

## PCI DSS gemakkelijk gemaakt

De PCI DSS norm (Payment Card Industry Data Security Standard)

De grote creditcardmaatschappijen streven ernaar om de financiële fraude-incidenten, waarmee verschillende soorten organisaties en hun consumenten geconfronteerd zijn, te stoppen. Daarom zijn organisaties die betalingstransacties uitvoeren, verplicht om tegen eind 2007 te voldoen aan de PCI DSS norm. Organisaties die hieraan niet voldoen, lopen het risico dat ze geen gegevens van kaarthouders meer mogen verwerken en kunnen geconfronteerd worden met boetes van tot \$500.000 wanneer de gegevens verloren of gestolen zijn. In dit white paper wordt aandacht besteed aan de noodzakelijke eisen om aan de PCI DSS norm te voldoen, de implicaties van niet-naleving alsook de rol van event log management en netwerk risicomangement bij het bereiken van de naleving van deze norm.

---

## Inleiding

Creditcards worden wereldwijd geaccepteerd en het gebruik van deze kaarten voor online betalingen neemt drastisch toe. In 2004 waren er in de Verenigde Staten 1,3 miljard creditcards in omloop, waarvan 76% van de Amerikanen minstens een creditcard hebben. De omzet van de Amerikaanse retail e-commerce was in het vierde kwartaal van 2006 \$33,9 miljard, een stijging van 25% over hetzelfde kwartaal in 2005.

Er is echter slecht nieuws: Van alle gemelde incidenten in 2006 was creditcardfraude (met 25%) de meest voorkomende vorm van identiteitsdiefstal. Gezien dat financiële ondernemingen en bedrijven hierdoor een verlies van méér dan \$48 miljard opliepen en particulieren een verlies van \$5 miljard, kan men zeggen dat creditcardfraude iedereen diep in de beurs tast. Bovendien stijgt de fraude in e-commerce. Met een stijging van 7% ten opzichte van het jaar 2005 bedraagt de schade in 2006 \$3 miljard. Dit white paper beschrijft de consequenties van gegevensdiefstal van kaarthouders en besteed aandacht aan de volgende belangrijke vragen:

- Wat is de PCI norm?
- Waarom is het voor uw onderneming belangrijk om aan deze norm te voldoen?
- Wat zijn de consequenties bij niet-naleving?
- Welke oplossingen zijn er voor de naleving van de PCI norm?

---

## Diefstal van gegevens van kaarthouders en fraude – enkele waargebeurde gevallen

- 18 februari 2005 – Bank of America beweerde een verlies van méér dan 1,2 miljoen klantengegevens te hebben opgelopen. De bank vermeldde echter dat er geen bewijs is dat de gegevens in de handen van criminelen zijn beland.
- 16 juni 2005 – CardSystems, een Amerikaanse provider die betalingstransacties verwerkt in opdracht van handelaren/verkopers, werd verschillende keren aangeklaagd wegens het falen om persoonlijke informatie van 40 miljoen klanten adequaat te beschermen. CardSystems zag een ondergang onder ogen, aangezien VISA en American Express de relatie met de onderneming hadden verbroken en waardoor de onderneming hun kaartgegevens niet meer mocht verwerken. CardSystems werd vervolgens door een ander bedrijf overgekocht.
- 9 februari 2006 – Ongeveer 200.000 debitcardaccounts waren door onbekende detailhandelaren, waarschijnlijk OfficeMax en anderen, gelekt. Hieronder vielen accounts met betrekking tot nationale banken en kredietverstrekkers, zoals CitiBank en Wells Fargo.
- 31 januari 2006 – Boston Globe en The Worcester Telegram & Gazette hebben onbewust

240.000 credit- en debitcardgegevens gelekt en ook routeringsinformatie voor persoonlijke onderzoeken, die op kringlooppapier van krantenpakketten voor distributie waren gedrukt.

- 12 januari 2007 – MoneyGram, een provider voor betalingstransacties, deelde mee dat een bedrijfserver afgelopen maand illegaal toegang via het internet had verkregen. Deze server bevatte gegevens van ongeveer 79.000 klanten, die betalingen verrichtten tussen verschillende rekeningen (bill payment), inclusief namen, adressen, telefoonnummer en bij enkele gevallen, zelfs banknummers.
- 17 januari 2007 – TJX Companies Inc. maakte bekend dat een buitenstaander ongeautoriseerde toegang tot het elektronische verwerkingssysteem van credit-/debitcards had verkregen. Deze inbraak behoort tot op heden tot de meest opmerkelijke inbraken op het netwerk; 45.700.000 credit-/debitcardnummers en méér dan 455.000 gegevens over de handel in goederen en diensten (inclusief namen van klanten en nummers van rijbewijzen) waren van het IT-systeem van de onderneming gestolen.

