PCI… DSS et SSC, c'est quoi ?

Que veut dire PCI DSS ?

PCI DSS est l'acronyme anglais de Payment Card Industry Data Security Standard. Une traduction française serait « *standard de sécurité des données pour l'industrie des cartes de paiement* ».

Qu'est ce que le programme PCI DSS ?

Les données de la carte bancaire que sont le numéro de carte, la date de fin de validité et les trois chiffres au dos de la carte sont devenues sensibles car elle permettent de faire un paiement sur internet sans présence physique de la carte. Les fraudeurs cherchent à capturer ces numéros en attaquant les systèmes d'information des acteurs qui stockent ces données. Le programme PCI DSS vise à améliorer la sécurité physique et logique des systèmes d'information en demandant aux acteurs de respecter des bonnes pratiques de sécurité.

Qu'est ce que le standard PCI DSS ?

Le standard PCI DSS liste un ensemble de points de contrôles relatifs aux systèmes d'informations qui capturent, transportent, stockent et traitent des données de cartes bancaires. Les points de contrôles sont relatifs à des techniques informatiques mais également à des procédures et à des contrôles organisationnels sur ces systèmes.

Le standard PCI DSS et les autres standards associés sont disponibles sur le site de PCI Security Standards Council (PCI SSC, voir ci-dessous) à l'adresse https://www.pcisecuritystandards.org/security_standards/documents.php

Qu'est ce que la conformité à PCI DSS ?

La conformité à PCI DSS permet de vérifier que les points de contrôles sont bien mis en œuvre et qu'ils sont efficaces pour la protection des données de cartes bancaires. Cette conformité passe selon la taille du commerçant (voir niveau de commerçant) par un audit effectué par un auditeur agréé ou par un questionnaire d'auto-évaluation à remplir par l'acteur concerné et à le transmettre à sa banque. Cette conformité doit être vérifiée annuellement ainsi que par des tests techniques validant la bonne protection du site de l'acteur.

A qui s'adresse PCI DSS ?

PCI DSS s'adresse à tous les acteurs qui capturent, transportent, stockent et/ou traitent des données de cartes bancaires. Les commerçants de proximité, les marchands sur internet, les réseaux de transport, les centres d'appels, les banques, les émetteurs de cartes font partie des acteurs concernés par PCI DSS.

Est-ce que PCI DSS s'applique à moi ?

Le programme PCI DSS s'applique à tout acteur qui stocke, traite ou transmet des données de cartes bancaires. Le nombre de données cartes manipulées importe peu même si le risque est proportionnel au volume de transactions de paiement traitées. Les acteurs qui traitent manuellement et stockent des supports papier contenant des données de cartes bancaires sont également concernés (reçus papier, talon de commande, données reçues par fax ou mail.

A - Les rôles des réseaux et de PCI SSC

Qu'est-ce que le PCI Security Standards Council (PCI SSC) ?

Le PCI SSC est une organisation américaine dont le rôle est de définir les standards PCI et de gérer leur cycle de vie pour le compte de la communauté des acteurs concernés, réseaux, établissements bancaires et marchands. Le PCI SSC maintient également une liste de sociétés agréées pour effectuer les contrôles de conformité et les analyses de vulnérabilité des systèmes d'information. Enfin le PCI SSC dispense des formations (ISA, Internal Security Assessor), qualifie les auditeurs de sécurité (QSA, Qualified Security Assessor)) habilités à réaliser des audits sur site et approuve les fournisseurs de solutions de sécurité pour effectuer des scans de vulnérabilité (ASV, Approved Scanning Vendor).

La présentation du PCI SSC et les standards associés sont disponibles sur le site de PCI SSC à l'adresse **https://www.pcisecuritystandards.org**

Quel est le lien entre PCI DSS et les programmes SDP de MasterCard et AIS de Visa ?

Les programmes Security Data Protection de MasterCard et Account information Security de Visa sont des règles contractuelles établies entre ces réseaux et leurs affiliés (Etablissements de crédit et de paiement) qui définissent le niveau de mise en conformité au regard des normes définies par le PCI SSC. Par exemple ce n'est pas le PCI SSC qui applique les éventuelles pénalités mais chaque réseau en fonction de ses règles.

B – Valider sa conformité à PCI DSS ?

Est-ce que tous les commerçants doivent être conformes PCI DSS ?

Oui, tous les commerçants devront à terme être conformes à PCI DSS.

Que signifie le classement par niveau de 1 à 4 ?

