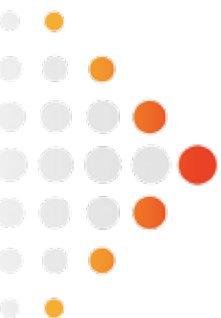


LE PCI : DE QUOI S'AGIT-IL ET QU'ELLE EST SON IMPORTANCE POUR LES PETITS COMMERCE ?

ADVANCING COMMERCE™



Le terme « PCI » (*Payment Card Industry*) désigne généralement le Conseil des normes de sécurité du secteur des cartes de paiement (PCI SSC ou « Conseil du SCP »). Le Conseil du SCP est un forum international ouvert qui a été lancé en 2006 par MasterCard Worldwide et quatre autres marques de paiement afin de créer et de gérer des normes de sécurité visant à protéger les données sur les cartes de paiement. La norme prépondérante est la norme de sécurité des données PCI DSS (*PCI Data Security Standard*). Lorsqu'on demande à un commerçant son statut de conformité à la sécurité des données, on veut généralement savoir s'il respecte les processus et les contrôles de sécurité de la PCI DSS.

Le principal objectif de la PCI DSS est de réduire le risque de perte de données sur les cartes de paiement (cartes de débit et de crédit) en prévenant, en détectant et en contrant les infractions ou les attaques potentielles qui pourraient mener à la compromission des données sur les comptes (*Account Data Compromise event ou incident ADC*). En d'autres termes, la PCI DSS sert à protéger les données sur les cartes de paiement contre les menaces criminelles et à réduire le risque d'atteinte à la sécurité des données pour les commerces de toutes tailles.

MON COMMERCE EST-IL OBLIGE DE RESPECTER LES NORMES DE SECURITE PCI ?

Le règlement de MasterCard stipule que toutes les entités qui stockent, transmettent ou traitent des données sur les titulaires de carte, quelle que soit leur taille, sont tenues de respecter toutes les exigences PCI DSS en matière de sécurité des données. Les commerçants qui traitent au plus un million de transactions effectuées avec présentation d'une carte de paiement et au plus 20 000 transactions de commerce électronique sont classés par MasterCard comme des commerçants de niveau 4.

Les commerçants de niveau 4 peuvent être tenus de déclarer périodiquement leur statut de conformité aux normes PCI DSS de sécurité des données. Le commerçant devrait toujours vérifier auprès de l'acquéreur (ou de son délégué) s'il est préférable qu'il déclare son statut de conformité et selon quelles modalités PCI DSS. L'acquéreur peut exiger que le commerçant remplisse un Questionnaire d'auto-évaluation (*Self-Assessment Questionnaire ou SAQ*). Il existe plusieurs SAQ qui s'adressent à différents types de commerces. Par exemple, un commerçant qui accepte seulement les paiements par carte à l'aide d'un terminal avec une connexion par ligne commutée et qui ne stocke pas les données des cartes devra remplir le SAQ B. À l'heure actuelle, il y a cinq SAQ différents; l'acquéreur du commerçant aidera ce dernier à choisir le questionnaire SAQ approprié. Pour plus de détails, consultez ce site : https://www.pcisecuritystandards.org/merchants/self_assessment_form.php (en anglais) ou <https://frca.pcisecuritystandards.org/minisite/en/saq-v2.0-documentation.php> (en français)

POURQUOI LA SECURITE DES DONNEES EST-ELLE IMPORTANTE POUR UN PETIT COMMERCE ?

