

## Hoe veilig zijn de creditcard gegevens van mijn klanten?

De winkelier op de hoek, een bank of een internationale retail keten, elke organisatie die met creditcard transacties werkt, heeft te maken met de Payment Card Industrie Data Security Standard (PCI DSS). Een standaard die het toenemende aantal creditcard fraudes dient te beperken. De geleden schade loopt namelijk wereldwijd op tot meer dan 3 miljard US dollar (bron: pci-dss-made-easy). Deze zal naar verwachting alleen maar toenemen door het groeiende aantal verkopen via e-commerce.

Op 17 januari 2007 gaf TJX Companies Inc. aan dat de opgeslagen creditcard gegevens van sommige van zijn winkels mogelijk was benaderd. Dit betrof circa 45 miljoen cards. De totale kosten van deze fraude worden geschat op 25 tot 256 miljoen US dollar.  
Bron: <http://www.boston.com>

Als gevolg van de stijgende risico's en de toenemende belangen heeft de PCI Security Standards Council in december 2004 PCI DSS geïntroduceerd. PCI Council is een samenwerkingsverband van American Express, Discover Financial Services, JCB, MasterCard Worldwide en Visa International.

Hoewel de PCI DSS een Amerikaanse norm is, is deze standaard vereist voor alle organisaties die creditcard transacties verwerken, verzenden of hierover rapporteren. PCI DSS bestaat uit 6 principes die opgedeeld zijn in 12 aandachtsgebieden. In oktober 2008 komt de nieuwste versie uit, PCI DSS 1.2.

<i>Bouw en onderhoud een beveiligd netwerk</i>	
1	Installeer en onderhoud een firewall om card gegevens te beschermen
2	Gebruik geen standaard wachtwoorden voor systemen en beveiligingsinstellingen
<i>Beveilig Cardholder Data</i>	
3	Beveilig opgeslagen cardholder data.
4	Encrypt cardholder data die over open, publieke netwerken verzonden wordt.
<i>Onderhoud een Vulnerability Management Programma</i>	
5	Gebruik anti-virus software met up-to-date virus definities.
6	Ontwikkel en onderhoud afgeschermd systemen en applicaties.
<i>Implementeer sterke logische toegangsbeveiliging</i>	
7	Schermt 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.
<i>Monitor and Test Netwerken op reguliere basis</i>	
10	Volg en monitor alle toegang tot netwerken en cardholder data.
11	Test de beveiliging van systemen en processen op periodieke basis.
<i>Onderhoud een Informatie beveiligingsbeleid</i>	
12	Onderhoud een beleid voor informatie beveiliging

Onderdeel van PCI DSS is het periodiek uitvoeren van een review en hierover verantwoording afleggen. Mede afhankelijk van het transactievolume houdt een dergelijke review in een volledige audit of een risk self assessment. De exacte vereisten zijn te vinden op [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

### *Non-compliance*

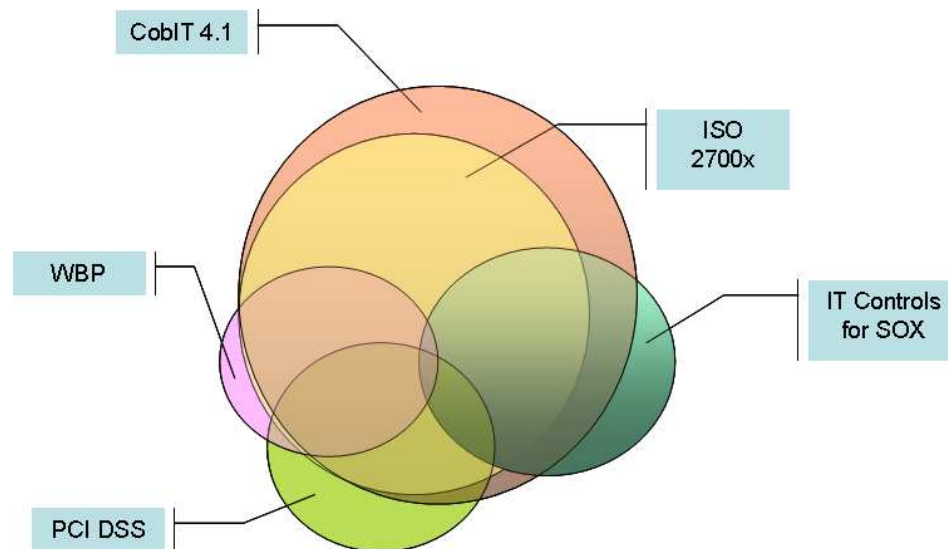
Bij non-compliance kunnen financiële sancties worden opgelegd. Zo kan Visa zijn leden tot 500.000 dollar per incident beboeten. Als een lid Visa niet op de hoogte stelt van een (potentieel) verlies of diefstal van data, dan kan dit bedrag oplopen tot 100.000 dollar per incident.

