

# Stringenter richtlijnen voor het beveiligen van creditcardgegevens

drs. F. Drevers, drs. ing. I. Meinema RE CISSP en drs. J. Bikker RE CIA\*

## 1. Inleiding

Fraude is een fenomeen waarmee bedrijven en overheden in toenemende mate te maken krijgen. In het kader van de Wet op het financieel toezicht (Wft) dienen instellingen te beschikken over een beheerste bedrijfsvoering. Dit geldt onder meer ten aanzien van bescherming van persoonsgegevens. Toegang tot deze gegevens wordt steeds eenvoudiger door onder meer het Internet en de koppeling van diverse gegevensbestanden en de veelal beperkte beveiliging van gegevens. Bedrijven worden op onverwachte tijdstippen en plekken getroffen door fraude. Dit heeft een grote impact.

Fraude met persoonsgegevens kan het vertrouwen van klanten in onder andere dienstverlening of producten schaden. Hierdoor komt de continuïteit of reputatie van de betreffende leverancier onder druk te staan. Het frauderisico wordt steeds vaker bij specifieke personen binnen een organisatie neergelegd waaronder de compliance officer. Dit om fraude beter te beheersen, te voorkomen, te ontdekken en te redigeren. Daarnaast is het de uitdaging om met compliance commerciële kansen te creëren en onderscheidend te zijn als organisatie.

Bedrijven die creditcardgegevens verwerken zijn een gewild doelwit voor fraudeurs. In dat kader is vanuit de vijf grote creditcardmaatschappijen een specifieke beveiligingsstandaard opgesteld voor creditcardgegevens, de Payment Card Industry Data Security Standard (PCI DSS). Vanwege het toenemend aantal creditcardfraudes wereldwijd neemt het belang toe om aan PCI DSS te voldoen. De geleden schade loopt wereldwijd op tot meer dan 3 miljard US dollar<sup>1</sup>. Deze schade zal naar verwachting alleen maar toenemen door het groeiende aantal verkopen via e-commerce.

Creditcardmaatschappijen stimuleren organisaties die creditcardtransacties verwerken steeds meer om zich aan de PCI DSS standaard te confirmeren. Dit doen zij door het opleggen van boetes aan organisaties die creditcardgegevens verwerken en niet aan deze standaard voldoen. Deze boetes kunnen oplopen tot 500 000 US dollar. De creditcardmaatschappijen hebben aangekondigd de standaarden ook in Europa strenger toe te zullen passen. Visa heeft reeds een deadline afgegeven waarop aan deze standaarden moeten voldoen. Des te meer een reden voor Compliance Officers om tijdig intern aandacht voor deze problematiek te vragen.

## 2. PCI DSS standaard nader toegelicht

Als gevolg van de stijgende risico's en de toenemende belangen heeft de PCI Security Standards Council in december 2004 PCI DSS geïntroduceerd. PCI Security Standards Council is een samenwerkingsverband van organisaties zoals

American Express, MasterCard Worldwide en Visa International.

Hoewel PCI DSS een Amerikaanse norm is, is deze standaard vereist voor alle organisaties die creditcardtransacties verwerken, verzenden of hierover rapporteren. De partijen die hierbij worden onderscheiden, betreffen:

1. Merchants: onder andere retailers, horecaondernemers en webwinkels;
2. Service Providers: de bedrijven die andere organisaties helpen met loyaliteitsprogramma's, creditcarddata verwerking en opslag;
3. Acquiring: banken of andere organisaties die creditcardtransacties verwerken; en
4. Issuers: organisaties, zoals banken, die creditcards uitgeven.

Afhankelijk van de categorie en het transactievolume geeft PCI DSS een bepaald beveiligingsniveau aan. In het onderstaande overzicht zijn per niveau de kenmerken aangegeven inclusief de gestelde eisen (zie figuur 1).