Er wordt niet alleen op de grote online detailhandelaren gericht. De publieke aandacht kan op opvallende gegevensverliezen zijn gericht, maar deskundigen die financiële fraude onderzoeken, zeggen dat hackers zich steeds meer op kleinere, commerciële websites richten. In sommige gevallen zijn criminelen in staat om realtime toegang te verkrijgen tot transactie-informatie van de websites, waardoor zij geldige creditcardnummers kunnen stelen en snel grote aantallen frauduleuze aankopen kunnen doen. Bij kleine e-businesses vallen er minder slachtoffers, maar zij vormen wel een gemakkelijk doel, hetzij door defecten in de software die handelaren gebruiken om online bestellingen te verwerken, hetzij door een te groot vertrouwen in de veiligheid van outsourcing websites.

Het vertrouwen van gebruikers en consumenten wordt door cybercriminaliteit en het gevaar op identiteitsdiefstal verminderd, waardoor e-commerce niet altijd geaccepteerd wordt. Hierdoor is computerbeveiliging, een kritieke activiteit voor de bescherming van deze systemen, rechtswege een belangrijke maatregel geworden.

---

## **PCI-norm (Payment Card Industry)**

De PCI-norm (Payment Card Industry) voor gegevensbeveiliging was door American Express, Discover Financial Services, JCB, MasterCard Worldwide en Visa International ontwikkeld. Elk van deze organisaties had voor 2004 eigen eisen met betrekking tot informatiebeveiliging. Deze eisen waren vaak moeilijk en herhalend voor deelnemers in meerdere netwerken. De organisaties ontwikkelden vervolgens een aantal uniforme eisen met betrekking tot informatiebeveiliging voor alle nationale merken debit-/creditcards (exclusief winkelmerken en huismerken). Deze eisen werden onder de naam PCI DSS (PCI Data Security Standard) bekend en bepalen alle betaalkanalen: detailhandel, postorder, telefonische bestellingen en e-commerce.

## De PCI DSS-norm

De PCI DSS-norm bestaat uit 12 beveiligingseisen (volgens VISA verwijzen deze naar de 'Digital Dozen') die in de volgende zes categorieën zijn onderverdeeld:

PCI DSS
<b>Een veilig netwerk installeren en onderhouden</b>
Eis 1: Een firewallconfiguratie installeren en onderhouden om gegevens van kaarthouders te beschermen
Eis 2: Geen door verkopers geleverde standaardwaarden gebruiken voor systeemwachtwoorden en andere veiligheidparameters
<b>Gegevens van kaarthouders beschermen</b>
Eis 3: Opgeslagen gegevens van kaarthouders beschermen
Eis 4: Gegevens van kaarthouders over open, publieke netwerken coderen
<b>Een programma voor risicomanagement uitvoeren</b>
Eis 5: Antivirussoftware of –programma's gebruiken en regelmatig updaten
Eis 6: Veilige systemen en applicaties ontwikkelen en onderhouden
<b>Strengere maatregelen met betrekking tot toegangsbeheer toepassen</b>
Eis 7: Een beperking leggen op de toegang tot gegevens van kaarthouders door need-to-know van ondernemingen
Eis 8: Een uniek ID toewijzen aan elke persoon met toegang tot een computer
Eis 9: Fysieke toegang tot gegevens van kaarthouders beperken
<b>Netwerken regelmatig monitoren en testen</b>
Eis 10: Alle toegang tot netwerkbronnen en gegevens van kaarthouders traceren en monitoren
Eis 11: Beveiligingssystemen en –processen regelmatig testen
Een beleid met betrekking tot informatiebeveiliging handhaven
Eis 12: Een beleid handhaven inzake informatiebeveiliging voor werknemers en contractanten

**Table 1: Het PCI DSS raamwerk**

Naleving van deze eisen kan in 3 belangrijke stadia samengevat worden:

- **Verzameling en opslag:** Veilige verzameling en opslag van alle log data, waarmee niet geknoeid kan worden, zodat deze voor analyse beschikbaar zijn.
- **Verslaggeving:** Het in staat zijn om naleving, indien geaudit, te bewijzen en aantonen dat de normen inzake gegevensbescherming van kracht zijn.
- **Monitoring en alerting:** Het in bezit zijn van systemen, zoals auto-alerting, om beheerders te helpen om continu de toegang tot en het gebruik van gegevens te monitoren. Beheerders worden onmiddellijk gewaarschuwd wanneer er problemen optreden en kunnen deze snel aanpakken. Bovendien zouden deze systemen zich tot de log data moeten uitbreiden – er

moet een bewijs zijn dat log data verzameld en opgeslagen wordt.