Qu'un marchand accepte quelques paiements par carte par an ou plusieurs millions, il peut être classé dans l'un des quatre niveaux suivants définis par les réseaux internationaux :

Niveau	Type d'activité	Actions requises pour la conformité
1	Tout commerçant traitant plus de 6 millions de transactions Visa ou MasterCard par an, Tout commerçant ayant subit une compromission	Audit de sécurité sur site (ou SAQ pour Visa Europe) Scan de vulnérabilité trimestriel (si commerce en ligne)
2	Tout commerçant traitant de 1 à 6 millions de transactions Visa ou MasterCard par an	Questionnaire d'auto-évaluation annuel Scan de vulnérabilité trimestriel (si commerce en ligne)
3	Tout commerçant traitant de 20.000 à 1 million de transactions Visa ou MasterCard par an	Questionnaire d'auto-évaluation annuel Scan de vulnérabilité trimestriel (si commerce en ligne)
4	Tout commerçant traitant moins de 20.000 transaction de commerce en ligne Visa ou MasterCard par an. Tous les autres commerçants traitant jusqu'à 1 million de transactions Visa ou MasterCard par an	Questionnaire d'auto-évaluation annuel Scan de vulnérabilité trimestriel recommandé (si commerce en ligne) (cela dépend si les données sont capturées, stockées ou transmises par l'infrastructure du commerçant ou par un fournisseur de services)

Si une compromission intervient chez un commerçant ou l'un de ses prestataires, le commerçant est automatiquement reclassifié en niveau 1 pour 12 mois après avoir validé sa conformité.

Des tableaux similaires précisant les spécificités de chaque réseau peuvent être consultés sur les sites de **Visa** et **MasterCard**.

Que sont les questionnaires d'auto-évaluation ?

Un commerçant qui est de niveau 2 à 4 doit remplir un questionnaire d'auto-évaluation adapté à son activité. Les questionnaires d'auto-évaluation (SAQ, Self-Assessment Questionnaire) sont des documents contenant une série de questions auxquelles le commerçant doit répondre. Les formats types de ces questionnaires sont maintenus par le PCI SSC et sont disponibles sur son site.

Le commerçant doit remplir deux documents, le questionnaire d'auto-évaluation et l'attestation de conformité par laquelle il certifie que les réponses au questionnaire sont vraies et qu'il a mis en place toutes les mesures de PCI DSS pour protéger les données cartes de paiement, qu'il traite.

Quel processus doit suivre le questionnaire d'auto-évaluation ?

Une fois que le questionnaire et l'attestation de conformité ont été remplis et signés par l'acteur concerné, celui-ci doit le remettre à l'établissement de paiement ou de crédit avec lequel il a un contrat d'acceptation de cartes de paiement.

Comment choisir le questionnaire d'auto-évaluation pour mon domaine d'activité ?

Il y a cinq types de questionnaires différents selon l'activité du commerçant :

Questionnaire A : s'applique à une activité où la carte est non-présente (commerce électronique ou commande par téléphone ou mail) ou lorsque toutes les fonctions liées aux données cartes bancaires sont externalisées.

Questionnaire B : s'applique à une activité où seule une empreinte de carte est prise sans stockage électronique des données ou pour un terminal autonome qui ne stocke pas les données.

Questionnaire C-VT : s'applique à une activité qui utilise des terminaux virtuels basés sur un site web sans stockage électronique des données.

Questionnaire C : s'applique à une activité qui utilise une application de paiement connectée à Internet sans stockage électronique des données.

Questionnaire D : s'applique à toutes les autres activités non décrites dans les types A à C ci-dessus et tous les fournisseurs de service définis par un réseau international éligibles à remplir un questionnaire d'auto-évaluation.

Est-ce que toutes les exigences du standard PCI DSS sont obligatoires ?

Toutes les exigences des 12 rubriques de sécurité doivent être remplies. En revanche certaines exigences peuvent ne pas être applicables par la nature même de l'activité du commerçant (vente à distance, proximité, commerce électronique, etc.). Par exemple, si un commerçant n'utilise pas de solutions Wifi, les exigences correspondantes ne s'appliquent pas.

Qu'est-ce qu'une mesure compensatoire ?

Une mesure compensatoire est une solution visant à atteindre l'objectif de sécurité d'une exigence qui peut être différente de celle proposée par le standard. Dans certains cas dus à des contraintes issues de l'activité métier ou à des implémentations techniques particulières, l'exigence ne peut pas être remplie selon les dispositions explicitement proposées par la norme.

