



Protect what you value.

GOODBYE HACKERS, HELLO TRUST



www.pcisecuritystandards.org

's Werelds grootste verstreker van PCI-certificaten

In reactie op het overweldigende aantal gevallen van diefstal van creditcardgegevens door hackers hebben Visa en MasterCard de PCI DSS-standaard (Payment Card Industry Data Security Standard) ontwikkeld. Deze standaard wordt eveneens gehanteerd door American Express, Discover Card en JCB. De standaard moet worden geïmplementeerd door alle webwinkeliers (merchants), online retailers en hun webhosts en door alle internetkassa's en PSP's (betaalserviceproviders).

McAfee, 's werelds grootste verstreker van certificeringen voor websitebeveiliging, is door Visa International verkozen tot exclusieve leverancier van PCI-validatieservices met het merk Visa in meer dan 70 landen.

Een beveiligd netwerk configureren en onderhouden

- 1 Installeer en onderhoud een fire wall-configuratie om gegevens te beschermen
- 2 Gebruik nooit de door de leverancier ingestelde standaardwaarden voor systeemwachtwoorden en andere beveiligingsparameters

Informatie van creditcardhouders Beschermen

- 3 Beveilig de opgeslagen gegevens
- 4 Gebruik encryptie bij de overdracht van kaarthoudergegevens en andere gevoelige informatie via open netwerken

Programma voor het beheer van veiligheidslekken

- 5 Gebruik antivirussoftware en zorg voor regelmatige updates
- 6 Ontwikkel en onderhoud veilige systemen en applicaties

Implementatie van sterke Toegangscntrole

- 7 Beperk de toegang tot gegevens op basis van "need-to-know"
- 8 Wijs een unieke gebruikers-ID toe aan alle personen met toegang tot de computersystemen
- 9 Beperk de fysieke toegang tot de Gegevens van creditcardhouders

Regelmatige controle en tests van netwerken

- 10 Bewaak en observeer elk gebruik van de netwerkbronnen en de kaarthouder gegevens
- 11 Zorg voor regelmatige tests van de systemen en processen voor beveiliging

Beleid voor informatiebeveiliging

- 12 Definieer en onderhoud beleidsrichtlijnen voor de beveiliging van informatie

Snel en eenvoudig aan de PCI-standaard voldoen

In nauwe samenwerking met Visa en MasterCard heeft McAfee een unieke, betrouwbare en gebruiksvriendelijke online PCI-wizard ontwikkeld, waarmee zowel grote als kleine webwinkeliers goedkoper en betrouwbaarder kunnen zorgen dat ze voldoen aan de PCI-standaard.

Deze service, die alleen beschikbaar is via McAfee en zijn partners, automatiseert het invullen van de vragenlijst voor zelfevaluatie, controleert automatisch elk kwartaal op de aanwezigheid van veiligheidslekken en genereert de noodzakelijke PCI-compatibiliteitsrapporten met de bijbehorende documentatie.

Daarnaast wordt onbeperkte telefonische en online technische ondersteuning geboden.

De PCI-certificering van McAfee voldoet aan de vereisten die worden gesteld door Visa (CISP en AIS), MasterCard (SDP), American Express (DSS), JCB en Discover Card.

**Geen hardware of software nodig
Eerste scanresultaten binnen 24 uur
Online inschrijven**

www.hackersafe.eu

PCI / DSS

- Kwartaal scan conform de PCI-standaard
- Download van PCI-Self Assessment vragenlijst
- PCI-rapport als PDF-rapport te downloaden voor aanlevering aan uw acquirer/bank
- Ongelimiteerd handmatig opstarten van extra scans

Aantal URL/IP	Kosten ^{1/2} per URL/IP-nr		
	1 jaar	2 jaar	3 jaar
1	€ 204	€ 306	€ 407
2 - 3	€ 118	€ 177	€ 236
4 - 7	€ 73	€ 110	€ 147
8 - 15	€ 47	€ 71	€ 95
16 - 31	€ 36	€ 54	€ 72
32 - 63	€ 29	€ 43	€ 57
64 - 127	€ 24	€ 37	€ 49
128 +	€ 20	€ 31	€ 41

¹ Excl. eenmalige setup-kosten van €100,-

² Alle hierboven genoemde prijzen zijn excl. BTW

Alle hierboven genoemde prijzen zijn excl. BTW

PCI Niveau	Type webwinkelier	Certificeringsvereisten
Niveau 1	> Jaarlijks meer dan 6 miljoen Visa/MC-transacties via alle kanalen, inclusief e-commerce.	Jaarlijkse onsite PCI-evaluatie van gegevensbeveiliging en driemaandelijkse netwerkscan
Niveau 2	> Jaarlijks meer dan 150.000 Visa/MC transacties via alle kanalen, inclusief e-commerce	Jaarlijkse zelfevaluatie en driemaandelijkse netwerkscan
Niveau 3	> Jaarlijks meer dan 20.000 Visa/MC-transacties via e-commerce	Jaarlijkse zelfevaluatie en driemaandelijkse netwerkscan
Niveau 4	< Jaarlijks minder dan 20.000 Visa/MC-transacties via e-commerce	Jaarlijkse zelfevaluatie en jaarlijkse netwerkscan



Protect what you value.