## Niveaus van handelaren/verkopers en service providers

Handelaren/verkopers en service providers die aan de PCI DSS moeten voldoen, worden gecategoriseerd naar het aantal transacties die zij gedurende een periode van 12 maanden hebben uitgevoerd. Tabel 2 en 3 hieronder beschrijven de verschillende soorten niveaus en de eisen van naleving voor zowel handelaren/verkopers alsook service providers.

**Handelaren/verkopers** zijn geautoriseerde ontvangers van credit-/debitcards voor betalingen van goederen en diensten. Voorbeelden van industrieën waar handelaren/verkopers verplicht zijn om aan deze normen te voldoen, zijn onder andere, maar niet beperkt tot:

- Online handel, zoals Amazon.com online retailer
- Detailhandel, zoals Wal-Mart
- Hoger onderwijs, zoals universiteiten
- Gezondheidszorg, zoals ziekenhuizen
- Toerisme en recreatie, zoals hotels en restaurants
- Energie, zoals tankstations
- Financiën, zoals banken en verzekeringsmaatschappijen

Niveaus van handelaren/verkopers	
DEFINITIE HANDELAREN/VERKOPERS*	DEFINITIE HANDELAREN/VERKOPERS**
<b>Niveau 1</b>	
<ul style="list-style-type: none"> <li>• Handelaren/verkopers waarvan de gegevens van kaarthouders in gevaar gebracht zijn</li> <li>• Handelaren/verkopers met jaarlijks méér dan zes miljoen creditcardtransacties via alle kanalen, waaronder e-commerce</li> </ul>	<ul style="list-style-type: none"> <li>• Handelaren/verkopers waarvan de gegevens van kaarthouders in gevaar gebracht zijn</li> <li>• Handelaren/verkopers met jaarlijks méér dan zes miljoen creditcardtransacties via alle kanalen, waaronder e-commerce</li> </ul>
<b>Niveau 2</b>	
<ul style="list-style-type: none"> <li>• Handelaren/verkopers met jaarlijks 1 tot 6 miljoen creditcardtransacties</li> </ul>	<ul style="list-style-type: none"> <li>• Handelaren/verkopers met jaarlijks 1 tot 6 miljoen creditcardtransacties</li> </ul>
<b>Niveau 3</b>	
<ul style="list-style-type: none"> <li>• Handelaren/verkopers met jaarlijks 20.000 tot 1.000.000 creditcardtransacties</li> </ul>	<ul style="list-style-type: none"> <li>• Handelaren/verkopers met jaarlijks 20.000 tot 1.000.000 creditcardtransacties</li> </ul>
<b>Niveau 4 **</b>	
<ul style="list-style-type: none"> <li>• Alle andere handelaren/verkopers</li> </ul>	<ul style="list-style-type: none"> <li>• Alle andere handelaren/verkopers</li> </ul>

**Tabel 2: Niveaus van handelaren/verkopers**

\* De niveaus van handelaren/verkopers zijn gebaseerd op de definities van VISA USA

\*\* De PCI DSS vereist dat alle handelaren/verkopers externe netwerkscans uitvoeren om naleving te bereiken. Afnemers

kunnen vragen naar scanrapporten en/of ingevulde vragenlijsten van handelaren/verkopers van niveau 4.

