De Payment Card Industry – Data Security Standard

Drs. J.G. IJkel RE CISSP CISA
is werkzaam als senior manager bij KPMG IT Advisory. Hij is gespecialiseerd in (technische) informatiebeveiliging en operationeel verantwoordelijk voor de penetratietestdiensten die door KPMG in Nederland worden uitgevoerd.

ijkel.hans@kpmg.nl

Drs. Hans IJkel RE CISSP CISA

Berichten over grote aantallen gecompromitteerde creditcardgegevens komen regelmatig in het nieuws. Indien met deze gestolen gegevens vervolgens ook fraude wordt gepleegd, kan dit invloed hebben op het vertrouwen dat gebruikers in het gebruik van creditcards hebben en dus uiteindelijk resulteren in mogelijk lagere opbrengsten voor creditcardmaatschappijen door het verminderde gebruik. Daarom is al enige tijd geleden de Payment Card Industry – Data Security Standard in het leven geroepen die moet voorkomen, dan wel tijdig detecteren, dat creditcardgegevens worden gecompromitteerd. In dit artikel wordt beschreven wat deze standaard inhoudt, welke problemen er kunnen optreden bij de implementatie en hoe deze kunnen worden aangepakt en wat de gevolgen kunnen zijn als men niet compliant is.

Inleiding

De leden van de Payment Card Industry (PCI) Security Standards Council (American Express, Discover, JCB, MasterCard en Visa) monitoren continu gevallen van het compromitteren van creditcardgegevens. Een beveiligingsincident en vervolgens het compromitteren van creditcardgegevens kan verstrekkende gevolgen hebben voor de betrokken organisaties, inclusief mogelijke notificatievereisten ten aanzien van het incident (in bijvoorbeeld de Verenigde Staten[1]) reputatierisico, verlies van klanten, mogelijke financiële verplichtingen en rechtszaken.

Uit analyse achteraf is gebleken dat veelvoorkomende beveiligingszwakheden die door de Payment Card Industry Data Security Standard (PCI DSS) worden geadresseerd, niet waren geïmplementeerd door organisaties ten tijde van het beveiligingsincident. De PCI DSS werd opgezet en bevat gedetailleerde vereisten om exact deze reden – om de kans op en de gevolgen van een beveiligingsincident te minimaliseren. De PCI DSS is opgezet door de oprichters van de PCI Security Standards Council (PCI SSC) om de brede globale acceptatie van consistente databeveiligingsmaatregelen te bewerkstelligen. De standaard bevat onder andere vereisten voor security management, policies, procedures, netwerkarchitectuur en softwareontwikkeling.

1 Hoewel in Europa ook wordt gesproken over zogenaamde 'security breach notification', wil men op dit moment dat zo'n notificatie alleen van toepassing zal zijn op telecomproviders en niet op bijvoorbeeld online banking.

Heartland Payment Systems processes payments for over 250,000 mostly small and mid-size businesses and merchants in the U.S. and is considered to be the sixth-largest payment processor in the country. On 20 January 2009, the company announced that, during an internal audit prompted by a Visa warning, it had discovered that transaction data passing through its network had been intercepted and a significant number of credit cards had been compromised.
RBS WorldPay offers payment-processing solutions that cover credit, debit, Electronic Bank Transfers, gift cards, customer loyalty cards, checks, ATM, and tailored solutions for retail, restaurant, petroleum, convenience stores, grocery, hospitality, transport, and cardholders not present in these sectors. On 23 December 2008, the company announced that, at the beginning of November, unidentified parties had illegally obtained access to its computer systems and potentially compromised the personal information of 1.5 million customers.
RBS also noted that 100 payroll cards had been fraudulently used and had, subsequently, been disabled. It was later revealed that these cards had been employed in one of the most complex and well-coordinated fraud schemes to have ever been instrumented. Over 130 different ATM machines in 49 cities worldwide were hit in a 30-minute period, the crooks successfully withdrawing a whooping $9 million.
(Bron: news.softpedia.com)

PCI DSS

Welke data moet worden beschermd?