GOODBYE HACKERS, HELLO TRUST

PCI-WIZARD

Stap 1: Interactieve vragenlijst voor zelfevaluatie

De wizard begeleidt u bij het invullen van de vragenlijst, met toelichtingen en suggesties om aan de verschillende eisen te voldoen. Bovendien biedt de wizard een workflow-systeem om de oplossing van problemen te volgen en te delegeren naar de juiste personen binnen uw organisatie.

Stap 2: Configuratie van het netwerk en de websites



Van een correcte registratie van de domeinen en IP-adressen van uw organisatie tot en met het plannen van scans en complete ondersteuning bij de probleemoplossing. De wizard zorgt ervoor dat de vereiste scanprocedures voor de beveiliging eenvoudig en correct kunnen worden uitgevoerd.

Stap 3: Afgifte van het PCI- certificaat



U kunt uw PCI-certificaat beveiligd downloaden in HTML- of PDF-opmaak. Documentvergrendeling is beschikbaar om de informatie veilig te kunnen raadplegen en afleveren. De verwerkende banken (acquirers) kunnen uw compatibiliteitsrapporten online bekijken.

PCI- en McAfee SECURE-certificering is gebaseerd op rigoureuze controles van de netwerkbeveiliging.

Stap 1: Poortscan

Dit is een grondige, interactieve poortscan van het doelsysteem. Onze geavanceerde, dynamische poortscanner kan overweg met alle soorten doelsystemen, uiteenlopend van desktopcomputers tot de meest agressieve firewalls en IDS- en IPS-systemen.

Stap 2: Controle op veiligheidslekken in netwerkservices

We ondervragen alle services die op de beschikbare poorten aanwezig zijn, om exact vast te stellen welke software er wordt uitgevoerd en hoe deze is geconfigureerd. Deze informatie wordt gekoppeld aan onze database met informatie over veiligheidslekken, waardoor we gerichte applicatiespecifieke en algemene tests kunnen uitvoeren.

Stap 3: Scan van webapplicaties

Alle HTTP-services en virtuele domeinen worden gecontroleerd op de aanwezigheid van potentieel gevaarlijke modules, CGI's en andere scripts, configuratie-instellingen en als standaard geïnstalleerde bestanden. Vervolgens wordt de website geheel doorzocht via een procedure voor "deep crawling", waarbij ook koppelingen in Flash-animaties en pagina's met wachtwoordbeveiliging worden verkend. Hierdoor worden alle formulieren en andere potentieel riskante interactieve elementen opgespoord. Deze elementen worden daarna gericht geactiveerd om eventuele veiligheidslekken op applicatieniveau aan het licht te brengen, zoals onthulling van code, scripts die verdeeld zijn over meerdere sites, XSS en SQL-injecties. Ook wordt gescand op adware, spyware en virussen.

Stap 4: Waarschuwingen

Na elke geplande dagelijkse of handmatig uitgevoerde scan ontvangt u waarschuwingen wanneer er veiligheidslekken zijn aangetroffen. De waarschuwingen kunnen per gebruiker, per apparaatgroep en per risiconiveau worden geconfigureerd. Daarnaast kunnen handmatige scans worden geconfigureerd om alleen de eerder herkende veiligheidslekken te testen teneinde de getroffen maatregelen (patches) te verifiëren, of om agressieve tests met DOS-aanvallen en "full exploits" uit te voeren.

Stap 5: Analyse en oplossingen

Veiligheidslekken kunnen worden gesorteerd op combinaties van apparaatgroepen, op risiconiveau of op de hoeveelheid werk die nodig is om het lek te dicht. De indeling in apparaatgroepen leidt tot snellere planning van de oplossing, meer mogelijkheden om te delegeren en beter patchbeheer. Vanuit het beheerportaal voor veiligheidslekken worden complete, gedetailleerde en gemakkelijk uit te voeren instructies voor patchprocedures verstrekt. Bovendien wordt er verwezen naar externe informatiebronnen, zoals CVE, CERT, BugTraq en de websites van leveranciers.

Stap 6: McAfee SECURE-certificering (alleen bij PCI-dagelijks)

De technologie van McAfee zorgt ervoor dat het McAfee SECURE-logo alleen wordt weergegeven indien de huidige beveiligingsstatus van de website voldoet aan de strengste door de overheid opgestelde standaarden. Als eventuele veiligheidslekken niet binnen maximaal 72 uur zijn gedicht, wordt het certificeringsvignet vervangen door een transparante GIF-afbeelding van 1x1 pixel.



Informatie over PCI

- www.pcisecuritystandards.org
- www.visaeurope.com/aboutvisa/security/ais/
- www.visaeurope.com/documents/ais/merchants_guide.pdf
- www.mastercard.com/us/sdp/index.html
- www.mastercard.com/us/sdp/merchants/index.html
- www.americanexpress.com/merchants (kies Processing & Supplies, Data Security)

BVB Media B.V. is reseller McAfee SECURE

BVB Media B.V.
Maasdijk 62
5308 JD Aalst
T. +31 418820211
E. info@bvbmedia.nl
I. www.bvbmedia.nl