**Service providers** zijn organisaties die gegevens van kaarthouders verwerken, opslaan of verstrekken namens credit-/debitcardbezitters, handelaren/verkopers of andere service providers. Voorbeelden van service providers die aan de PCI DSS norm moeten voldoen, zijn onder andere, maar niet beperkt tot:

- Betalingsgateways
- E-commerce hosting providers
- Managed Service Providers (MSP's)
- Ondernemingen met betrekking tot kredietrapportages
- Ondernemingen met betrekking tot backup management
- Papierverwerkende bedrijven

DEFINITIE SERVICE PROVIDER	NALEVING
<b>Niveau 1</b>	
Alle organisaties die credit/debitcardgegevens verwerken (leden en niet-leden) en alle betalingsgateways.*	Jaarlijkse, plaatselijke evaluatie van PCI Data Security en ieder kwartaal netwerkscans
<b>Niveau 2</b>	
Elke service provider die niet tot niveau 1 behoort en jaarlijks méér dan 1 miljoen creditcardrekeningen/-transacties opslaat, verwerkt of verstrekt	Jaarlijkse, plaatselijke evaluatie van PCI Data Security en ieder kwartaal netwerkscans
<b>Niveau 3</b>	
Elke service provider die niet tot niveau 1 behoort en jaarlijks minder dan 1.000.000 creditcardrekeningen/-transacties opslaat, verwerkt of verstrekt	Jaarlijkse vragenlijst voor zelfevaluatie en ieder kwartaal netwerkscans

**Table 3: Niveaus service providers**

\* Betalingsgateways zijn agenten of service providers die gegevens van kaarthouders opslaan, verwerken en/of verstrekken in het kader van een betalingstransactie (bijvoorbeeld PayPal). Zij maken betalingstransacties mogelijk (bv. machtiging of betaling) tussen handelaren/verkopers en organisaties die credit-/debitcards verwerken (bijvoorbeeld VisaNet endpoints). Handelaren/verkopers kunnen hun betalingstransacties direct naar een endpoint sturen of indirect naar een betalingsgateway. Strenge deadlines voor naleving.

De grootste creditcardmaatschappijen streven ernaar dat handelaren/verkopers aan de PCI DSS norm voldoen. Verschillende deadlines zijn vastgesteld en zware sancties en boetes worden opgelegd voor organisaties die falen om op tijd aan deze norm te voldoen. De belangrijkste deadlines die Visa USA heeft vastgelegd, zijn:

- 31 maart 2007 – De deadline waarbij handelaren/verkopers van niveau 1 en 2 aan moeten

tonen dat zij geen volledige track data, CVV2 of PIN-gegevens opslaan.

- 30 september 2007 – De dag waarop alle handelaren/verkopers van niveau 1 verwacht worden volledig aan de PCI DSS norm te voldoen.
- 31 december 2007 – De dag waarop alle handelaren/verkopers van niveau 2 verwacht worden volledig aan de PCI DSS-norm te voldoen.

De deadlines voor naleving kunnen tussen creditcardmaatschappijen en regio's verschillen; daarom dienen onzekere handelaren/verkopers en service providers afnemers of creditcardmaatschappijen voor de respectievelijke deadlines raadplegen .

---

## **Waarom is het voor uw onderneming belangrijk om aan deze richtlijn te voldoen?**

Hoewel de PCI DSS een Amerikaanse norm is, is deze eis wereldwijd voor alle entiteiten die gegevens van kaarthouders verwerken, vereist. Niet alle landen zijn hiervan bewust. In Australië, bijvoorbeeld, leidde de wijdverspreide verwarring over de nieuwe nalevingsmaatregelen bij banken tot vijf inbraken in 2006.

Het is in het eigen belang van ontvangende banken om ervoor te zorgen dat hun handelaren/verkopers bewust zijn van de naleving van de PCI DSS. De reden is vrij logisch: Ontvangende banken spelen de belangrijkste rol bij het opbouwen van een vertrouwensband tussen creditcardmaatschappijen en handelaren/verkopers. Daarom zijn zij ook degene die onmiddellijk in de vuurlinie van credit-/debitcardmaatschappijen terecht komen wanneer een of meerdere handelaren/verkopers van hun door een inbraak getroffen worden. Om een goede en succesvolle zakenrelatie met creditcardmaatschappijen te onderhouden, moeten ontvangende banken ervoor zorgen dat hun handelaren/verkopers adequaat beschermd zijn; en PCI DSS is dé tool die de bescherming van gegevens van kaarthouders aan de kant van de handelaar/verkoper bepaalt.

Evenzo wordt er verwacht dat handelaren/verkopers en service providers aangeven tot welk niveau van naleving van de PCI DSS zij behoren. Hierdoor wordt een goede zakenrelatie met ontvangende banken onderhouden en worden consequenties van niet-naleving voorkomen.