Creditcardgegevens kunnen worden gedefinieerd als het zogenaamde Primary Account Number (PAN) en andere gegevens die worden verkregen als onderdeel van een betaaltransactie, waaronder de volgende gegevens vallen:

- naam van kaarthouder;
- vervaldatum;
- servicecode;
- gevoelige authenticatie-informatie, zoals:
  - de volledige 'magnetic stripe'-gegevens (op magnetische strip, op een chip of elders opgeslagen);
  - zogenaamde card validation codes;
  - pingegevens.

Het PAN is de factor die bepaalt of de PCI DSS en de PA DSS (Payment Application Data Security Standard) van toepassing zijn. Indien het PAN niet wordt opgeslagen, verwerkt of verstuurd, dan zijn de PCI DSS en de PA DSS ook niet van toepassing.

In dit artikel zal overigens verder niet worden ingegaan op de PA DSS. Het is wel goed om te weten dat de standaard bestaat om de beveiliging van third party payment applicaties te beoordelen. De beveiliging van zelfontwikkelde applicaties wordt door de PCI DSS afgedekt. Een lijst van gecertificeerde applicaties is beschikbaar via de PCI SSC.

Naam van kaarthouder, vervaldatum en servicecode moeten beschermd worden indien deze worden opgeslagen samen met het PAN, conform de PCI DSS. Tevens zouden op deze gegevens nog additionele (wettelijke) regels van toepassing kunnen zijn, zoals privacyregels.

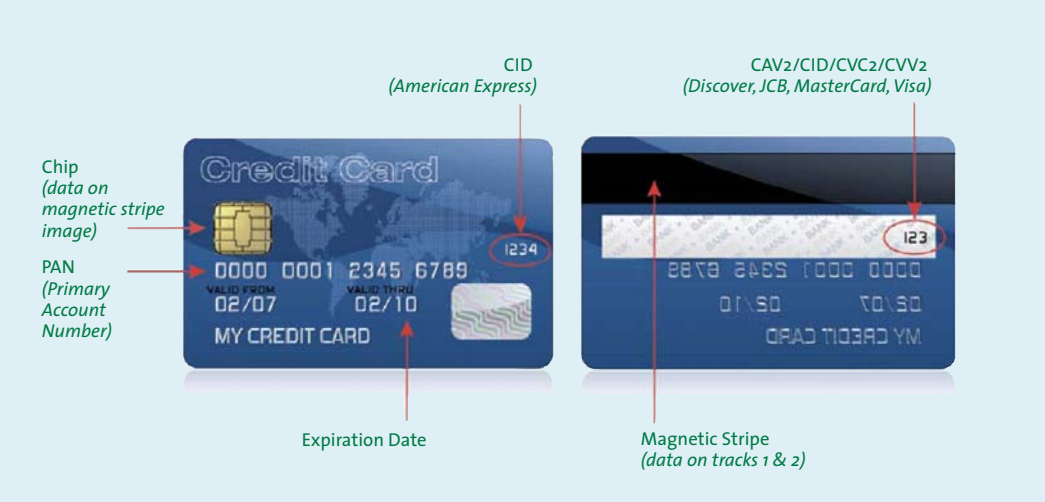
De gevoelige authenticatie-informatie mag volgens de PCI-standaard nooit worden opgeslagen nadat autorisatie voor een betaling al is verkregen.

Zoals boven vermeld is het niet toegestaan gevoelige authenticatie-informatie op te slaan. Dit is om de eenvoudige reden dat indien deze gegevens samen met het PAN kunnen worden verkregen, er grote risico's ontstaan dat deze gegevens worden misbruikt voor het uitvoeren van frauduleuze transacties.

Indien een crimineel de 'magnetic stripe'-gegevens in handen zou krijgen, dan zou er zelfs een volledige kopie van de creditcard gemaakt kunnen worden. De figuren 2 en 3 laten zien welke informatie op de magnetic strip van een creditcard staat.