On cible les petits commerçants — Depuis quelque temps, les petites entreprises sont de plus en plus ciblées par les attaquants. Peut-être vous demanderez-vous : « Pourquoi voudrait-on s'introduire par effraction dans mon entreprise ? Ne serait-il pas plus intéressant de cibler une banque, par exemple ? ». En fait, les attaquants ciblent n'importe quelle entité qui traite ou stocke des données sur des cartes de paiement et qui peut être vulnérable à la compromission des données. Les grandes institutions financières et les gros commerçants se dotent généralement de mesures de sécurité coûteuses et efficaces pour se protéger contre les attaques, mais ce niveau de sécurité n'est peut-être pas accessible aux petits commerçants. Par conséquent, lorsqu'ils cherchent des cibles vulnérables, les attaquants constatent que nombre de petits commerçants n'ont pas recours aux mesures de sécurité même les plus élémentaires exigées par la norme PCI DSS. Il en résulte que, de plus en plus, les attaquants s'emploient à compromettre les données des petites entreprises en lançant des attaques ciblées en chaîne qui passent souvent inaperçues pendant longtemps, parce que les petits commerçants ne disposent pas de mécanismes de détection.

Les pertes de données sur les cartes de paiement peuvent coûter cher — Si les données de cartes de paiement d'un commerçant sont compromises, par exemple parce que ses systèmes ont été piratés, l'acquéreur peut tenir l'entreprise financièrement responsable de toute perte due à la fraude qui y est associée et de tous les autres coûts. Si un incident ADC est soupçonné, le commerçant peut être tenu de faire faire une enquête judiciaire par un expert enquêteur en matière de fraude PCI, ce qui peut lui coûter cher.

Les attaquants peuvent également compromettre d'autres types de données, par exemple les dossiers des services des finances et des ressources humaines de même que des secrets commerciaux ou des renseignements exclusifs qui pourraient être très préjudiciables aux affaires et à la réputation du commerçant.

QU'EST-CE QU'UN INCIDENT LIE A LA COMPROMISSION DES DONNEES DE COMPTES ?

En termes simples, il s'agit d'un incident ADC qui provoque, directement ou indirectement, l'accès non autorisé ou la divulgation de données de cartes de paiement de marque MasterCard. L'incident peut porter sur des reçus physiques, mais les attaques les plus courantes ciblent le stockage des données de paiements électroniques par carte et sont perpétrées soit à l'interne par un employé malhonnête qui clone les cartes, ou à l'externe par des attaquants qui réussissent à accéder à distance aux systèmes du commerçant ou d'un prestataire de services et subtilisent ensuite les données.

COMMENT PUIS-JE ME PROTEGER CONTRE LES ATTAQUES ?

À l'heure actuelle, deux principaux types de commerçants sont habituellement la cible d'incidents ADC :

1) Les commerçants qui ont pignon sur rue et ont un magasin où ils traitent des transactions sur présentation de carte

Dans la plupart des cas de vol de données de cartes de paiement, la compromission est due à des technologies d'accès à distance mal configurées dans les applications point de vente (PDV).— À titre d'exemple, mais sans s'y restreindre, ces technologies sont : PCAnywhere, VNC, GoToMyPC.

com et Windows Remote Access. **(Remarque : Bien que ces technologies offrent des fonctions de sécurité, celles-ci sont souvent mises en place sans avoir été sécurisées.)** Il est fréquent que ces technologies soient utilisées par un fournisseur de solutions ou un fournisseur de terminaux PDV qui est autorisé à accéder à distance au réseau du commerçant afin d'assurer la maintenance et la mise à jour de son environnement. Les technologies d'accès à distance peuvent également être utilisées par les gérants, les propriétaires ou les superviseurs de magasin pour remplir des tâches telles que la mise à jour des dossiers financiers, la gestion des stocks ou la création des horaires du personnel à partir de leur domicile ou d'un autre endroit à l'aide d'une connexion Internet. Cependant, les attaquants peuvent se servir des applications logicielles d'accès à distance par Internet qui ont été mal configurées pour avoir un accès complet aux systèmes des commerçants.

Ces outils d'accès à distance prévoient une configuration adéquate en matière de sécurité, de sorte qu'une authentification à deux facteurs devrait être mise en œuvre pour tout accès à distance, conformément aux exigences de la PCI DSS. L'authentification à deux facteurs est communément effectuée à l'aide de deux des identifiants suivants :

- un élément que l'utilisateur connaît (p. ex., un mot de passe)
- un élément que l'utilisateur possède (p. ex., un jeton sécurisé), et (ou)
- un élément qui identifie l'utilisateur (p. ex., une empreinte digitale)

Les codes d'utilisateur ou ID d'utilisateur ne sont pas admissibles comme facteurs pour l'authentification à deux facteurs.