---

## **Wat zijn de consequenties van niet-naleving?**

Creditcardmaatschappijen kunnen boetes op hun leden (banken) leggen, wanneer blijkt dat handelaren/verkopers niet aan de PCI DSS norm voldoen. Ontvangende banken mogen op hun beurt handelaren/verkopers contractueel verplichten de schade te vergoeden en hun van dergelijke boetes schadeloos te stellen. Boetes kunnen tot \$500.000 per incident oplopen, als gegevens in gevaar gebracht zijn en als blijkt dat handelaren/verkopers niet aan de PCI DSS norm voldoen. In het ergste geval kan het voorkomen dat handelaren/verkopers geen

creditcardtransacties voor klanten meer mogen uitvoeren.

Ondernemingen waarvan de gegevens van kaarthouders in gevaar gebracht zijn, zijn verplicht om overheidsinstanties hiervan op de hoogte te stellen en worden verwacht gratis kredietbeschermingsdiensten aan te bieden aan degene die mogelijkervijze getroffen zijn.

Naast deze boetes kunnen er nog andere consequenties zijn. Verlies van gegevens van kaarthouders, hetzij per ongeluk, hetzij door diefstal, kan ook tot door kaarthouders ondernomen gerechtelijke stappen leiden. Dergelijke stappen leiden tot slechte publiciteit, waardoor vervolgens bedrijfsschade kan ontstaan.

---

## **Welke oplossingen biedt GFI aan om u bij de naleving van de PCI eisen te helpen?**

Technologische oplossingen kunnen geïmplementeerd worden om een aantal taken, die u moet ondernemen om aan de PCI eisen te voldoen, te automatiseren. Deze oplossingen stellen u in staat om de naleving van de norm te monitoren en waarschuwen u wanneer ongeautoriseerde events met betrekking tot gegevens van kaarthouders zich voordoen. GFI biedt softwaretools aan die u hierbij helpen.

GFI EventsManager, GFI LANguard Network Security Scanner (N.S.S.) en GFI EndPointSecurity zijn drie awardwinnende GFI producten voor netwerkbeveiliging. Door middel van auditing, monitoring, verslaggeving en alerting kunnen deze producten u helpen meerdere onderdelen in negen van de twaalf PCI eisen aan te pakken.

PCI DSS EISEN			
	GFI EventsManager	GFI LANguard N.S.S.	GFI EndPointSecurity
1. Een firewallconfiguratie installeren en onderhouden om gegevens van kaarthouders te beschermen	•	•	
2. Geen door verkopers geleverde standaardwaarden gebruiken voor systeemwachtwoorden en andere veiligheidsparameters	•	•	
3. Opgeslagen gegevens van kaarthouders beschermen	•		•
4. Gegevens van kaarthouders over open, publieke netwerken coderen			
5. Antivirussoftware of –programma's gebruiken en regelmatig updaten		•	
6. Veilige systemen en applicaties ontwikkelen en onderhouden		•	
7. Een beperking leggen op de toegang tot gegevens van kaarthouders door need-to-know van ondernemingen	•		
8. Een uniek ID toewijzen aan elke persoon met toegang tot een computer	•	•	
9. Fysieke toegang tot gegevens van kaarthouders beperken			
10. Alle toegang tot netwerkbronnen en gegevens van kaarthouders traceren en monitoren	•	•	
11. Beveiligingssystemen en -processen regelmatig testen	•	•	•
12. Een beleid handhaven inzake informatiebeveiliging voor werknemers en contractanten			

Tabel 4: PCI DSS Eisen

## **GFI EventsManager**

Analyse van events data is in eis 10 omschreven (tabel 4 hierboven), maar het is ook goed voor elke onderneming om events te monitoren.

Events data (van grote omvang en van cryptische aard) wordt in een typische netwerkgeving geanalyseerd. De tools voor de event analyse, die standaard in de meeste besturingssystemen geïnstalleerd zijn, bieden slechts de basiskenmerken. Daarom hebben beheerders geen middelen om gewaarschuwd te worden als bepaalde, belangrijke of problematische events zich voordoen, zoals de ongeautoriseerde toegang van gegevens van kaarthouders. De tools om door events te bladeren en te filteren die door bovengenoemde tools geleverd worden, hebben zeer beperkte zoek- en filtermogelijkheden.

