

Le standard PCI DSS simplifié

La solution au standard PCI DSS (Payment Card Industry Data Security Standard)

Les principales institutions des cartes de paiement luttent pour arrêter les incidents financiers de fraude qui ont affecté de nombreux organisations et leurs consommateurs. En conséquence, les organisations qui acceptent des transactions de carte de paiement sont dûment tenues de se conformer au standard PCI DSS à la fin de 2007. Les organisations qui ne se conforment pas, risquent de se voir interdites de manipuler des données de détenteur de carte et des amendes pouvant aller jusqu'à 500.000\$ si les données sont perdues ou volées. Ce livre blanc examine les conditions nécessaires pour adhérer au standard PCI DSS, les implications du manque de conformité aussi bien que la façon dont la gestion efficace d'enregistrements d'événements et la gestion de vulnérabilité de réseau jouent un rôle principal dans la réalisation de la conformité au standard PCI DSS.

Introduction

Les cartes de crédit sont très répandues et leur utilisation pour effectuer des paiements en ligne augmente considérablement. Il y avait 1,3 milliard de cartes de crédit en circulation aux ETATS-UNIS en 2004, avec 76% d'Américains ayant au moins une carte de crédit. Les ventes au détail d'e-commerce aux ETATS-UNIS dans le quatrième trimestre de 2006 étaient \$33,9milliard, une augmentation de 25% pour le même trimestre en 2005.

Il y a de mauvaises nouvelles cependant: La fraude de carte de crédit (25%) était la forme la plus commune de vol d'identité rapportée en 2006. Considérant que plus de \$48 milliards ont été perdus par les institutions financières et les entreprises au cours de cette année du au vol d'identité, et \$5 milliards perdus par des individus, on peut dire que la fraude de carte de crédit creuse profondément dans les poches de chacun. La fraude d'e-commerce est également en augmentation, atteignant \$3 milliards en 2006 avec une hausse de plus de 7% en 2005 ! Ce livre blanc examine les conséquences du vol de données de détenteur de carte et adresse les questions principales suivantes:

- Qu'est-ce que la directive PCI ?
- Pourquoi est-il important pour votre entreprise de se conformer au standard PCI DSS ?
- Quelles sont les conséquences de la non-conformité ?
- Quelles solutions sont disponibles pour répondre à la directive PCI ?

Le vol et la fraude de données de détenteur de carte – quelques cas réels

- Le 18 février 2005 – Bank of America a affirmé qu'elle avait perdu plus de 1.2 million de fiches de données de client - cependant il a indiqué qu'il n'y avait aucune preuve que les données étaient tombées entre les mains de criminels.
- Le 16 juin, 2005 – CardSystems, un fournisseur de service de traitement des transactions de paiement, a été poursuivi dans une série de cas d'action de classe alléguant qu'il n'avait pas protégé adéquatement l'information personnelle de 40 millions de clients. L'entreprise CardSystems était au bord de la faillite étant donné que VISA et American Express avaient coupé tous les liens avec l'entreprise, l'interdisant de traiter leurs données de carte. CardSystems a été plus tard acquis par une autre compagnie.
- Le 9 février 2006 – On estimait qu'autour de 200.000 comptes de carte de débit avaient été révélés par des marchands au détail inconnus, apparemment OfficeMax et d'autres. Ceux-ci incluaient des comptes liés aux acquéreurs de banque et de syndicats de carte de crédit dans tout le pays tel que CitiBank et Wells Fargo.

- Le 31 janvier, 2006 – Boston Globe et The Worcester Telegram & Gazette ont inconsciemment exposé 240.000 fiches de données de carte de crédit et de débit avec l'information de transmission de chèques personnels imprimés sur le papier recyclé utilisé dans l'emballage des paquets de journaux destinés à la distribution.
- Le 12 janvier 2007 – MoneyGram, un fournisseur de services de paiement a rapporté qu'un serveur de l'entreprise avait été illégalement accédé à travers Internet le mois précédent. Il contenait l'information de facturation d'environ 79.000 clients, y compris des noms, adresses, numéros de téléphone, et dans certains cas, des numéros de comptes bancaires.
- Le 17 janvier 2007 – TJX Companies Inc. a publiquement révélé qu'il avait été victime d'une intrusion non autorisée dans le système de traitement électronique de carte de crédit. Dans ce qui est considéré jusqu'ici comme les infractions de sécurité les plus fascinantes, pas moins 45.700.000 numéros de comptes de cartes de crédit et plus de 455.000 de fiches de retour de marchandises (contenant les noms de client et les numéros de permis de conducteurs) ont été volés à partir du système informatique de l'entreprise.