2) Les cybercommerçants, ou commerces en ligne

Les attaques par injection SQL (langage de gestion du modèle relationnel) constituent la principale forme d'attaque réussie contre les cybercommerçants. – Une attaque par injection SQL se produit lorsqu'un attaquant insère un code de base de données dans un champ sur un site Web, et que ce code est subséquemment exécuté par la base de données. Cette forme d'attaque peut permettre à l'attaquant d'avoir un accès complet à une base de données, laquelle pourra servir à compromettre le reste du réseau.

Les commerces en ligne peuvent utiliser leurs propres ressources pour héberger et gérer leur présence sur Internet ou encore confier à un tiers l'hébergement de leur site en leur nom. Allez sur le site www.mastercard.com/pci360 (en anglais) pour consulter un livre blanc sur les pages de paiement hébergées. Les cybercommerçants devraient être informés de leurs responsabilités en matière d'acceptation des cartes de paiement et de protection des données de cartes de paiement contre les criminels qui cherchent à cibler ces sites. Par exemple, la PCI DSS exige la mise en œuvre d'un codage sécurisé pour protéger les systèmes contre les attaques par injection SQL. De plus, cette norme permet l'installation de pare-feu pour applications Web, ce qui renforce la protection des sites Web des commerçants contre ce type d'attaque.

QU'ADVIENDRA-T-IL DE MES TERMINAUX PDV ET DES APPLICATIONS DE PAIEMENT PDV ?

La conformité à la PCI DSS est obligatoire, car les petits commerçants acceptent les cartes de paiement (cartes de crédit ou de débit) au moyen d'un terminal PDV ou d'une application de paiement. Si le commerçant ne dispose pas d'autres processus opérationnels pour recueillir ou stocker les données de cartes de paiement, ses efforts pour assurer la sécurité des données et la conformité de son entreprise aux normes de sécurité devraient porter sur son terminal PDV ou les applications de paiement PDV.

Terminaux PDV — Les terminaux PDV sont surtout utilisés par les commerçants ayant pignon sur rue. Ce type de petit commerçant devrait travailler directement avec son fournisseur de matériel informatique ou son acquéreur au moins une fois par année pour s'assurer qu'il reçoit l'information nécessaire à la sécurisation de ses terminaux conformément aux exigences de la PCI DSS. Dans la plupart des cas, l'acquéreur peut aider le commerçant à communiquer avec ses fournisseurs de terminaux.

Le Conseil des normes de sécurité du secteur des cartes de paiement gère une liste de dispositifs conformes aux exigences en matière de sécurité des transactions effectuées à l'aide de NIP (*Pin Transaction Security* ou PTS) qui peuvent être utilisés pour accepter en toute sécurité les données saisies à l'aide de NIP. MasterCard exige que les commerçants utilisent un dispositif de saisie du NIP dont la conformité PTS a été validée pour qu'ils puissent accepter les NIP.

Une liste des dispositifs de saisie du NIP approuvés par le Conseil des normes de sécurité du secteur des cartes de paiement est accessible sur son site Web :

https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php (en anglais)

Applications de paiement PDV — Les cybercommerçants et les petits commerçants ayant pignon sur rue peuvent utiliser un terminal PDV ainsi qu'une application informatique de paiement pour ordinateur personnel, pour traiter les opérations de paiement, gérer les comptes des consommateurs, gérer leurs stocks, etc. La norme de sécurité des données des applications de paiement [*Payment Application Data Security Standard* (PA-DSS)] exige des fournisseurs d'applications de paiement qu'ils sécurisent les solutions qu'ils mettent au point afin d'atténuer le risque de compromission des données pour les commerçants qui utilisent des applications de paiement disponibles commercialement (« grand public »). À compter du 1^{er} juillet 2012, MasterCard exigera que tous les commerçants qui utilisent des applications de paiement grand public se servent d'une application de paiement dont la conformité à la PA-DSS a été validée.

