LES DOSSIERS TECHNIQUES

PCI DSS v3.0 : Un standard mature ?

Juin 2014

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

11 rue de Mogador - 75009 Paris
Tél. : +33 1 53 25 08 80 – Fax : +33 1 53 25 08 88
clusif@clusif.fr – www.clusif.fr

Table des matières

Remerciements

Le CLUSIF tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

Le responsable du groupe de travail :

Gabriel	**LEPERLIER**	*Verizon*

Les contributeurs :

Thierry	**AUTRET**	*GIE CB*
Pierre-Emmanuel	**LERICHE**	*Verizon*
Thomas	**NGUYEN VAN**	*Sekoia*
Annabelle	**TRAVERS-VIAUD**	*Bull*
Jean-Marc	**GREMY**	*Cabestan*
Loïc	**BREAT**	*Verizon*
Ronan	**BERTHIN-HUGAULT**	*Provadys*
Xavier	**MICHAUD**	*Solucom*
Sebastien	**GIORIA**	*Advens*
Hervé	**SCHAUER**	*HSC*

Le **CLUSIF** remercie également les adhérents ayant participé à la relecture.

Introduction – Synthèse de la brève

Le 7 novembre 2013 est parue la nouvelle version 3.0 du standard PCI DSS (Payment Card Industry Data Security Standard), l'occasion pour le CLUSIF de publier cette brève présentant les quelques évolutions majeures relevées par les membres de ce groupe de travail.

Pour rappel, le standard PCI DSS, visant à harmoniser et renforcer la protection des données bancaires des réseaux cartes Visa, MasterCard, American Express, JCB et Discover, suit un cycle de vie de 3 ans avant qu'une nouvelle version majeure ne soit publiée. Ainsi cette nouvelle mouture est applicable depuis le 1er janvier 2014, tout comme l'est encore la version 2.0, et sera exigible au 1er janvier 2015, date à laquelle la version 2.0 sera rendue obsolète.

Ce référentiel de sécurité est-il d'ores et déjà mature ?

La version 3.0 de PCI DSS apporte beaucoup de clarifications, nombre de conseils ou orientations ainsi que quelques évolutions d'exigences. Le présent document présente certaines évolutions identifiées, leurs incidences sur l'implémentation par l'organisme, et le contrôle de la conformité par le QSA (« Qualified Security Auditor »).

PCI DSS 3.0 met tout d'abord l'accent sur la prise en compte des exigences PCI DSS dans l'activité quotidienne des équipes impliquées, et non pas seulement à l'échéance de jalons récurrents dans l'année. Cette notion de conformité traitée comme « Business-as-Usual » fait l'objet d'une nouvelle section complète de 2 pages, preuve s'il en est que nombreuses encore seraient les sociétés qui n'appliquent PCI DSS qu'au coup par coup, avant chaque échéance d'audit de certification. On pourrait apparenter cette activité à une sorte de contrôle permanent interne, qui n'est pas une réelle évolution par rapport à la version 2.0 tant les sujets évoqués étaient déjà bien présents mais « Si cela va sans dire, cela ira encore mieux en le disant » *Talleyrand-Périgord*.

Quelles sont alors ces réelles évolutions ?

La première des évolutions ne serait qu'une clarification selon l'avis de certains, mais une clarification ayant un impact fort pour bon nombre de sociétés assujetties à PCI DSS, surtout dans le domaine de l'eCommerce : la définition du périmètre soumis à PCI DSS a été précisée et celle-ci fait mention de l'utilisation des serveurs de redirection, serveurs sur lesquels le référentiel s'applique. L'actuel SAQ-A était destiné aux acteurs du eCommerce. Ce SAQ se focalisait sur quelques considérations de sécurité physique et organisationnelle, et pouvait sembler vidé de toute substance pertinente du fait de l'externalisation par les acteurs du eCommerce des flux de paiement vers leur banque ou un PSP (Payment Service Provider). Un nouveau SAQ eCommerce a été publié par le PCI SSC depuis peu pour remplacer l'actuel et ainsi mieux représenter cette activité clé dans l'écosystème des transactions par carte bancaire.

Une autre évolution concerne la gestion des données d'authentification sensibles par les émetteurs de cartes. Ces données, interdites de stockage pour la plupart des acteurs concernés par PCI DSS, doivent faire l'objet d'un traitement particulier par les sociétés émettrices de cartes qui, par la nature même de leur activité, se doivent de les conserver. La version 3.0 ajoute des exigences applicables à la gestion spécifique des données d'authentification sensibles, là où le référentiel 2.0 ne l'évoquait qu'à peine. Des précisions sont également apportées pour ceux qui reçoivent ces données sans besoin de stockage post-autorisation.

Aussi, une nouvelle exigence concerne la protection des clés de chiffrement. Si le dossier technique du CLUSIF paru en 2012 « **Gestion des secrets cryptographiques : usages et bonnes pratiques »** vous donne déjà toutes les bonnes clés en la matière, la version 3.0 du standard PCI DSS précise également quelque peu ce qui est attendu.