Les grands détaillants en ligne ne sont pas les seules organisations qui sont ciblées. L'attention du public peut être fixée sur des pertes d'importantes données, mais les experts étudiant la fraude financière disent que de plus en plus les intrus visent de petits sites Web commerciaux. Dans certains cas, les criminels peuvent accéder en temps réel à l'information des transactions des sites Web, leur permettant de voler des numéros de carte valides de crédit et d'effectuer rapidement un grand nombre d'achats frauduleux. Au total, les petites entreprises de commerce électronique sont moins victimes, mais elles constituent souvent une cible plus facile, soit dû à des lacunes dans le logiciel utilisé pour traiter les commandes d'achat en ligne ou une dépendance sur la sécurité externe d'un site Web tiers.

Le cybercrime et la menace rampante du vol d'identité réduisent la confiance des utilisateurs et des consommateurs, ralentissant l'acceptation de l'e-commerce. En conséquence, le degré de sécurité d'ordinateur, une activité critique qui aide à protéger ces systèmes, a légitimement évolué vers une position de prééminence.

Directive PCI de l'industrie de carte de paiement

Le cadre du standard de sécurité de données de l'industrie de carte de paiement (PCI) a été créé par American Express, Discover Financial Services, JCB, MasterCard Worldwide, et Visa International. Avant 2004, chacune des associations avait un ensemble séparé de normes de propriété industrielle de conditions de sécurité de l'information qui étaient souvent onéreuses et répétitives pour des participants aux réseaux de multiples marques. Les associations ont par conséquent créé un ensemble uniforme de conditions de sécurité de l'information pour toutes les marques nationales de carte (excepté pour les noms d'entreprises et les étiquettes privées). Ces conditions sont devenues la norme de sécurité de données de l'industrie de carte de

paiement et sont connues sous le nom de « PCI Data Security Standard (PCI DSS) », régissant tous les circuits de paiement: Ventes au détail, les ventes par correspondance, les commandes par téléphone et l'e-commerce.

Le cadre du standard PCI DSS

Le standard PCI DSS est divisé en 12 conditions de sécurité (VISA se rapporte à elles comme la « douzaine numérique » - Digital Dozen) qui sont organisées en six catégories comme suit :

PCI DSS
<p>Etablir et maintenir un réseau sécurisé</p> <p>Condition 1 : Installez et entretenez une configuration de firewall pour protéger les données de détenteurs de cartes</p> <p>Condition 2 : N'utilisez pas de mots de passe fournis par des fournisseurs ou tout autre paramètre de sécurité par défaut</p>
<p>Protéger les données des titulaires de carte de paiement</p> <p>Condition 3 : Protégez les données stockées</p> <p>Condition 4 : Cryptez la transmission des données de titulaire de carte et de toute information sensible à travers les réseaux publics</p>
<p>Maintenir un programme de gestion des vulnérabilités</p> <p>Condition 5 : Utilisez et mettez à jour régulièrement vos logiciels ou programmes antivirus</p> <p>Condition 6 : Développez et maintenez la sécurité de vos systèmes et de vos applications</p>
<p>Implémenter des mesures strictes de contrôles d'accès</p> <p>Condition 7 : Limitez l'accès aux seules données de titulaire de carte dont l'utilisateur a besoin ("business need-to-know").</p> <p>Condition 8 : Assignez un identifiant unique à chaque personne ayant accès à l'ordinateur</p> <p>Condition 9 : Limitez l'accès physique aux données de titulaire de la carte de paiement</p>
<p>Surveiller et tester régulièrement les réseaux</p> <p>Condition 10 : Traquez et surveillez tout accès aux ressources du réseau et aux données de titulaire de carte de paiement</p> <p>Condition 11 : Testez régulièrement les systèmes et les processus de sécurité</p>
<p>Maintenir une politique de sécurité d'information</p> <p>Condition 12 : Maintenez une politique axée sur la sécurité de l'information pour vos employés et les entrepreneurs</p>