	Data Element	Storage Permitted?	Protection Required?	PCI DSS Req. 3, 4
Cardholder Data	• Primary Account Number	Yes	Yes	Yes
	• Cardholder Name	Yes	Yes	No
	• Service Code	Yes	Yes	No
	• Expiration Date	Yes	Yes	No
Sensitive Authentication Data	• Full Magnetic Stripe Data	No	N/A	N/A
	• CAV2/CVC2/CVV2/CID	No	N/A	N/A
	• PIN/PIN Block	No	N/A	N/A

Tabel 1. **Overzicht creditcardgegevens en vereisten ten aanzien van opslag en beveiliging (ofwel versleuteling).**

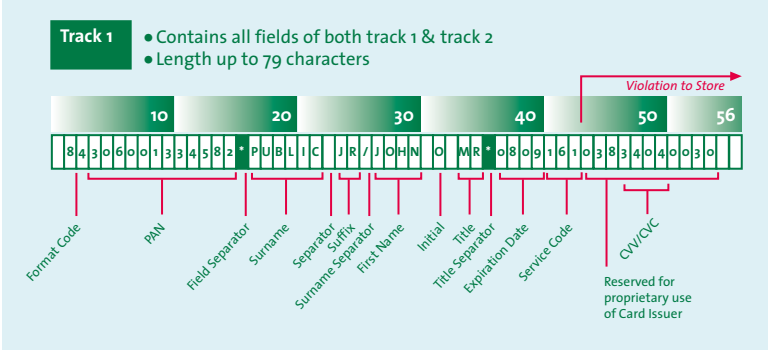


Figuur 1. **Visuele weergave elementen creditcardgegevens, voor- en achterzijde.**

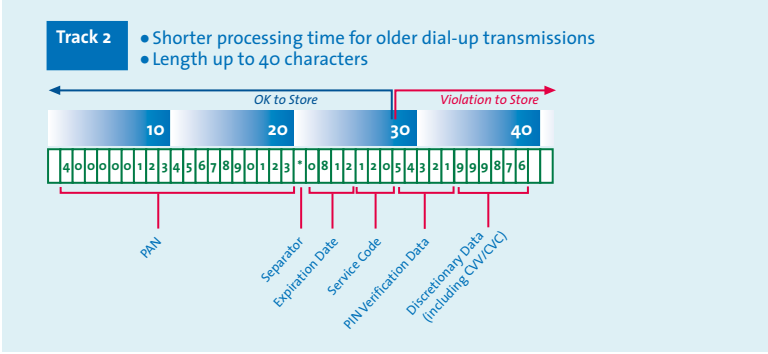
Voor wie en waarop is de PCI DSS van toepassing?

In principe dient eenieder (met uitzondering van de eindgebruiker) die creditcardgegevens *opslaat, verwerkt* of *verstuurt* te voldoen aan de PCI DSS. Dit geldt dus voor zowel grote partijen, bijvoorbeeld Equens, als kleine partijen, zoals een webwinkel met maar enkele creditcardtransacties per jaar. De wijze waarop compliance moet worden aangetoond verschilt echter, enerzijds op basis van de rol die men heeft (serviceprovider of merchant) en anderzijds op basis van het volume van transacties per jaar.

De scope waarvoor compliance moet worden aangetoond, wordt in de PCI DSS gedefinieerd als alle systeemcomponenten die onderdeel zijn van of een connectie hebben met de zogenaamde 'cardholder data'-omgeving. De 'cardholder data'-omgeving is dat gedeelte van het netwerk waar cardholder data of gevoelige authenticatiegegevens zich bevinden, inclusief netwerkcomponenten, servers en applicaties. Uiteindelijk zou deze regel vanuit de PCI DSS kunnen resulteren in het toepasbaar zijn van de PCI DSS op het gehele interne netwerk van een bedrijf en niet alleen de 'cardholder data'-omgeving zelf!



Figuur 2. **Visuele weergave gegevens op track 1 van de magnetic stripe.**



Figuur 3. **Visuele weergave gegevens op track 2 van de magnetic stripe.**

Hoe moet de data worden beschermd?

De PCI DSS bevat min of meer 6 onderwerpen, 12 gebieden en 62 hoofdvereisten. Deze 62 hoofdvereisten bestaan op hun beurt weer uit een aantal meer gedetailleerde vereisten waaraan men moet voldoen om aan de hoofdvereisten te kunnen voldoen. In tabel 4 zijn de onderwerpen en gebieden weergegeven, inclusief een korte uitleg over wat deze betekenen.