La mesure compensatoire doit présenter la même couverture de risque que la mesure initialement prévue et doit satisfaire des critères précis :

- Elle doit respecter l'intention et la rigueur de la mesure initiale ;
- Elle doit fournir une protection similaire à celle de la mesure initiale, de sorte que la mesure compensatoire couvre autant le risque que la mesure initiale devait le faire ;
- Elle ne doit pas se réduire à reprendre d'autres mesures déjà en place afin couvrir l'objectif de sécurité concerné, mais aller au-delà des autres mesures de PCI DSS ;
- Elle doit prendre en compte le risque additionnel qu'implique le non respect strict de la mesure initiale.

Comment faire si je confie mes flux CB à plusieurs banques ?

A ce jour, chaque banque est dans l'obligation de communiquer aux réseaux internationaux son propre déclaratif de conformité à PCI DSS, pour les commerces et prestataires de services qu'elle gère.

CB travaille avec ses membres et les réseaux internationaux sur une possibilité de déclaratif unique qu'il pourrait émettre pour le compte de ses membres

Y-a-t-il une date limite pour être conforme ?

OUI, elle dépend de la réglementation des réseaux en la matière :

Pour VISA :

Implémentation au travers des programmes AIS (Account Information Security) et DCRS (Data Compromise Recovery Solution de Juil. 2007).

Implémentation obligatoire de ce programme depuis le 27 Fev. 2009 (Cf. ML VE 28/06)

cf. ML VE 27/09 :

Pour le 01 Oct. 2009 : Tous les commerçants Internet doivent soit être conformes à PCI DSS, soit utiliser un prestataire de service conforme à PCI DSS.

A compter du 1 octobre 2010 : les acquéreurs doivent s'assurer que tous leurs sous traitants de services relatifs au paiement, sont certifiés PCI DSS.

Pour le 31 décembre 2012 : les acquéreurs doivent s'assurer que tous leurs commerçants sont totalement conformes à PCI DSS ou bien utilisent une application conforme PA DSS.

Pour MCW :

Implémentation au travers des programmes SDP (Site Data Protection) et ADC (Account Data Compromise de Avr. 2010).

Cf. Global Security Bulletin N°12 (déc. 2009) , modifié par Q2 2010 newsletter:

Immédiatement :

Pour les commerces de niveau 1: ils doivent être conformes à PCI DSS. L'audit par un *QSA est non formellement obligatoire (peut être réalisé en interne).*

A partir du 1 juillet 2011 **:** Si 'self audit' ,l'auditeur interne doit avoir suivi la formation PCISSC (ISA training) et subi les examens avec succès.

Immédiatement :

Pour les commerces de niveau 2: ils doivent être conformes à PCI DSS, via la réalisation d'un SAQ.

A partir du 1 juillet 2011 **:** les personnels d'audit interne doivent avoir suivi la formation PCISSC (ISA training) et subi les examens avec succès.

Pour CB :

CODIR de Juin 2007 : le GIE CB demande aux industriels de développer immédiatement le masquage de la zone discrétionnaire de la piste magnétique (Bulletin N°10 CB).

CODIR de Nov. 2007 : L'ensemble des contrats acceptation 'VAD sécurisée' doit être modifié avec une clause d'interdiction de stockage des données sensibles, éditée comme suit : ' l'Accepteur s'engage à ne pas stocker, sous quelque forme que ce soit, aucune des données cartes suivantes : cryptogramme visuel, piste magnétique dans son intégralité, code confidentiel'.

➔ **Aspects obligatoirement inclus dans les contrats 'Acceptation CB VADS' à partir de Juillet 2008.**

CODIR de Juin. 2010 : Une clause mentionnant clairement l'obligation de conformité à PCI DSS sera intégrée à l'ensemble des contrats acceptation CB à compter du 2nd semestre 2010.

Le bulletin N°13 CB (obligatoire à compter du 1er janvier 2011) permet une mise en conformité à PCI DSS de la troncature du PAN présent sur le ticket commerçant.

C - Les scans externes trimestriels

A qui s'adresser pour réaliser des scans externes ?

Pour être conforme à PCI DSS tout acteur doit réaliser des tests de vulnérabilité trimestriels de ses points d'accès sur Internet. Pour cela l'acteur peut choisir parmi les fournisseurs de solutions de sécurité approuvés pour effectuer des scans de vulnérabilité (ASV, Approved Scanning Vendors) disponible sur le site de PCI SSC.

Qu'est-ce qu'une adresse IP

Une adresse IP (Internet Protocol) est un numéro d'identification qui est attribué à chaque branchement d'appareil à un réseau informatique utilisant l'Internet Protocol. En particulier les points d'accès réseau sur Internet sont référencés par une adresse IP.

Lors d'un scan de vulnérabilité le dispositif analyse chaque adresse IP de l'acteur afin de contrôler la vulnérabilité des services disponibles sur cette adresse.