De PCI Security Standards Council raadt aan om Qualified Security Assessor (QSA) gecertificeerde bedrijven de on-site beveiligingsaudits te laten uitvoeren. Bedrijven kunnen de audit ook intern laten uitvoeren door de eigen interne audit afdeling, mits de benodigde kennis beschikbaar is en het bedrijf officieel akkoord gaat met de uitkomsten van de betreffende audit. De benodigde PCI DSS kennis kan bijvoorbeeld worden opgedaan via trainingen van het PCI Council. Het betreffende audit rapport dient als input voor de creditcardmaatschappijen om vast te stellen of het betreffende bedrijf PCI DSS compliant is. De scan van het IT netwerk (bijvoorbeeld op het gebied van firewalls, datalijnen, servers) dient altijd door een Approved Scan Vendor (ASV) gecertificeerd bedrijf te worden uitgevoerd.

De PCI DSS-standaard bestaat uit ruim 200 controles, waaraan aantoonbaar dient te worden voldaan. Dit controleraamwerk is opgedeeld in de volgende 12 aandachtsgebieden:

### *Bouw en onderhoud een beveiligd netwerk*

1. Installeer en onderhoud een firewall om card gegevens te beschermen.
2. Gebruik geen standaard wachtwoorden voor systemen en beveiligingsinstellingen.

\* Frenkel Drevers, Irma Meinema en Hans Bikker zijn werkzaam bij Protiviti – Risk & Business Consulting en Internal Audit.

1. [www.pci-dss-made-easy.com](http://www.pci-dss-made-easy.com).

Handelaar en Service Provider niveaus en validatie acties					
	Niveau	Criteria	On-site beveiligingsaudit	Self-assessment vragenlijst	Netwerk scan
<b>Merchants</b>	1	Elke handelaar die meer dan 6,000,000 Visa transacties per jaar verwerkt. Elke handelaar die een beveiligingsincident heeft gehad of een aanval heeft ondergaan die tot klant data verlies leidde. Elke handelaar waarvan Visa vaststelt dat de handelaar aan de niveau 1 vereisten moet voldoen om de risico's voor het Visa systeem te beperken Elke handelaar die door een andere credit card maatschappij als niveau 1 wordt aangemerkt.	Jaarlijks verplicht		Elk kwartaal verplicht
	2	Elke handelaar -onafhankelijk van acceptatie kanaal, die tussen de 1,000,000 en 6,000,000 Visa transacties per jaar verwerkt		Jaarlijks verplicht	Elk kwartaal verplicht
	3	Elke handelaar die tussen de 20,000 en 1,000,000 Visa e-commerce transacties per jaar verwerkt		Jaarlijks verplicht	Elk kwartaal verplicht
	4	Elke handelaar die minder dan 20,000 Visa e-commerce transacties per jaar verwerkt, en alle andere handelaren die tot 1,000,000 Visa transacties per jaar verwerken.		Jaarlijks verplicht	Elk kwartaal verplicht
<b>Service providers</b>	1	Alle VisaNet verwerkers (leden en niet-leden) en alle betalings gateways	Jaarlijks verplicht		Elk kwartaal verplicht
	2	Elke service provider die niet level 1 is en jaarlijks meer dan 1.000.000 Visa accounts/transacties opslaat, verwerkt of verzendt.	Jaarlijks verplicht		Elk kwartaal verplicht
	3	Elke service provider die niet level 1 is en jaarlijks minder dan 1.000.000 Visa accounts/transacties opslaat, verwerkt of verzendt.		Jaarlijks verplicht	Elk kwartaal verplicht

Figuur 1

*Beveilig Cardholder Data*

3. Beveilig opgeslagen cardholder data.
4. Encrypt cardholder data die over open, publieke netwerken verzonden wordt.

*Onderhoud een Vulnerability Management Programma*

5. Gebruik anti-virus software met up-to-date virusdefinities.
6. Ontwikkel en onderhoud afgeschermd systemen en applicaties.

*Implementeer sterke logische toegangsbeveiliging*

7. Scherm toegang tot cardholder data af op need-to-know basis.
8. Elke persoon met toegang tot systemen met cardholder data moet een unieke user-ID hebben.
9. Beperk fysieke toegang tot cardholder data.