Table 1 : Le cadre du standard PCI DSS

La conformité à ces conditions peut être récapitulée dans 3 étapes principales :

- **Rassemblement et stockage** : Collection et stockage sécurisés de tout l'enregistrement des données de sorte qu'il soit disponible pour l'analyse.
- **Compte rendu de toutes les activités** : La capacité de prouver spontanément la conformité en cas d'audit et de produire la preuve que les mesures de contrôle pour la

protection des données sont bien en place et fonctionnent.

- **Surveillance et alertes** : Avoir en place des systèmes automatiques de surveillance et d'alertes pour aider les administrateurs à constamment surveiller l'accès et l'utilisation des données. Les administrateurs sont avertis immédiatement en cas de problèmes et peuvent les corriger rapidement. Ces systèmes devraient également être appliqués à l'enregistrement des données – il doit y avoir une preuve de l'enregistrement des données qui sont rassemblées et stockées.

Niveaux de négociant et de fournisseur de services

Les négociants et des fournisseurs de services qui doivent se conformer au standard PCI DSS sont classés par catégorie selon le nombre de transactions de carte qu'ils traitent sur une période de douze mois. Le Tableau 2 et le Tableau 3 ci-dessous décrivent les divers niveaux et conditions de conformité pour les négociants et les fournisseurs de services.

Les négociants sont les accepteurs agréés des cartes pour le paiement des marchandises et des services. Les exemples d'industries où les négociants doivent être conformes incluent, mais ne sont pas limités à :

- Le commerce en ligne tel que le détaillant en ligne Amazon.com
- La vente au détail tel que les magasins de la chaîne de vente au détail Wal-Mart
- Les institutions d'enseignement supérieur telles que des universités
- Les établissements de soins de santé tels que des hôpitaux
- Les agences de voyage et les établissements de divertissement tels que des hôtels et des restaurants
- Les établissements de vente d'énergie tels que des stations de carburants
- Les institutions financières telles que des banques et des compagnies d'assurance

NIVEAUX DE NEGOCIANT	
DEFINITION D'UN NEGOCIANT *	DEFINITION D'UN NEGOCIANT*
Niveau 1	
<ul style="list-style-type: none"> • Les négociants dont des données de titulaire de carte ont été compromises • Les négociants effectuant plus de six millions de transactions annuelles de carte de paiement à travers tous les circuits, y compris l'e-commerce 	Inspection annuelle sur place de la sécurité de données PCI et des balayages trimestriels de réseau
Niveau 2	
<ul style="list-style-type: none"> • Les négociants effectuant entre 1 et 6 millions de transactions annuelles de cartes de paiement 	Auto-inspection annuelle et balayages trimestriels de réseau
Niveau 3	

<ul style="list-style-type: none"> Les négociants effectuant entre 20.000 et 1.000.000 de transactions annuelles de cartes de paiement d'e-commerce 	Auto-inspection annuelle et balayages trimestriels de réseau
Niveau 4 **	
<ul style="list-style-type: none"> Tous les autres négociants 	Auto-inspection annuelle et balayages annuels de réseau

Table 2 : Niveaux de négociant

* Les niveaux de négociant basés sur les définitions de Visa USA

** Le standard PCI DSS exige que tous les négociants effectuent le balayage de réseau externe pour réaliser la conformité. Les acquéreurs peuvent avoir besoin de la soumission des rapports et/ou des questionnaires de balayage par les négociants du niveau 4.

