Worldline | SIX Payment Services

INSTRUCTIES OVER DE NALEVING VAN DE PCI DSS VEILIGHEIDSVOORSCHRIFTEN VOOR CONTRACTANTEN

Wereldwijd zijn alle contractanten die kaartgegevens verzenden, verwerken of opslaan verplicht om zich te houden aan de in de Payment Card Industry Data Security Standard (PCI DSS) vastgelegde beveiligingsrichtlijnen. Als deze richtlijnen worden veronachtzaamd, kan SIX Payment Services het contract met onmiddellijke ingang opzeggen en een schadevergoeding voor eventuele boetes en vorderingen opeisen.

De hierna volgende instructies zijn als technische en organisatorische richtlijnen bindende bestanddelen van elk contract met SIX Payment Services.

WAT HOUDT PCI DSS IN?

PCI DSS omvat 12 verplichte eisen, die de bescherming van kaartgegevens tijdens verwerking, opslag en verzending moeten waarborgen. De implementatie van PCI DSS wordt aangestuurd via de beveiligingsprogramma's van de kaartorganisaties. Hiertoe behoren AIS van Visa, SDP van Mastercard en de dienovereenkomstige programma's van American Express, Discover (Diners Club) en JCB.

WAAROM WERD PCI DSS INGEVOERD?

De afgelopen jaren nam de diefstal van kaartgegevens voortdurend toe. Door oneigenlijk gebruik van de gestolen kaartgegevens ontstond voor alle betrokkenen aanzienlijke schade.

WAT IS HET DOEL VAN PCI DSS?

De kaartorganisaties willen met PCI DSS de veiligheid van kaartbetalingen verder versterken en hierdoor handelaren, kaarthouders en de gehele branche nog doeltreffender beschermen tegen diefstal en misbruik van kaartgegevens.

WIE IS VERPLICHT OM PCI DSS NA TE LEVEN?

PCI DSS verplicht wereldwijd alle contractpartners die kaartgegevens verzenden, verwerken of opslaan ertoe om doeltreffende beveiligingsmaatregelen te nemen en zich hieraan te houden.

Daarnaast zijn de contractpartners ervoor verantwoordelijk dat externe ondernemingen zoals Payment Service Providers (PSP) of Data Storage Entities (DSE), die namens hen gegevens verzenden, verwerken of opslaan, eveneens aan deze beveiligingsrichtlijnen voldoen.

Zie ook de bepalingen over gegevensbescherming en aansprakelijkheid in de algemene voorwaarden voor kaartaanvaarding die van toepassing zijn.

WIE IS ERVOOR VERANTWOORDELIJK DAT PCI DSS NAGELEEFD WORDT?

In principe is het de eigen verantwoordelijkheid van elke contractpartner om zich aan de veiligheidsvoorschriften te houden. De kaartorganisaties eisen echter dat de contractanten de door hun genomen beveiligingsmaatregelen waarborgen (laten certificeren). De omvang van de certificering is afhankelijk van het aantal transacties en van het feit of de contractpartner met kaartgegevens in contact komt tijdens de verzending, verwerking en opslag.

WELKE SOORTEN CERTIFICERING ZIJN ER?

Onder PCI DSS bestaan de volgende drie soorten certificeringsmaatregelen (zie ook de tabel op de achterzijde):

- **Self-Assessment Questionnaire (SAQ)**
  Een zelfbeoordelingsformulier dat moet worden ingevuld.
- **Network Scan**
  Een geaccrediteerde certificeringsonderneming (Approved Scanning Vendor) voert driemaandelijks en na afstemming met de contractpartner overeengekomen hackingaanvallen uit, om mogelijke zwakke punten vast te stellen.
- **On-Site Audit**
  Acceptanten met grote transactievolumes of acceptanten die slachtoffer zijn geworden van een diefstal van kaartgegevens zijn verplicht een ROC (Report on Compliance) in te vullen. De resultaten moeten worden gecontroleerd en bevestigd door een geaccrediteerde certificeerder (QSA –Qualified Security Assessor) of door een geschoolde auditor (ISA – Internal Security Assessor).

Als een contractant niet voldoet aan alle certificeringseisen, is hij verplicht om zijn beveiligingsmaatregelen op de betreffende terreinen onmiddellijk te verbeteren.

WIE BETAALT DE KOSTEN VAN EEN CERTIFICERING?

De kosten voor de certificeringsmaatregelen komen volledig voor rekening van de contractant, respectievelijk de derde partij waaraan hij opdracht geeft. Ditzelfde geldt voor de kosten van herstel voor de gebreken die bij de controle werden vastgesteld.