In principe moet men aan alle vereisten voldoen om PCI-compliant te worden. Hoewel veel van deze vereisten kunnen worden gezien als normale good practices om een IT-omgeving te beveiligen en te beheren, is er toch een aantal gebieden die het moeilijk (kunnen) maken om compliant te geraken.

Wat zijn veelvoorkomende problemen bij implementatie?

Op basis van de ervaringen die zijn voortgekomen uit het recente verleden bij bedrijven die reeds de PCI DSS hebben geïmplementeerd en ook zoals KPMG deze is tegengekomen bij haar klanten, kan een aantal implementatieproblemen worden gedefinieerd. Inmiddels is het ook tot creditcardmaatschappijen doorgedrongen dat compliancy niet altijd binnen korte tijd is te realiseren en daarom is het van belang om constant in contact te blijven met deze maatschappijen om afspraken te maken over het pad om uiteindelijk wel volledige compliancy te bereiken.

Locatie van cardholder data

Aan het begin van een PCI DSS-traject is vaak niet exact bekend waar cardholder data precies is opgeslagen en of deze opslag ook werkelijk noodzakelijk is. Een inventarisatie zal dus moeten worden gemaakt van alle systemen (inclusief eindgebruikersystemen) en er zal moeten worden bepaald of het aantal locaties waar data wordt opgeslagen niet kan worden teruggebracht.

Zonder inventarisatie kan ook niet worden vastgesteld of men PCI-compliant is, aangezien er geen informatie beschikbaar is over de scope. Het niet terugdringen van het aantal locaties waar cardholder data zich bevindt kan mogelijk resulteren in kostbare maatregelen die op meer systemen moeten worden geïmplementeerd (zoals de versleutelingseisen).

Scoping

De PCI DSS schrijft voor dat alle systeemcomponenten die onderdeel zijn van of een connectie hebben met de 'cardholder data'-omgeving compliant moeten worden gemaakt. Indien geen netwerkscheiding wordt aangebracht tussen de 'cardholder data'-omgeving en de rest van het interne netwerk van een bedrijf, dient het gehele interne netwerk PCI-compliant te worden gemaakt, wat een onmogelijke, dan wel zeer tijdrovende en kostbare taak kan blijken te zijn.

Level/ Tier[1]	Merchant Criteria	Validation Requirements
1	Merchants processing over 6 million Visa transactions annually (all channels) or Global merchants identified as Level 1 by any Visa region[2]	• Annual Report of Compliance ('ROC') by Qualified Security Assessor ('QSA') • Quarterly network scan by Approved Scan Vendor ('ASV') • Attestation of Compliance Form
2	Merchants processing 1 to 6 million Visa transactions annually (all channels)	• Annual Self-Assessment Questionnaire ('SAQ') • Quarterly network scan by ASV • Attestation of Compliance Form
3	Merchants processing 20,000 to 1 million Visa e-commerce transactions annually	• Annual SAQ • Quarterly network scan by ASV • Attestation of Compliance Form
4	Merchants processing less than 20,000 Visa e-commerce transactions annually and all other merchants processing up to 1 million Visa transactions annually	• Annual SAQ recommended • Quarterly network scan by ASV if applicable • Compliance validation requirements set by acquirer

1. Compromised entities may be escalated at regional discretion.
2. Merchant meeting Level 1 criteria in any Visa country/region that operates in more than one country/region, is considered a global Level 1 merchant. Exception may apply to global merchants if no common infrastructure, and if Visa data is not aggregated across borders; in such cases merchant validates according to regional levels.

Tabel 2. **Merchantniveaus en compliance-validatievereisten Visa; andere creditcardmaatschappijen hanteren een gelijksoortige indeling.**

Service Provider Level	Description
1[1]	• VisaNet processors or any service provider that stores, processes and/or transmits over 300,000 transactions per year
2[2]	• Any service provider that stores, processes and/or transmits less than 300,000 transactions per year

1. Eliminates payment gateway definition from several existing regional programs.
2. Effective February 1, 2009, Level 2 service providers will no longer be listed on Visa's List of PCI DSS Compliant Service Providers. Entities that wish to be on the List of PCI DSS Compliant Service Providers must validate as a Level 1 provider.