Les fournisseurs de services sont des organisations qui traitent, stockent, ou transmettent des données de titulaire de carte pour le compte des membres de carte, des négociants, ou d'autres fournisseurs de services. Les exemples de fournisseurs de services qui doivent être conformes incluent, mais ne sont pas limités à :

- Passerelles de paiement
- Serveurs de fournisseurs d'e-commerce
- Fournisseurs de service de contrôle
- Agences de contrôle de solvabilité
- Entreprises de gestion d'enregistrements de secours
- Entreprises de destruction de documents

DEFINITION DE FOURNISSEUR DE SERVICES	CONFORMITE
Niveau 1	
Tous les agents de traitement processeurs (membre et non membre) et toutes les passerelles de paiement*	Contrôle annuel de la sécurité des données sur le site selon les normes PCI et les balayages trimestriels de réseau
Niveau 2	
Tout fournisseur de services qui n'est pas de Niveau 1 et stocke, traite ou transmet plus de 1 million de transactions de comptes de cartes de crédit par an	Contrôle annuel de la sécurité des données sur le site selon les normes PCI et les balayages trimestriels de réseau
Niveau 3	
Tout fournisseur de services qui n'est pas du Niveau 1 et stocke, traite ou transmet moins de 1.000.000 de transactions de comptes de cartes de crédit par an	Questionnaire d'évaluation annuelle et les balayages trimestriels de réseau

Tableau 3 : Niveaux de fournisseurs de services

* Les passerelles de paiement sont une catégorie d'agent ou de fournisseur de services qui stocke, traite, et/ou transmet

les données de titulaire de carte faisant partie de la transaction de paiement (par exemple, Papal). Spécifiquement, ils permettent des transactions de paiement (par exemple, l'autorisation ou le règlement) entre les négociants et les processeurs (par exemple les terminaux de VisaNet). Les négociants peuvent envoyer leurs transactions de paiement directement à un terminal, ou indirectement à une passerelle de paiement.

Dates limites strictes pour la conformité.

Les principales entreprises de cartes exercent beaucoup de pression sur les négociants qui doivent adhérer au standard PCI DSS. Les diverses dates limites ont été fixées et des sanctions sévères et de lourdes amendes ont été prévues pour les organisations qui ne parviennent pas à réaliser la conformité à la date prévue. Parmi ces importantes dates limites, Visa USA a fixé au :

- 31 mars 2007 – date à laquelle les négociants de niveaux 1 et 2 doivent démontrer qu'ils ne stockent pas toutes les données de transmission, CVV2 ou le numéro secret d'identifiant personnel (PIN).
- 30 septembre 2007 – date à laquelle tous les négociants de niveau 1 doivent se conformer entièrement au standard PCI DSS.
- 31 décembre 2007 – date à laquelle tous les 2 négociants doivent se conformer entièrement au standard PCI DSS.

Les dates-limites pour la conformité peuvent changer entre les associations de carte et les régions ; partant, les négociants et les fournisseurs de service hésitants devraient consulter les acquéreurs ou les associations de carte pour s'enquérir de leurs dates-limites respectives.

Pourquoi est-il important à votre entreprise de se conformer ?

Bien que ce soit une initiative originaire des USA, le standard PCI DSS est une norme globale pour toutes les entités manipulant les données de titulaire de carte de paiement. Ce n'est pas tous les pays qui sont au courant de ce standard ; par exemple, la confusion répandue dans le secteur bancaire de l'Australie au sujet de nouvelles mesures de conformité a mené à cinq infractions du standard PCI DSS pendant 2006.

C'est dans l'intérêt des banques garantes de s'assurer que les négociants sont au courant du standard PCI DSS et qu'ils s'y conforment. La raison est tout à fait logique – les banques garantes sont les acteurs principaux qui constituent le lien vital entre les institutions financières de carte de paiement et les négociants – par conséquent ce sont également elles qui sont en amont de la ligne de front des institutions de carte de paiement toutes les fois qu'un ou plusieurs de leurs négociants subissent une infraction. Pour maintenir de bons rapports d'affaires avec les institutions de carte de paiement, les banques garantes doivent s'assurer que leurs négociants sont protégés adéquatement et que le standard PCI DSS est l'outil de

mesure de la sécurité de données de détenteur de carte du côté des négociants.