*Monitor and Test Netwerken op reguliere basis*

10. Volg en monitor alle toegang tot netwerken en cardholder data.
11. Test de beveiliging van systemen en processen op periodieke basis.

*Onderhoud een Informatiebeveiligingsbeleid*

12. Onderhoud een beleid voor informatiebeveiliging.

**3. Consequenties van non-compliance met de PCI DSS standaard**

Visa leden kunnen bij non-compliance financiële sancties opgelegd krijgen tot 500 000 US dollar per incident. Voor leden die wel compliant zijn, maar Visa niet tijdig op de hoogte stellen van een (potentieel) verlies of diefstal van

data, kan de boete oplopen tot 100 000 US dollar per incident. Verder kan een creditcardmaatschappij een deelnemend lid hogere kosten per transactie opleggen totdat wordt voldaan aan de richtlijnen.

Het financiële risico wordt niet alleen gevormd door mogelijke boetes. Ten eerste vereist bijvoorbeeld de Amerikaanse wet dat alle klanten van de betreffende organisatie op de hoogte worden gesteld. Dit kan een kostbare exercitie zijn voor grote bedrijven. Ten tweede schakelt Visa bij incidenten een forensisch team in. De organisatie in kwestie krijgt hiervan de rekening gepresenteerd. Andere vormen van risico's kunnen reputatieschade en claims van gedupeerden zijn.

**4. Aanpak**

Vanuit een compliance-oogpunt is databeveiliging geen nieuw onderwerp. De meeste organisaties hebben al maatregelen getroffen om hun systemen te beschermen. Ondanks het feit dat PCI DSS geen richtlijnen biedt voor een volledig beveiligingsraamwerk, overlapt het deels met bekende standaarden als ISO 2700x en CobIT. Daarnaast hebben PCI DSS gerelateerde controles overlap met diverse controles vanuit externe wet- en regelgeving, zoals Sarbanes-Oxley en de Wet Bescherming Persoonsgegevens. Zowel in het kader van PCI DSS als in het kader van de Wet Bescherming Persoonsgegevens dient bijvoorbeeld monitoring van systeemtoegang plaats te vinden. In de praktijk maakt deze overlapping het voor organisaties haalbaar om aan de PCI DSS standaarden te voldoen zonder het gehele interne beveiligingsraamwerk aan te hoeven passen.

De al aanwezige standaarden kunnen worden gebruikt bij de implementatie van PCI DSS. Dit voorkomt redundantie in

de te implementeren beheersmaatregelen en beperkt de benodigde resources. Vanuit de compliancefunctie is het daarom verstandig te beginnen met het vergelijken van het PCI DSS controleraamwerk met intern bestaande controlemaatregelen. Op basis van dat inzicht kunnen de ontbrekende controlepunten gericht en efficiënt worden aangepakt. Vervolgens wordt PCI DSS compliance vooral een periodieke herijking. Aanvullend zou een continue content filtering van transacties kunnen plaatsvinden als detectieve maatregel.

Een organisatie die creditcardgegevens verwerkt blijft altijd verantwoordelijk voor de verwerking van deze gegevens. Dit geldt ook wanneer creditcarddiensten zijn uitbesteed aan derden (zogenoeten Service Providers) of door derden worden afgenomen (zogenoeten Merchants). De organisatie die deze diensten uitbesteedt moet tevens aan kunnen tonen dat de betreffende derden voldoen aan de PCI DSS standaard. De vereiste self-assessments, on-site audits en netwerk scans, uitgevoerd door daartoe gecertificeerde partijen, dienen contractueel te worden vastgelegd. Uiteindelijk bepaalt een creditcardmaatschappij, zoals Visa of Mastercard, of een organisatie voldoet aan de PCI DSS standaard of niet.