WAT GEBEURT ER ALS EEN CONTRACTPARTNER ZICH NIET LAAT CERTIFICEREN?

Als een contractant die hiertoe verplicht is zich niet laat certificeren, heeft SIX Payment Services het recht om het contract met onmiddellijke ingang op te zeggen en een schadevergoeding te eisen voor eventuele boetes van de kaartorganisaties en voor vorderingen van de kaartemittenten.

WIE HEEFT ER TOEGANG TOT DE CERTIFICERINGSGEGEVENS?

Uitsluitend de contractant en de certificeringsonderneming die de opdracht krijgt, hebben toegang tot de gegevens die in het kader van een certificering worden vastgesteld. De contractant is echter verplicht om de samenvatting van de certificeringsresultaten aan SIX Payment Services te zenden. Daarnaast heeft SIX Payment Services inzage in de Self-Assessment Questionnaires. De kaartorganisaties ontvangen echter uitsluitend statistische analyses.

HOE VAAK MOET EEN CERTIFICERING WORDEN HERHAALD?

De certificeringsmaatregelen moeten periodiek worden herhaald volgens de onderstaande tabel:

Wijzigingen bij de contractant zoals de installatie van nieuwe hard- of software, een nieuwe website of een verandering van de dienstverleners die zijn verbonden aan de acceptatie van kaartbetalingen, moeten bovendien omgaand aan SIX Payment Services worden gemeld. In sommige gevallen is hierdoor een nieuwe certificering noodzakelijk.

WELKE ONDERNEMINGEN MOGEN DE CERTIFICERINGEN UITVOEREN?

Een overzicht van alle geaccrediteerde certificeringsondernemingen vindt u op internet:

- Voor de uitvoering van On-Site Audits: pcisecuritystandards.org/pdfs/pci_qsa_list.pdf
- Voor de uitvoering van Network Scans: pcisecuritystandards.org/pdfs/asv_report.html

WAAR VIND IK NOG MEER INFORMATIE OVER PCI DSS?

Nadere informatie over PCI DSS vindt u op de volgende websites:

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

WIE MOET WELKE CERTIFICERINGSMAATREGELEN NEMEN?

Niveau	Omschrijving	Visa, Mastercard/Maestro, Diners/Discover	JCB	American Express
1	Handelaren met meer dan 6 miljoen transacties per jaar	• jaarlijkse On-Site Audit[1] • driemaandelijkse Network Scan		
	Handelaar die slachtoffer werd van kaartgegevensdiefstal			
	Handelaren met meer dan 2,5 miljoen transacties per jaar			• jaarlijkse On-Site Audit • driemaandelijkse Network Scan
	Handelaren met meer dan 1 miljoen transacties per jaar		• jaarlijkse On-Site Audit • driemaandelijkse Network Scan	
2	Handelaren met 1–6 miljoen transacties per jaar	• jaarlijkse Self-Assessment Questionnaire[2] • driemaandelijkse Network Scan		
	Handelaren met 50 000 – 2,5 miljoen transacties per jaar			• driemaandelijkse Network Scan
3	E-commerce handelaren met 20 000 – 1 miljoen transacties per jaar	• jaarlijkse Self-Assessment Questionnaire • driemaandelijkse Network Scan		
	Handelaren met minder dan 50 000 transacties per jaar			• driemaandelijkse Network Scan
4	E-commerce handelaren met minder dan 20 000 transacties per jaar	• jaarlijkse Self-Assessment Questionnaire • driemaandelijkse Network Scan	• jaarlijkse Self-Assessment Questionnaire • driemaandelijkse Network Scan	
	Handelaren (excl. e-commerce) met minder dan 1 milj. transacties per jaar			

[1] De acceptant kan zelf beslissen of hij de On-Site Audit ter plaatse wil uitvoeren met ondersteuning van een QSA (Qualified Security Assessor) of een ISA (Internal Security Assessor).
[2] De voor het invullen van de SAQ verantwoordelijke personen moeten zijn gecertificeerd als ISA (Internal Security Assessor).

On-Site Audit en/of Network Scan zijn uitsluitend verplicht voor contractanten die kaartgegevens elektronisch verwerken, verzenden of opslaan. Niettemin raden wij in het bijzonder ook contractanten met complexe infrastructuren aan om deze controle toch uit te voeren. De contractant moet zich altijd houden aan de richtlijnen van PCI DSS. Het bewijs voor de naleving hoeft de contractant echter pas na schriftelijke aanvraag door SIX Payment Services te leveren.

U VINDT UW LOKALE CONTACTPERSOON OP:
six-payment-services.com/contacts

six-payment-services.com
worldline.com

110.0110.07 INT_NL/07.2020