De même, on s'attend à ce que les négociants et les fournisseurs de services démontrent leur niveau de conformité au standard PCI DSS. Ceci contribue à maintenir un climat de confiance avec les banques et à éviter des responsabilités éventuelles de manque de conformité.

Quelles sont les conséquences de ne pas se conformer au standard PCI DSS ?

Les institutions financières des cartes de paiement peuvent infliger des amendes à leurs institutions bancaires garantes s'il s'avère que les négociants ne sont pas conformés au standard PCI DSS. Alternativement, les banques garantes peuvent contractuellement obliger les négociants à les indemniser et rembourser de telles amendes. Les amendes peuvent aller jusqu'à 500.000\$ par incident si les données sont compromises et si les négociants s'avèrent non-conformes. Dans le pire des scénarios, les négociants pourraient également risquer de perdre l'autorisation de traiter les transactions de carte paiement des clients.

Les entreprises dont les données de détenteur de carte ont été compromises sont obligées d'informer les autorités légales et d'offrir une protection gratuite des services de paiement à ceux qui sont éventuellement affectés.

Il peut y avoir d'autres conséquences en plus des amendes. La perte de données de détenteur de carte, qu'elle soit accidentelle ou par le vol, peut également mener à des poursuites judiciaires par les détenteurs de carte. Une telle étape peut avoir comme conséquence la mauvaise publicité, qui en retour peut mener à la perte d'affaires.

Quelles solutions GFI fournit-il pour vous aider à répondre aux exigences du standard PCI DSS ?

Des solutions technologiques peuvent être mises en application pour automatiser une partie des tâches que vous devez entreprendre pour vous conformer aux exigences du standard PCI. Ces solutions vous permettent de surveiller l'adhésion à ces normes et de vous alerter quand des événements non autorisés concernant les données de détenteur de carte se produisent. GFI fournit exactement les outils de logiciels qui vous aident à faire juste cela.

GFI EventsManager, GFI LANguard Network Security Scanner (N.S.S.) et GFI EndPointSecurity sont trois produits bien connus de sécurité de réseau de GFI. Grâce aux fonctionnalités d'audit, de surveillance, de rapportage et d'alertes, ces produits peuvent vous aider à adresser les multiples sections de neuf des 12 conditions du standard PCI DSS, comme illustré dans le tableau 4 ci-dessous.

Conditions du standard PCI DSS			
	GFI EventsManager	GFI LANguard N.S.S.	GFI EndPointSecurity
1. Installez et entretenez une configuration de firewall pour protéger les données de détenteurs de cartes	•	•	
2. N'utilisez pas de mots de passe fournis par des fournisseurs ou tout autre paramètre de sécurité par défaut	•	•	
3. Protégez les données de titulaire de carte stockées	•		•
4. Cryptez la transmission des données de titulaire de carte et de toute information sensible à travers les réseaux publics			
5. Utilisez et mettez à jour régulièrement vos logiciels ou programmes antivirus		•	
6. Développez et maintenez la sécurité de vos systèmes et de vos applications		•	
7. Limitez l'accès aux seules données de titulaire de carte dont l'utilisateur a besoin ("business need-to-know").	•		
8. Assignez un identifiant unique à chaque personne ayant accès à l'ordinateur	•	•	
9. Limitez l'accès physique aux données de titulaires de carte de paiement			
10. Traquez et surveillez tout accès aux ressources du réseau et aux données de titulaire de carte de paiement	•	•	
11. Testez régulièrement les systèmes et les processus de sécurité	•	•	•

12. Maintenez une politique axée sur la sécurité de l'information pour vos employés et les entrepreneurs			
--	--	--	--

Tableau 4 : Les conditions du standard PCI DSS**GFI EventsManager**

L'analyse des données d'événements est directement spécifiée dans la condition 10 (Voir le Tableau 4 ci-dessus) mais dans la pratique, c'est également dans les bonnes habitudes de n'importe quelle organisation de surveiller les événements.