## 5. Valkuilen en lessen vanuit de praktijk

Bij implementatie van de PCI-standaarden kan aan een significant deel van de vereisten worden voldaan door een slimme aanpak en hergebruik van bestaande controlemaatregelen. Zowel functionarissen in compliancefuncties als in internal auditfuncties komen een aantal typische struikelblokken tegen. Voor zowel de compliancefunctie als de internal auditfunctie liggen de grootste struikelblokken op het gebied van:

- Organisatie (onvoldoende risicobewustzijn en onduidelijke of versnipperde verantwoordelijkheid).
- Inzicht in overige relevante wetgeving, interne en externe regelgeving en daarmee samenhangende controlemaatregelen die in de organisatie reeds zijn geïmplementeerd. Dit bemoeilijkt veelal het vaststellen van de potentiële overlap met het PCI DSS controleraamwerk.
- Contracten met derde partijen, waarbij de organisatie zelf de zaken wel goed op orde heeft, maar de betreffende partners niet. PCI DSS gaat uit van end-to-end verantwoordelijkheid, uitbesteding van procesonderdelen is dus geen uitbesteding van verantwoordelijkheid. Dit kan een lastig punt zijn bij langlopende contracten.

In de praktijk blijkt dat de bedrijven met de volgende karakteristieken een goede basis hebben voor een succesvolle PCI DSS implementatie:

### Organisatie

- Inzicht in de minimaal benodigde set van creditcardgegevens.
- Verankerde PCI DSS maatregelen in het beveiligingsbeleid en de beveiligingsstandaarden van het bedrijf.
- Een goed inzicht in de al binnen de organisatie geïmplementeerde controlemaatregelen, om efficiënt hergebruik van maatregelen mogelijk te maken.

### Infrastructuur

- Gebruik van netwerkcompartimentering en encryptie kan tot een duidelijke vermindering van nodige werkzaamheden leiden.
- Het zelf periodiek op hoog niveau IT risk-assessments uitvoeren stelt bedrijven in staat om PCI DSS zwakheden te identificeren en op te lossen.

### Monitoring proces

- Het op continue basis filteren van creditcardgegevens helpt bij de detectie van potentiële beveiligingsincidenten.
- De inrichting van een goed contractmanagement om richting derden het voldoen aan de PCI DSS-standaarden contractueel te bewerkstelligen en bij non-compliance aansprakelijkheid te regelen.
- De aanwezigheid van een compliance monitoringproces om naleving van de PCI DSS-standaard te kunnen waarborgen, de uitkomsten van relevante audits, self-assessments en netwerkscans te consolideren en daarover te rapporteren.

## 6. Conclusie

Een groeiend aantal bedrijven kiest ervoor om aan de PCI DSS standaard te voldoen. Betaalgemak voor de klant is belangrijk, maar bescherming van de persoonlijke en financiële gegevens verdienen evenzeer aandacht. Daarbij lopen bedrijven grotere financiële en reputatierisico's door een toenemend internationaal gebruik van creditcards.

Het is sterk aan te bevelen om PCI DSS niet op zichzelf te beschouwen. Ten eerste overlapt deze standaard met reeds aanwezige beveiligingsvereisten zoals de eerder aangegeven ISO 2700x en Wet Bescherming Persoonsgegevens. Ten tweede hebben veel bedrijven al een bestaande set aan beveiligingsmaatregelen, -processen en -procedures. Weten welke controles reeds in de organisatie zijn geïmplementeerd vanuit wet- en regelgeving en interne beveiligingsstandaarden, levert een efficiëntere en effectievere invoering van PCI DSS op. Een efficiëntere invoering, omdat het opnieuw implementeren van al bestaande controles zoveel mogelijk wordt voorkomen. Een effectievere invoering, omdat PCI DSS beter wordt geïntegreerd in de operationele uitvoering van de organisatie.

Voor de Compliance Officer ligt de uitdaging vooral in een goede samenwerking tussen Business en IT, operationeel risk management en de interne audit afdeling. In de situatie dat diensten zijn uitbesteed, zal een nauwe samenwerking met contractmanagement eveneens van toepassing zijn.