Level	Validation Action	Validated by	Due Date
1	• Annual On-Site PCI Data Security Assessment • Quarterly Network Scan	• Qualified Security Assessor • Approved Scanning Vendor	2/01/09
2	• Annual PCI Self-Assessment Questionnaire • Quarterly Network Scan	• Service Provider • Approved Scanning Vendor	2/01/09

Tabel 3. **Serviceproviderniveaus en compliance-validatievereisten Visa.**

	Onderwerp/ gebieden PCI DSS	Uitleg
	Build & maintain secure network	
1	Install and maintain a firewall configuration to protect cardholder data	Alle systemen moeten worden beschermd tegen ongeautoriseerde toegang vanaf niet vertrouwde netwerken zoals het internet en draadloze netwerken.
2	Do not use vendor-supplied defaults for system passwords and other security parameters	Kwaadwillende personen (in- of extern) maken vaak misbruik van door de leverancier van apparatuur en software meegeleverde standaardwachtwoorden en andere settings waarmee ongeautoriseerde toegang kan worden verkregen.
	Protect cardholder data	
3	Protect stored cardholder data	Indien andere beveiligingsmaatregelen worden doorbroken, dan dienen maatregelen zoals versleuteling, 'truncation', maskering en hashing van cardholder data te voorkomen dat misbruik kan worden gemaakt van deze gegevens.
4	Encrypt transmission of cardholder data across open, public networks	Cardholder data die via publieke netwerken dient te worden verstuurd, moet worden beveiligd met sterke versleuteling.
	Maintain vulnerable management program	
5	Use and regularly update anti-virus software	Antivirussoftware moet worden geïnstalleerd op alle systemen die normaal gesproken door malware kunnen worden getroffen om deze te beschermen tegen huidige en toekomstige kwaadaardige software.
6	Develop and maintain secure systems and applications	(Web)applicaties dienen te worden ontwikkeld op basis van OWASP en/of andere secure coding richtlijnen en systemen en applicaties dienen te worden gepatcht binnen een maand nadat een kritieke security patch is uitgebracht.
	Implement strong access control measures	
7	Restrict access to cardholder data by business need-to-know	Kritieke data mag alleen door geautoriseerd personeel worden benaderd op basis van het 'need to know'-principe (minimale toegang tot die gegevens die noodzakelijk zijn om een functie uit te voeren).
8	Assign a unique ID to each person with computer access	Alle acties op een systeem of applicatie dienen traceerbaar te zijn naar een individu, op basis van unieke user-ID's en adequate beveiliging van wachtwoorden.
9	Restrict physical access to cardholder data	Fysieke toegang tot data en systemen die cardholder data bevatten dient te worden beperkt.
	Regularly monitor & test networks	
10	Track and monitor all access to network resources and cardholder data	Loggingmechanismen en de mogelijkheid om gebruikers-activiteiten op te sporen moeten aanwezig zijn om te voorkomen dat (dan wel te detecteren of) data gecompromitteerd wordt.
11	Regularly test security systems and processes	Aangezien continu nieuwe beveiligingszwakheden worden ontdekt, dienen systemen, processen en zelfontwikkelde software regelmatig te worden getest om zeker te stellen dat deze nog steeds veilig zijn.
	Maintain information security policy	
12	Maintain a policy that addresses information security	De security policy dient zorg te dragen dat eenieder zich bewust is van de gevoeligheid van bepaalde gegevens en van zijn rol en verantwoordelijkheid in het beschermen van deze gegevens.

Tabel. 4. **Onderwerpen en gebieden van de PCI DSS, met korte toelichting.**

De 'cardholder data'-omgeving scheiden van het interne netwerk is van het grootste belang

Het is daarom van het grootste belang om te trachten de 'cardholder data'-omgeving af te scheiden van het interne netwerk via interne firewalls. Hierdoor kan de scope worden beperkt en dus ook de inspanning om de PCI DSS te implementeren.

Veranderingen in bedrijfsprocessen

Het invoeren van de PCI DSS, inclusief het beperken van de locaties waar cardholder data zich bevindt en overige pogingen om de scope te beperken, kan tevens resulteren in de noodzaak om bepaalde bedrijfsprocessen dan wel IT-beheerprocessen te wijzigen.

Organisatorische veranderingen kunnen soms rekenen op weerstand en tevens hebben nieuwe processen vaak een aanlooptijd nodig voordat deze volledig werken zoals voorzien.