Dans un environnement typique de réseau, les données d'événements sont dispersées, volumineuses et chiffrées. Les outils d'analyse d'événements fournis par défaut dans la plupart des logiciels d'exploitation offrent seulement le plus fondamental des dispositifs. En conséquence, les administrateurs n'ont aucun moyen d'être alerté quand un détail important ou des événements problématiques sont détectés, comme l'accès non autorisé aux données de détenteur de carte. Les outils de navigation d'événements et de filtrage fournis par ces dispositifs ont des capacités de recherche et de filtrage très limitées.

GFI EventsManager est une solution complète de gestion d'enregistrements qui surmonte tous ces obstacles, en vous permettant de centraliser les événements, d'automatiser la collection d'événements, de recevoir des alertes et de générer des rapports d'inspection. Pendant le rassemblement des événements, l'ensemble de règles incorporées de GFI EventsManager traite les événements afin de les classer et déclencher des alertes/actions en conséquence. Un des ensembles de règles par défaut fournis est spécifiquement destiné à la classification d'événements basée sur les conditions du standard PCI DSS. L'analyse d'événements peut être effectuée par le navigateur intégré d'événements ; des questions peuvent également être créées et exécutées pour rechercher et analyser des événements spécifiques.

Grâce à GFI EventsManager les entreprises peuvent s'assurer que tous les événements en rapport avec les données de titulaire de carte sont constamment surveillés. Pour plus d'information et pour télécharger le produit, visitez <http://www.gfsfrance.com/fr/eventsmanager/>.

GFI LANguard Network Security Scanner

La gestion des vulnérabilités est centrale aux conditions 5 et 6 (Voir le Tableau 4 ci-dessus). Cependant, la capacité de détecter des vulnérabilités dans divers domaines couverts par d'autres conditions est de plus grande importance.

GFI LANguard Network Security Scanner (N.S.S.) adresse les trois piliers de la gestion des vulnérabilités : le balayage de sécurité, la gestion de patches et l'inspection de réseau, trois logiciels intégrés dans une seule solution. GFI LANguard N.S.S. balaye le réseau entier pour à la recherche de plus de 15.000 vulnérabilités, identifie tous les problèmes possibles et fournit

aux administrateurs les outils dont ils ont besoin pour détecter, rapporter, évaluer et remédier à n'importe quelles menaces avant que les intrus ne les exploitent.

La gestion séparée des problèmes de vulnérabilité, de patches et d'inspection de réseau, parfois en utilisant les produits multiples, est un souci majeur pour les administrateurs. Non seulement ils doivent installer, apprendre à utiliser et contrôler plusieurs solutions, ils passent également la plupart de leur temps à essayer de comprendre où se trouvent les problèmes au lieu de s'occuper réellement des menaces éventuelles. En utilisant une console simple avec une puissante fonctionnalité de rapportage, la solution intégrée GFI LANguard N.S.S. aide les administrateurs à aborder ces questions plus rapidement et plus efficacement.

Grâce à GFI LANguard N.S.S. les entreprises peuvent avoir l'assurance que les données de titulaire de carte de paiement sont gardées dans un endroit sécurisé. Pour plus d'information et pour télécharger le produit, visitez <http://www.gfsfrance.com/fr/lannetscan/>.

GFI EndPointSecurity

La protection des données de titulaire de carte stockées, condition 3 (Voir le Tableau 4 ci-dessus), est une condition principale du standard PCI de sécurité des données. S'assurer que ces données ne tombent pas entre les mains de malfaiteurs est crucial.

C'est un fait bien connu que les dispositifs de mémoire massive, tels que les clés USB, ont acquis une grande popularité ces dernières années. Ils sont faciles et rapides à installer, capable de stocker des quantités énormes de données, et assez petit pour être transporté dans une poche. Sans un mécanisme de sécurité en place, copier toutes les données de détenteur de carte sur un tel dispositif peut être fait facilement et vite.