GFI EventsManager is een volledige oplossing voor log management die al deze problemen oplost en u in staat stelt om events te centraliseren, verzameling van events automatisch te genereren, alerts te ontvangen en onderzoeksrapporten op te stellen. Bij het verzamelen van events verwerken de ingebouwde rules de events om deze te classificeren en vervolgens alerts/acties te genereren. Een van de standaardregels richt zich specifiek op de verzameling van events op basis van de PCI eisen. Analyse van events kan door middel van de ingebouwde events browser uitgevoerd worden; onderzoeken kunnen ook opgezet en uitgevoerd worden om specifieke events te herstellen en te analyseren.

Door middel van GFI EventsManager kunnen ondernemingen verzekeren dat alle events met betrekking tot gegevens van kaarthouders constant gemonitord worden. U kunt meer informatie vinden en het product downloaden op: <http://www.gfi.nl/nl/eventsmanager/>.

## **GFI LANguard Network Security Scanner**

Risicomanagement is voor eis 5 en 6 (tabel 4 hierboven) van belang. Het is echter zéér belangrijk om kwetsbaarheden op verschillende locaties, die onder andere eisen vallen, te detecteren.

GFI LANguard Network Security Scanner (N.S.S.) richt zich op drie pijlers van risicomanagement: veiligheidsscans, patchmanagement en netwerkcontrole in één geïntegreerde oplossing. GFI LANguard N.S.S. scant het gehele netwerk op méér dan 15.000 kwetsbaarheden, identificeert alle mogelijke veiligheidsproblemen en biedt beheerders de tools aan die zij nodig hebben om zwakheden te beoordelen, vast te stellen, te melden en te herstellen voordat hackers deze kunnen vinden.

Bij de aanpak van problemen met betrekking tot veiligheidsproblemen, patchmanagement en netwerkcontrole, is het gebruik van meerdere producten voor beheerders soms van groot belang. Ze moeten niet alleen leren om meerdere oplossingen te gebruiken, te beheren en installeren, maar ook, en hieraan besteden ze de meeste tijd, proberen te begrijpen wáár de problemen liggen in plaats van zich op de mogelijk aanwezige risico's te richten. De geïntegreerde oplossing van GFI LANguard N.S.S. helpt beheerders door middel van één

enkele console met uitgebreide rapportagefunctionaliteit deze problemen sneller en effectiever aan te pakken.

Door middel van GFI LANguard N.S.S. kunnen ondernemingen er zeker van zijn dat de gegevens van kaarthouders in een veilige omgeving onderhouden worden. U kunt meer informatie vinden en het product downloaden op: <http://www.gfi.nl/nl/lannetscan/>.

### **GFI EndPointSecurity**

De bescherming van opgeslagen gegevens van kaarthouders (tabel 4 hierboven) is een belangrijke eis van de PCI DSS. Het is zéér belangrijk om te zorgen dat deze gegevens niet in de verkeerde handen vallen.

Het is wel bekend dat vele opslagmedia, zoals USB-pen drives, de laatste aantal jaren in populariteit zijn gegroeid. Ze zijn gemakkelijk en snel te installeren, kunnen grote hoeveelheden gegevens opslaan, en zijn klein genoeg om in een broekzak mee te nemen. Zonder een beveiligingsmechanisme kan een dergelijk apparaat gemakkelijk en snel alle gegevens van kaarthouders kopiëren.

GFI EndPointSecurity is de veiligheidsoplossing die u helpt de gegevensintegriteit te behouden door te voorkomen dat gegevens van en naar de draagbare opslagmedia ongeautoriseerd worden overgebracht. GFI EndPointSecurity stelt u door middel van zijn technologie in staat om toegang tot een bepaald apparaat al dan niet toe te staan en (waar toepasselijk) voor ieder ondersteund apparaat 'alleen lezen' of 'volledige' toegangsrechten toe te kennen of een lokale of Active Directory gebruiker/groep toe te wijzen. Door middel van GFI EndPointSecurity kunt u de activiteit van alle draagbare media die op de computers van uw netwerk worden gebruikt, registreren, inclusief de datum/tijd van gebruik en de persoon wie deze media heeft gebruikt.

Door middel van GFI EndPointSecurity kunnen ondernemingen er zeker van zijn dat gegevens van kaarthouders niet op ongeautoriseerde opslagmedia gekopieerd worden. U kunt meer informatie vinden en het product downloaden op: <http://www.gfi.nl/nl/endpointsecurity/>.