Monitoring

De PCI DSS bevat aanzienlijk uitgebreide vereisten ten aanzien van logging en monitoring. Ten eerste moet worden nagegaan in hoeverre bestaande applicaties en systemen wel voldoende mogelijkheden bieden om aan de vereisten te voldoen en wat er exact zou moeten worden gemonitord binnen de applicaties en systemen. Voorts dient mogelijk nieuwe software te worden geïmplementeerd en personeel te worden aangenomen om ook de monitoring goed te kunnen uitvoeren.

Versleuteling cardholder data

Het voldoen aan de vereisten van versleuteling van cardholder data is soms moeilijk te implementeren, bijvoorbeeld:

- omdat gebruik wordt gemaakt van legacy draadloze netwerken (met zwakke of geen versleuteling) in bijvoorbeeld winkels waar creditcardgegevens van 'point of sale'-systemen naar centrale systemen worden verstuurd;
- omdat er sprake is van legacy applicaties waarin het niet mogelijk is zodanige veranderingen in de software door te voeren dat de software versleuteling van en naar de database met de cardholder data ondersteunt.

Voortdurende compliance

Nadat de initiële PCI-compliance is gerealiseerd, is het noodzakelijk dat aandacht wordt besteed aan het compliant blijven. Nieuwe systemen en applicaties die worden geïntroduceerd zullen aan dezelfde eisen moeten voldoen als de initiële omgeving, daarnaast kunnen er ook updates plaatsvinden op de PCI DSS-vereisten die moeten worden opgevolgd. Tot slot zijn er ook bepaalde eisen in de PCI DSS die een bedrijf waarschijnlijk niet zelf kan en/of mag uitvoeren. Een voorbeeld hiervan zijn de vereisten in tabel 4 onder punt 11, die het minimaal jaarlijks uitvoeren van interne en externe penetratietests verplicht stellen en daarbij een mate van onafhankelijkheid eisen van degene die de penetratietest uitvoert ten opzichte van de organisatie die het beheer van de PCI-omgeving uitvoert.

Samenvatting en conclusie

De PCI DSS dient de kans op beveiligingsincidenten in de 'cardholder data'-omgeving te verkleinen en de detectie van (mogelijke) incidenten te verhogen, om uiteindelijk fraude met creditcardgegevens te voorkomen. Indien bedrijven die in principe verplicht zijn de PCI DSS te implementeren dit niet (goed) doen, kan dat tot onder andere boetes en het verlies van klanten leiden en dus negatieve financiële consequenties hebben of misschien zelfs wel de continuïteit schaden. In de Verenigde Staten zijn er zelfs staten (Minnesota) die compliance met de PCI DSS wettelijk verplicht hebben gesteld).

Het is dus van belang dat bedrijven zorgen dat ze compliant zijn. Hiertoe dient wel een aanpak te worden gehanteerd die efficiënt en effectief is en dus te hoge compliancekosten vermijdt. Hiervoor is het vooral van belang dat rekening wordt gehouden met de scope waarop de PCI DSS van toepassing is en die trachten zo klein mogelijk te maken. Tevens dient open communicatie plaats te vinden met de creditcardmaatschappijen, of de partij waaraan compliance moet worden aangetoond, om de voortgang van compliance te bespreken en eventueel te kunnen uitleggen waarom het voldoen aan bepaalde eisen meer tijd vergt.

Literatuur

https://www.pcisecuritystandards.org/, PCI DSS 1.2, oktober 2008.
https://www.pcisecuritystandards.org/, PCI DSS 1.2, 'Navigating PCI DSS', oktober 2008.
http://boonbox.net/resources.htm, Managers' Cheat Sheet for PCI DSS, december 2008.
http://www.pcicomplianceguide.org/
http://news.softpedia.com/news/Heartland-and-RBS-WorldPay-No-Longer-PCI-Compliant-106826.shtml, 16 maart 2009.
http://usa.visa.com/merchants/risk_management/cisp_merchants.html
http://www.out-law.com/page-9841, 'EU nations oppose extension of data breach notification law', 3 maart 2009.
https://www.revisor.leg.state.mn.us/bin/bldbill.php?bill=S1574.2.html&session=ls85