Het financiële risico wordt niet alleen gevormd door mogelijke boetes. Ten eerste vereist 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 zijn en claims van gedeputeerden.

### Aanpak

Dataveiligheid is geen nieuw onderwerp en de meeste organisaties hebben al maatregelen getroffen om hun systemen te beschermen. Ondanks dat PCI DSS geen richtlijnen biedt voor een volledig beveiligingsraamwerk, overlapt het deels met bekende standaarden als ISO 2700x en CobIT. Tevens heeft PCI DSS overlap met Sarbanes-Oxley en de Wet Bescherming Persoonsgegevens.



De meeste bedrijven kunnen dus gebruik maken van al aanwezige standaarden bij de implementatie van PCI DSS. Dit voorkomt redundantie in de te implementeren beheersmaatregelen en beperkt de benodigde IT resources. Het is daarom verstandig om te beginnen met een analyse van de betrokken systemen en het aanwezige beveiligingsniveau binnen een bedrijf. Op basis van dat inzicht kunnen de ontbrekende punten gericht en efficiënt worden aangepakt, waarna PCI DSS compliance een periodieke herijking wordt.

Een periodieke herijking omvat een netwerk scan, aangevuld met een risk self assessment of volledige audit. Netwerk scans dienen alleen te mogen worden uitgevoerd door Approved Scan Vendor (ASV) gecertificeerde bedrijven. Voor een audit kan een Qualified Security Assessor (QSA) gecertificeerd bedrijf worden ingehuurd. Grote organisaties kunnen een dergelijke audit ook intern laten uitvoeren, mits de benodigde kennis beschikbaar is en het bedrijf officieel aftekent.

### Valkuilen en lessen vanuit de praktijk

Bij implementatie van de PCI standaarden kan een significant deel van de vereisten door een slimme aanpak en hergebruik verminderd worden. Toch is er een aantal typische struikelblokken dat vaak naar boven komt. De grootste struikelblokken voor organisaties liggen op het gebied van:

- Organisatie (onvoldoende risico bewustzijn en onduidelijke of versnipperde verantwoordelijkheid voor IT-beveiliging)
- Infrastructuur (zwak encryptie proces, gebrekkige documentatie en verouderde systemen met zwakke beveiliging/protocollen)
- 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, outsourcing van procesonderdelen is dus geen outsourcing 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 creditcard gegevens
  - Verankerde PCI DSS maatregelen in het beveiligingsbeleid en de beveiligingsstandaarden van het bedrijf.
  - Een goed begrip van het huidige volwassenheidsniveau, om efficiënt hergebruik van maatregelen mogelijk te maken.
- Infrastructuur
  - Gebruik van netwerk compartimentering 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
  - Effectieve monitoring van log-bestanden helpt in de detectie van potentiële beveiligingsincidenten

### **Conclusie**

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

Het is sterk aan te bevelen om PCI standaarden niet op zichzelf te beschouwen. Ten eerste overlappen PCI standaarden deels met standaarden als ISO 27001 en Wet Bescherming Persoonsgegevens. Ten tweede hebben veel bedrijven al een bestaande set aan beveiligingsmaatregelen, -processen en -procedures. Het combineren van deze beide punten levert een efficiënte en effectieve invoering op.