### **GFI ReportCenter**

GFI ReportCenter is een gecentraliseerd rapportageraamwerk waarmee u diverse rapporten kunt opstellen door middel van gegevens die door elk GFI product is verzameld. GFI EventsManager, GFI LANguard N.S.S. en GFI EndPointSecurity bieden allemaal ReportPacks die u op het raamwerk van GFI ReportCenter kunt aansluiten.

Deze ReportPacks zijn sterke, toegevoegde rapportagetools met verscheidene, voorgeconfigureerde rapporten. Bovendien bevatten de ReportPacks een aantal uitgebreide kenmerken, zoals planning en export van rapporten en distributie van rapporten via e-mail. Rapporten die door middel van ReportPacks gegenereerd worden, zijn voor ondernemingen van groot belang bij de beoordeling van de effectiviteit van hun PCI nalevingsprogramma. U kunt meer informatie vinden en een ReportPack downloaden op:

<http://www.gfi.nl/nl/reportcenter/>.

## Stimulans

Het is voor organisaties die gegevens van creditcards verwerken van groot belang te voldoen aan de PCI DSS. Tevens is voor banken belangrijk om er zeker van te zijn dat handelaren/verkopers aan de PCI norm voldoen.

Banken zouden, als deel van de overeenkomst, handelaren/verkopers bij de naleving kunnen stimuleren door hun GFI licenties aan te bieden voor producten voor netwerkbeveiliging. Bovendien kunnen zij extra diensten aanbieden, zoals technische expertise van de GFI producten. Dit zou vele voordelen met zich mee kunnen brengen, aangezien handelaren/verkopers een mate van veiligheid kunnen bereiken door aan de PCI DSS te voldoen. Daarnaast kunnen ze ook van alle andere voordelen profiteren die de producten van GFI aanbieden. Banken kunnen ook een mate van veiligheid bereiken door te realiseren dat de handelaren/verkopers, die zij toestemming hebben verleend om betalingen van creditcards te accepteren, een grote stap hebben genomen naar de het bereiken van de naleving van de PCI.

---

## Conclusie

Ondernemingen lopen constant het risico om gevoelige gegevens van kaarthouders te verliezen. Dergelijk verlies kan leiden tot boetes, gerechtelijke stappen en slechte publiciteit. Dit kan op zijn beurt leiden tot bedrijfsschade. Naleving van de PCI DSS moet daarom bij ondernemingen die creditcardtransacties uitvoeren, hoog op de agenda staan.

Door softwaretools voor log management, risicomanagement, veiligheidsscans en endpoint security te installeren, heeft u nog lang niet de naleving van de PCI norm bereikt. GFI's producten voor netwerkbeveiliging kunnen u helpen de naleving van deze norm te bereiken.

---

## Over GFI

GFI is een toonaangevende ontwikkelaar van software voor netwerkbeveiliging, inhoudsbeveiliging en messaging. Dankzij bekroonde technologie, een agressieve prijsstrategie en een sterke focus op MKB-bedrijven helpt GFI bedrijven over de hele wereld om maximale continuïteit en productiviteit te bewerkstelligen. GFI is opgericht in 1992 en heeft kantoren in Malta, Londen, Raleigh, Hong Kong, Adelaide en Hamburg die wereldwijd meer dan 200.000 installaties ondersteunen. GFI is een kanaalgericht bedrijf met meer dan 10.000 partners over de hele wereld. GFI is ook een Microsoft Gold Certified Partner. Meer informatie over GFI is te vinden op <http://www.gfi.nl>.

---

## Referenties

CreditCards.com (2006) *Credit Card Industry Facts and Personal Debt Statistics* beschikbaar op: <http://www.creditcards.com/statistics/statistics.php> (laatst bewerkt 29 dec 2006).

U.S. Census Bureau (2006) *Quarterly retail e-commerce sales 2nd quarter 2006* beschikbaar op: <http://www.census.gov/mrts/www/data/html/06Q2.html> (laatst bewerkt 29 dec 2006).

Federal Trade Commission (2006) *Consumer Fraud and Identity Theft Complaint Data januari – december 2005*.

United States Postal Service *Identity Theft: Stealing Your Name and Your Money* beschikbaar op: <http://www.usps.com/postalinspectors/IDtheft2.htm> (laatst bewerkt 29 dec 2006).

Bednarz A. (2006) *Online merchants will lose \$3 billion to fraud in 2006*, Network World, Inc. beschikbaar op: <http://www.networkworld.com/news/2006/111406-online-merchants-fraud.html?nlhtsec=1113securityalert2> (laatst bewerkt 29 dec 2006).