Plus de 1 200 applications de paiement validées sont actuellement indiquées dans le site Web du Conseil des normes de sécurité du secteur des cartes de paiement, à l'adresse suivante :

https://www.pcisecuritystandards.org/approved_companies_providers/validated_payment_applications.php?agree=true (en anglais)

Veuillez vous reporter à cette liste ou vérifier auprès de votre fournisseur, de votre acquéreur ou de l'entreprise qui traite vos données si la conformité de votre application de paiement à la PA-DSS a été validée.

POUR EN SAVOIR PLUS

Votre acquéreur peut vous communiquer plus de détails au sujet de l'applicabilité des exigences de la PCI DSS. De plus, les ressources ci-dessous sont à votre disposition :

MasterCard

Le site Web PCI 360 de MasterCard contient des renseignements complémentaires, soit des livres blancs et une vingtaine de webinaires sur la sécurité des données des titulaires de carte. Ce site offre des programmes de formation de niveaux débutant à expert adaptés aux besoins des commerces de toute taille et complexité.

Portail d'information PCI 360 de MasterCard : <http://www.mastercard.com/pci360> (en anglais)

Conseil des normes de sécurité du secteur des cartes de paiement

Le Conseil des normes de sécurité du secteur des cartes de paiement propose un éventail de documents sur son site Web ainsi qu'un microsite qui s'adresse aux petits commerçants.

Site du Conseil des normes de sécurité du SCP : <https://www.pcisecuritystandards.org>

Site du Conseil des normes de sécurité du SCP destiné aux petits commerçants :

<https://www.pcisecuritystandards.org/smb> (en anglais)

Évaluateurs qualifiés en matière de sécurité (QSA)

Le Conseil des normes de sécurité du SCP gère un programme à l'intention des évaluateurs qualifiés en matière de sécurité (*Qualified Security Assessor* ou *QSA*) attestant que ces évaluateurs ont été dûment formés pour évaluer la conformité des entreprises à ses exigences. Les QSA reçoivent une formation complète sur les exigences de la PCI DSS, disposent d'une solide expérience en matière de sécurité de l'information et sont soumis périodiquement à un programme d'assurance qualité rigoureux. Les QSA peuvent faire office de consultants et de vérificateurs spécialisés dans les exigences de la PCI DSS.

Une liste de QSA agréés figure sur le site Web du Conseil des normes de sécurité du SCP :

https://www.pcisecuritystandards.org/approved_companies_providers/qualified_security_assessors.php
(en anglais)

Fournisseurs de balayages de sécurité agréés (ASV)

Le Conseil des normes de sécurité du SCP gère les fournisseurs de balayages de sécurité agréés (Approved Scanning Vendors ou ASV). Les ASV valident l'adhésion des commerçants et des fournisseurs de services à certaines exigences en matière de sécurité des données en effectuant des analyses de vulnérabilité de leurs environnements en ligne. Dans le cas où un commerçant utilise des technologies Internet pour ses processus d'affaires parallèlement à ses systèmes de cartes de paiement, le recours à un ASV est nécessaire pour assurer que les pirates informatiques ne tirent pas parti d'un accès ouvert au moyen d'Internet pour s'introduire dans les systèmes du commerçant contenant les données des titulaires de carte. Le Conseil des normes de sécurité du SCP a approuvé plus de 130 ASV, mais les petits commerçants sont invités à se faire recommander des ASV par leur acquéreur ou l'entreprise qui traite leurs données.

Une liste des ASV actuellement agréés est accessible sur le site Web du Conseil des normes de sécurité du SCP :

https://www.pcisecuritystandards.org/approved_companies_providers/approved_scanning_vendors.php
(en anglais)

DE JOSHUA KNOPP, CISSP MASTERCARD WORLDWIDE



Pour toutes informations complémentaires sur les ressources éducatives MasterCard PCI 360, veuillez visiter notre site: www.mastercard.com/pci360 ou www.mastercard.com/sdp.