Pourquoi réaliser des scans ?

Les services disponibles derrière une adresse IP peuvent dans certains cas présenter des vulnérabilités connues utilisables par des personnes mal intentionnées (hackers) pour pénétrer le système d'information à l'insu de son propriétaire. Si le hacker arrive à prendre la main sur le système d'information il peut retrouver des fichiers ou bases de données contenant des numéros de cartes bancaires. Il est alors en mesure de les voler.

Les scans de vulnérabilité analysent les failles connues et établissent un rapport qui permettra le cas échéant à l'acteur concerné de corriger ces failles.

Pourquoi renouveler les scans tous les trimestres ?

Un système d'information évolue en permanence avec l'ajout ou la suppression de matériels, avec la mise à jour de logiciels de systèmes d'exploitation ou d'application informatiques, avec la modification du paramétrage des équipements de sécurité et de réseaux.

Même si à un moment donné le rapport de scan ne présente aucune vulnérabilité, les modifications apportées sur le système ou des erreurs de programmation qui ont pu être faites postérieurement à ce scan ont pu ouvrir de nouvelles failles. Par ailleurs, la veille sur les vulnérabilités fait régulièrement apparaître de nouvelles failles qui sont rapidement prises en compte par les outils d'analyse.

Il est donc important de réaliser les scans périodiquement. Il est même conseillé de réaliser des scans immédiatement après une modification majeure du système d'information et ne pas attendre le prochain scan trimestriel.

Les scans ne s'appliquent-ils qu'aux sites internet ?

Les scans s'appliquent à tout système d'information visible depuis Internet (adresse IP accessible depuis Internet). Il peut s'agir d'un site web commerçant mais également de tout autre point d'entrée sur un système d'information de l'acteur concerné (ex : téléphonie IP).

La réalisation des scans peut-elle avoir des conséquences sur mon système ?

Oui, les scans doivent etre réalisées par des professionnels habilités (ASVs)

Un exemple, les logiciels de scans utilisent couramment des attaques de type 'PortScan', qui correspondent à un balayage de ports. Cette activité est considérée comme suspecte par un **système de détection d'intrusion** (IDS). Un système de détection d'intrusion peut être réglé à différents niveaux de sensibilité. Un niveau de sensibilité élevé génèrera plus de fausses alertes, un niveau de sensibilité bas risque de laisser passer les balayages effectués par des systèmes sophistiqués comme '**Nmap**' qui disposent de diverses options pour camoufler leurs balayages.

Pour tromper la vigilance des systèmes de détection et des **pare-feu**, les balayages peuvent se faire dans un ordre aléatoire, avec une vitesse excessivement lente (par exemple sur plusieurs jours), ou à partir de plusieurs **adresses IP**.

Les balayages de ports se font habituellement sur le protocole **TCP** ; néanmoins, certains logiciels permettent aussi d'effectuer des balayages **UDP**. Cette dernière fonctionnalité est beaucoup moins fiable, UDP étant orienté sans connexion, le service ne répondra que si la requête correspond à un modèle précis variant selon le logiciel serveur utilisé.

Que trouve-t-on dans le rapport de scan ?

Un rapport de scan liste, pour chaque adresse IP déclarée dans la portée de l'analyse, la liste des constats effectué par l'outil sur les services visibles derrière cette adresse IP. L'outil se base sur les failles connues en l'état de l'art de la veille sécuritaire.

Le rapport présente généralement un classement par importance des failles de sécurité constatées sur le système analysé. Le rapport doit être analysé par un spécialiste informatique afin de prendre les mesures appropriées pour corriger les failles constatées.

D -Les prestataires

Comment savoir si mon prestataire de service de paiement est conforme PCI DSS ?

Il suffit de consulter les listes régulièrement mises à jour sur les sites :

MasterCard : http://www.mastercard.com/us/sdp/serviceproviders/index.html

Cliquer sur « Service Providers » puis « Compliant Service Providers » puis « Compliant Service Provider List »

Visa : http://www.visaeurope.com/aboutvisa/security/ais/resourcesanddownloads.jsp

Cliquer sur « List of Service Providers » dans la rubtique « Procedures and guidelines »

Vous pouvez également demander au prestataire son Attestation de Conformité.

De quels autres prestataires parle-t-on ?

Il s'agit de tout prestataire qui, pour une raison ou une autre, stocke, traite ou transmet des données cartes. De tels prestataires peuvent être : des revendeurs, des prestataires de traitements de paiement (PSP), des hébergeurs de sites web, des centres d'appel, etc.