Payment Services 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 SIX Payment Services.

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 bezpie--czeństwa organizacji kart płatniczych. Do tych progra--mów 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 pochodzących z kart płatniczych. Bezprawne użycie skradzionych informacji pochodzących z kart płatniczych spowodowało powstanie znacznych szkód u wszystkich, których ten problem dotyczy.

Czemu służy standard PCI DSS?

Organizacje kart płatniczych za pomocą standardu PCI DSS podwyższają bezpieczeństwo płatności dokonywanych kartami płatniczymi, aby w ten sposób 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 z kart płatniczych, do podjęcia i skutecznego przestrzegania podanych środków bezpieczeństwa.

Poza tym akceptanci są odpowiedzialni za przestrzeganie dyrektyw w sprawie bezpieczeństwa przez upoważnione podmioty niebędące stroną, takie jak Payment Service Provider (PSP) lub Data Storage Entities (DSE), które w ich imieniu przesyłają, przetwa-rzają i przechowują dane. W tym celu proszę porównać zawarte w Ogólnych Warunkach Handlowych punkty „Ochrona danych" i „Odpowiedzialność", znajdujące 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 oraz od tego, czy akceptant ma kontakt z danymi kart płatniczych przy przesyłaniu, przetwarzaniu i przechowywaniu.

Jakie rodzaje sposobów weryfikacji zgodności można wyróżnić?

W zakresie standardu PCI DSS można wyróżnić trzy następujące sposoby weryfikacji zgodności (patrz również na tabelę na odwrocie strony):

- Self Assessment Questionnaire (SAQ)
  Polega na samodzielnym wypełnieniu kwestionariusza.
- Network Scan
  Akredytowana jednostka weryfikująca (Approved Scanning Vendor) przeprowadza raz na kwartał i po uzgodnieniu z akceptantem, „przyjazne ataki hakerskie" w celu wykazania potencjalnie istniejących słabych punktów.
- On-Site Audit
  Akceptanci realizujący dużą liczbę transakcji lub tacy, którzy padli ofiarą kradzieży danych kart płatniczych, mają obowiązek skompletować raport dotyczący zapewnienia zgodności z przepisami (ROC – Report on Compliance). Wyniki muszą zostać sprawdzone i potwierdzone przez certyfiko--wanego audytora bezpieczeństwa (QSA – Qualified Security Assessor) lub wewnętrznego audytora bezpieczeństwa (ISA – Internal Security Assessor).

Jeżeli któryś z akceptantów nie spełnia wszystkich kryteriów weryfikacyjnych, jest zobowiązany niezwłocznie polepszyć swoje środki bezpieczeństwa w odpowiednich obszarach.

Kto ponosi koszty weryfikacji zgodności?

Koszty związane z działaniami certyfikacyjnymi obciążają akceptantów, względnie upoważnioną osobę trzecią; to samo dotyczy wydatków poniesionych w celu usunięcia wad, 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 SIX Payment Services 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 cer-tyfikująca. Jednakże akceptant jest zobowiązany do przesłania firmie SIX Payment Services podsumowania wyników z weryfikacji zgodności. Firma SIX Payment Services ma także wgląd do Self Assess ment Question-naire. Natomiast organizacje kart płatniczych przecho-wują tylko analizy statystyczne.

Jak często należy odnawiać weryfikację zgodności?

Środki certyfikacyjne muszą być powtarzane cyklicznie, zgodnie z zamieszczoną poniżej tabelą. Takie zmiany u akceptanta jak: instalacja nowego sprzętu czy oprogramowania, nowa strona internetowa czy też zmiana dostawcy usług, muszą być niezwłocznie zgłoszone firmie SIX Payment Services. W zależności od okoliczności zmiany te mogą pociągać za sobą konieczność przeprowadzenia nowej certyfikacji.

Przez jakie firmy musi być przeprowadzana certyfikacja zgodności?

Spis wszystkich akredytowanych jednostek certyfikacyjnych znajduje się w Internecie.

– Do przeprowadzania On-Site-Audits:
  www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf
– Dla przeprowadzania Network Scans:
  www.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

– SIX Payment Services:
  www.six-payment-services.com/pci
– PCI Security Standards Council:
  www.pcisecuritystandards.org

Kto i jakie środki certyfikacyjne musi podjąć

Poziom	Oznaczenie	Visa, MasterCard/Maestro, Diners/Discover	JCB	American Express
1	Akceptant – więcej niż 6 mln transakcji na rok	– coroczny On-Site Audit[1] – kwartalny Network Scan		
	Akceptant, który stał się ofiarą kradzieży danych pochodzących z kart płatniczych			
	Akceptant – więcej niż 2,5 mln transakcji na rok			– coroczny On-Site Audit – kwartalny Network Scan
	Akceptant – więcej niż 1 mln transakcji na rok		– coroczny On-Site Audit – kwartalny Network Scan	
2	Akceptant – od 1 do 6 mln transakcji na rok	– coroczny Self Assessment Questionnaire[2] – kwartalny Network Scan		
	Akceptant – 50 000–2,5 mln transakcji na rok			– kwartalny Network Scan
3	Akceptant świadczący usługi teleinformatyczne 20 000–1 mln transakcji na rok	– coroczny Self Assessment Questionnaire – kwartalny Network Scan		
	Akceptant – mniej niż 50 000 transakcji na rok			– kwartalny Network Scan
4	Akceptant świadczący usługi teleinformatyczne – mniej niż 20 000 transakcji na rok	– coroczny Self Assessment Questionnaire – kwartalny Network Scan	– coroczny Self Assessment Questionnaire – kwartalny Network Scan	
	Akceptant (za wyjątkiem usług teleinformatycznych) – mniej niż 1 mln transakcji na rok			

[1] Sprzedawca może zdecydować, czy przeprowadzić audyt na miejscu, korzystając z pomocy certyfikowanego audytora bezpieczeństwa (QSA), czy wewnętrznego audytora bezpieczeństwa (ISA).
[2] Osoby odpowiedzialne za wypełnienie kwestionariusza SAQ muszą posiadać certyfikat ISA (Internal Security Assessor).

Weryfikacja On-Site Audit i/lub Network Scan jest obowiązkowa tylko dla tych akceptantów, którzy elektronicznie przetwarzają, przesyłają lub przechowują dane pochodzące z kart płatniczych. Jednakże zaleca się przede wszystkim akceptantom z kompleksową infrastrukturą przeprowadzenie opisanych kroków walidacyjnych. Akceptant zobowiązany jest każdorazowo do przestrzegania standardów PCI DSS. Akceptant zobowiązany jest przedstawić dowód przestrzegania ww. standardów dopiero po otrzymaniu pisemnego wezwania ze strony SIX Payment Services.

Osobę do kontaktu w Państwa kraju znaleźć można pod adresem: www.six-payment-services.com/kontakt

SIX Payment Services Ltd
Hardturmstrasse 201
Skrytka pocztowa
CH-8021 Zurych

SIX Payment Services (Europe) S.A.
10, rue Gabriel Lippmann
5365 Munsbach
Luksemburg

SIX Payment Services (Austria) GmbH
Marxergasse 1B
1030 Wiedeń
Austria

110.0110.05 INT_PL/05.2016