GFI EndPointSecurity est la solution de sécurité qui vous aide à maintenir l'intégrité des données en empêchant le transfert non autorisé de données vers et en provenance des dispositifs de stockage portatifs. Grâce à sa technologie, GFI EndPointSecurity vous permet de d'autoriser ou de refuser l'accès à un dispositif aussi bien que d'assigner (là où c'est applicable) les privilèges d'accès 'total' ou de 'lecture seulement' pour un dispositif particulier, un dossier local ou un utilisateur/ groupe d'utilisateur d'Active Directory.

Grâce à GFI EndPointSecurity les entreprises peuvent s'assurer que les données de titulaires de carte de paiement ne sont pas copiées sur des dispositifs non autorisés. Pour plus d'information et télécharger le produit, visitez <http://www.gfsfrance.com/fr/endpointsecurity/>.

GFI ReportCenter

GFI ReportCenter est un cadre de rapportage centralisé qui vous permet de produire divers rapports en utilisant des données rassemblées par chacun des produits de GFI, c'est à dire GFI EventsManager, GFI LANguard N.S.S. et GFI EndPointSecurity, tous incluent le module ReportPack qui se branche à GFI ReportCenter.

Ces ReportPacks sont de puissants outils de rapportage avec plusieurs modèles de rapports standard préconfigurés par défaut. Ils incluent également un ensemble complet de fonctionnalités telles que le rapportage programmable, l'export de rapports et la distribution automatique des rapports par e-mail. Les rapports créés par les ReportPacks sont très utiles pour les entreprises lorsqu'il s'agit d'évaluer l'efficacité de leur programme de conformité au standard PCI. Pour plus d'information et pour télécharger un ReportPack, visitez <http://www.gfsfrance.com/fr/reportcenter/>.

Des initiatives

C'est dans l'intérêt des organisations détenant les données de carte de paiement de se conformer au standard de sécurité de données de l'industrie de carte de paiement, « PCI Data Security Standard ». C'est également dans l'intérêt des banques garantes de s'assurer que les négociants se conforment à ce standard.

Les banques pourraient offrir des initiatives aux négociants pour se conformer au standard PCI en leur proposant des permis de produits de sécurité de réseau de GFI en tant qu'élément faisant partie de leur contrat de services. Elles pourraient également fournir des services supplémentaires tels que l'expertise technique sur les produits de GFI. Ceci serait mutuellement avantageux étant donné que les négociants pourraient avoir la conscience tranquille concernant la conformité au standard PCI DSS sans compter les autres avantages offerts par les produits de GFI. Les banques peuvent également avoir la conscience tranquille sachant que les négociants qu'elles ont autorisés à accepter des paiements par carte de crédit ont effectué un grand pas vers la réalisation la conformité au standard PCI DSS.

Conclusion

Les entreprises courent continuellement le risque de perdre des données sensibles de titulaire de carte. Une telle perte pourrait avoir comme conséquence des amendes, des poursuites judiciaires et la mauvaise publicité. Ceci mènera à leur tour à la perte d'affaires. La réalisation de la conformité au standard PCI DSS devrait être la priorité des organisations qui effectuent des transactions avec les cartes de crédit.

La mise en application des outils et des logiciels pour la gestion des enregistrements, la gestion des vulnérabilités, le balayage de sécurité et la sécurité de terminal vous accompagneront dans vos efforts pour vous conformer au standard PCI. Les produits de sécurité de réseau de GFI peuvent justement vous aider à réaliser cet objectif.

A propos de GFI

GFI est l'un des leaders dans le domaine de la réalisation de logiciels qui fournit une seule source intégrée permettant aux administrateurs de résoudre les problèmes de sécurisation de réseaux, de contenu et de messageries. Grâce à sa technologie innovatrice, une stratégie agressive de commercialisation et sa concentration sur le marché de petites et moyennes entreprises, GFI répond aux besoins de continuité d'affaires et de productivité des entreprises et d'autres organisations sur une grande échelle. Fondée en 1992, GFI est une entreprise internationale qui possède des bureaux à Malte, à Londres, Raleigh, Hong Kong, Adelaïde et à Hambourg avec plus de 200.000 installations de ses logiciels à travers le monde. GFI est une entreprise spécialisée et possède un réseau de plus de 10.000 partenaires à travers le monde. Partenaire stratégique de Microsoft, GFI est membre certifié du partenariat Microsoft Gold Certified Partner. Pour plus d'informations à propos de GFI, visitez le site <http://www.gfsfrance.com>.