Marlin S. (2005) *Customer Data Losses Blamed On Merchants And Software*, CMP Media LLC beschikbaar op: <http://www.informationweek.com/showArticle.jhtml?articleID=161601930> (laatst bewerkt 29 dec 2006).

Ward M. (2005) *Web shops face tighter security*, BBC beschikbaar op: <http://news.bbc.co.uk/2/hi/technology/4449759.stm> (laatst bewerkt 29 dec 2006).

Evers J. (2005) *Credit card breach exposes 40 million accounts*, CNET Networks, Inc. beschikbaar op: [http://news.com.com/Credit+card+breach+exposes+40+million+accounts/2100-1029\\_3-5751886.html](http://news.com.com/Credit+card+breach+exposes+40+million+accounts/2100-1029_3-5751886.html) (laatst bewerkt 29 dec 2006).

Extended Retail Solutions (2006) *Fighting spyware and retail identity theft*, GDS Publishing Ltd. beschikbaar op: <http://www.extendedretail.com/pastissue/article.asp?art=25770&issue=147> (laatst bewerkt 29 dec 2006).

Schneier B. (2005) *Schneier on Security: Visa and Amex Drop CardSystems*, Schneier.com beschikbaar op: [http://www.schneier.com/blog/archives/2005/07/visa\\_and\\_amex\\_d.html](http://www.schneier.com/blog/archives/2005/07/visa_and_amex_d.html) (laatst bewerkt 29 dec 2006).

Harris Interactive (2005) *Global Consumer Attitudes and Behaviors Toward Data Security*, Visa International.

Krebs B. (2006) *ID Thieves Turn Sights on Smaller E-Businesses*, The Washington Post beschikbaar op: <http://www.washingtonpost.com/wp-dyn/content/article/2006/09/28/AR2006092800333.html> (laatst bewerkt 29 dec 2006).

Cybertrust (2006) *PCI Merchant & Service Provider Levels* beschikbaar op: [http://www.cybertrust.com/solutions/compliance\\_governance/pci\\_compliance/pci\\_levels/](http://www.cybertrust.com/solutions/compliance_governance/pci_compliance/pci_levels/) (laatst bewerkt 29 dec 2006).

MasterCard *Merchant Levels Defined* beschikbaar op: [http://www.mastercard.com/us/sdp/merchants/merchant\\_levels.html](http://www.mastercard.com/us/sdp/merchants/merchant_levels.html) (laatst bewerkt 29 dec 2006).

Pauli D. (2006) *Australian Compliance Confusion Leads to Security Breaches*, CXO Media Inc. beschikbaar op: [http://www2.csoonline.com/blog\\_view.html?CID=25049](http://www2.csoonline.com/blog_view.html?CID=25049) (laatst bewerkt 29 dec 2006).

Wells Fargo *Merchant Services - Payment Card Industry (PCI) Data Security Standards FAQs* beschikbaar op: <https://www.wellsfargo.com/biz/help/merchant/faqs/pci#Q24> (laatst bewerkt 29 dec 2006).

PCI Security Standards Council (2006) *Payment Card Industry (PCI) Data Security Standard* (Versie 1.1) beschikbaar op: [https://www.pcisecuritystandards.org/pdfs/pci\\_dss\\_v1-1.pdf](https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf).

© 2007 GFI Software Ltd. Alle rechten voorbehouden. De informatie in dit document geeft het standpunt van GFI weer betreffende de besproken onderwerpen op de datum van publicatie. Aangezien GFI moet reageren op veranderende marktomstandigheden, moet dit document niet als een toezegging van GFI worden geïnterpreteerd. Na de publicatiedatum kan de correctheid van de informatie niet worden gegarandeerd. Dit white paper dient puur ter informatie. GFI GEEFT IN DIT DOCUMENT GEEN ENKELE GARANTIE, EXPLICIET NOCH IMPLICIET. GFI, GFI EndPointSecurity, GFI EventsManager, GFI FAXmaker, GFI MailEssentials, GFI MailSecurity, GFI MailArchiver, GFI LANguard, GFI Network Server Monitor, GFI WebMonitor en de bijbehorende logo's zijn ofwel geregistreerde handelsmerken of handelsmerken van GFI Software Ltd. in de Verenigde Staten en/of andere landen. Alle product- en bedrijfsnamen in dit persbericht zijn mogelijk handelsmerken van hun respectievelijke eigenaren.