Références

CreditCards.com (2006) *Credit Card Industry Facts and Personal Debt Statistics* available from: <http://www.creditcards.com/statistics/statistics.php> (last cited 29 Dec 2006).

U.S. Census Bureau (2006) *Quarterly retail e-commerce sales 2nd quarter 2006* available from: <http://www.census.gov/mrts/www/data/html/06Q2.html> (last cited 29 Dec 2006).

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

United States Postal Service *Identity Theft: Stealing Your Name and Your Money* available from: <http://www.usps.com/postalinspectors/IDtheft2.htm> (last cited 29 Dec 2006).

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

Marlin S. (2005) *Customer Data Losses Blamed On Merchants And Software*, CMP Media LLC available from: <http://www.informationweek.com/showArticle.jhtml?articleID=161601930> (last cited 29 Dec 2006).

Ward M. (2005) *Web shops face tighter security*, BBC available from: <http://news.bbc.co.uk/2/hi/technology/4449759.stm> (last cited 29 Dec 2006).

Evers J. (2005) *Credit card breach exposes 40 million accounts*, CNET Networks, Inc. available from: http://news.com.com/Credit+card+breach+exposes+40+million+accounts/2100-1029_3-5751886.html (last cited 29 Dec 2006).

Extended Retail Solutions (2006) *Fighting spyware and retail identity theft*, GDS Publishing Ltd. available from: <http://www.extendedretail.com/pastissue/article.asp?art=25770&issue=147> (last cited 29 Dec 2006).

Schneier B. (2005) *Schneier on Security: Visa and Amex Drop CardSystems*, Schneier.com available from: http://www.schneier.com/blog/archives/2005/07/visa_and_amex_d.html (last cited 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 available from: <http://www.washingtonpost.com/wp-dyn/content/article/2006/09/28/AR2006092800333.html> (last cited 29 Dec 2006).

Cybertrust (2006) *PCI Merchant & Service Provider Levels* available from:

http://www.cybertrust.com/solutions/compliance_governance/pci_compliance/pci_levels/ (last cited 29 Dec 2006).

MasterCard *Merchant Levels Defined* available from: http://www.mastercard.com/us/sdp/merchants/merchant_levels.html (last cited 29 Dec 2006).

Pauli D. (2006) *Australian Compliance Confusion Leads to Security Breaches*, CXO Media Inc. available from: http://www2.csoonline.com/blog_view.html?CID=25049 (last cited 29 Dec 2006).

Wells Fargo *Merchant Services - Payment Card Industry (PCI) Data Security Standards FAQs* available from: <https://www.wellsfargo.com/biz/help/merchant/faqs/pci#Q24> (last cited 29 Dec 2006).

PCI Security Standards Council (2006) *Payment Card Industry (PCI) Data Security Standard* (Version 1.1) available from: https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf.

© 2007 GFI Software. Tous droits réservés. L'information contenue dans ce document représente le point de vue actuel de GFI sur les questions abordées à la date de sa publication. Etant donné que GFI doit répondre aux conditions dynamiques du marché, il ne devrait pas être interprété comme un engagement de la part de GFI, et GFI ne peut pas garantir l'exactitude d'aucune information présentée après la date de la publication. Ce livre blanc est seulement à titre informationnel. GFI NE FAIT AUCUNE GARANTIE, EXPRESSE OU IMPLICITE, DANS CE DOCUMENT. GFI, GFI EndPointSecurity, GFI EventsManager, GFI FAXmaker, GFI MailEssentials, GFI MailSecurity, GFI MailArchiver, GFI LANguard, GFI Network Server Monitor, GFI WebMonitor et leurs logos de produit sont des marques déposées ou des brevets commerciaux de GFI Software aux Etats-Unis et/ou dans d'autres pays. Tous les noms de produit ou d'entreprises mentionnés ci-dessus peuvent être les marques déposées de leurs propriétaires respectifs.