Les virus et autres malwares (logiciels malveillants) ne sont pas en reste car eux aussi ont attiré l'attention des rédacteurs du PCI DSS 3.0. En effet, l'idée est de mettre fin au débat souvent quasi passionnel qui anime l'évaluation du chapitre 5 PCI DSS : Alors Anti-virus ou pas sur mon Linux ou mon MAC ? Et bien ce processus de décision doit être maintenant décrit et sous contrôle.

Si la version finale du standard PCI DSS 3.0 est édulcorée d'une nouvelle exigence présente dans la version « Draft » quant aux développements sécurisés du traitement du PAN (Primary Account Number) en mémoire, il n'en demeure pas moins une nouvelle exigence présente pour améliorer la protection autour de la gestion des ID utilisateurs.

Au chapitre de la protection physique, de nouvelles exigences se rapportent à la protection des terminaux de paiements. En effet, ces derniers ont été la cible des attaques parmi les plus spectaculaires et il n'est pas vain de préciser quelles sont les nouvelles attentes en la matière. Cette partie aura un impact considérable pour les plus gros commerçants disposant de centaines voire de milliers d'équipements en magasins.

Enfin, la partie contractuelle liant les acteurs PCI DSS à leurs fournisseurs de services, qu'ils soient de sécurité ou de paiement a été grandement précisée. L'idée étant que l'on peut s'affranchir de certaines exigences en les transférant, mais que l'on ne s'affranchit jamais des responsabilités associées.

Ces évolutions sont clairement issues d'un processus d'amélioration continue dont les points d'entrée ont été les nombreux cas de compromission survenus sur la période 2011-2013, visant en particulier, mais non exclusivement, les eCommerçants.

Vous trouverez ci-dessous une analyse plus en détails des évolutions abordées dans cette introduction sous forme de fiches de synthèse.

Bonne lecture !

Clarifications apportées pour la définition du périmètre PCI DSS

Exigence impactée	Type d'exigence	Type d'évolution
Portée/périmètre de l'évaluation de la conformité aux exigences PCI DSS	Organisationnelle et technique	Clarification et nouvelle exigence

Libellé de l'exigence

1. **Additional examples in the introduction of this chapter "Scope of Assessment for Compliance with PCI DSS Requirements":**

   Examples of system components include but are not limited to the following:

   - Systems that provide security services (for example, authentication servers), facilitate segmentation (for example, internal firewalls), or may impact the security of (for example, name resolution or web redirection servers) the CDE1;
   - Any other component or device located within or connected to the CDE.

2. **Clarification in the introduction of this chapter:**

   To confirm the accuracy and appropriateness of PCI DSS scope, perform the following:

   - The entity considers any cardholder data found to be in scope of the PCI DSS assessment and part of the CDE. If the entity identifies data that is not currently included in the CDE, such data should be securely deleted, migrated into the currently defined CDE, or the CDE redefined to include this data;
   - The entity retains documentation that shows how PCI DSS scope was determined. The documentation is retained for assessor review and/or for reference during the next annual PCI DSS scope confirmation activity.

   For each PCI DSS assessment, the assessor is required to validate that the scope of the assessment is accurately defined and documented.

3. **Clarification in the section "Use of Third-Party Service Providers / Outsourcing":**

   Parties should clearly identify the services and system components which are included

[1] CDE : Cardholder Data Environment

Exigence impactée	Type d'exigence	Type d'évolution
Portée/périmètre de l'évaluation de la conformité aux exigences PCI DSS	Organisationnelle et technique	Clarification et nouvelle exigence

in the scope of the service provider's PCI DSS assessment, the specific PCI DSS requirements covered by the service provider, and any requirements which are the responsibility of the service provider's customers to include in their own PCI DSS reviews. For example, a managed hosting provider should clearly define which of their IP addresses are scanned as part of their quarterly vulnerability scan process and which IP addresses are the customer's responsibility to include in their own quarterly scans.

There are two options for third-party service providers to validate compliance:

- They can undergo a PCI DSS assessment on their own and provide evidence to their customers to demonstrate their compliance;
- If they do not undergo their own PCI DSS assessment, they will need to have their services reviewed during the course of each of their customers' PCI DSS assessments.

If the third party undergoes their own PCI DSS assessment, they should provide sufficient evidence to their customers to verify that the scope of the service provider's PCI DSS assessment covered the services applicable to the customer and that the relevant PCI DSS requirements were examined and determined to be in place. The specific type of evidence provided by the service provider to their customers will depend on the agreements/contracts in place between those parties. For example, providing the AOC 2and/or relevant sections of the service provider's ROC 3(redacted to protect any confidential information) could help provide all or some of the information.

Traduction française (à titre informatif)

1. **Ajout dans l'introduction de ce chapitre "Scope of Assessment for Compliance with PCI DSS Requirements":**

Exemples supplémentaires de composants en plus de ceux déjà donnés dans la version 2.0 :

- Systèmes fournissant des services de sécurité (par ex, les serveurs d'authentification), ou facilitant la segmentation (par ex, les firewalls internes), ou pouvant impacter la sécurité du CDE (par ex, les serveurs DNS ou les serveurs de redirection web) ;
- Tout autre composant ou périphérique situé à l'intérieur ou connecté au CDE.

[2] AOC : Attestation Of Compliance

[3] ROC : Report On Compliance

Exigence impactée	Type d'exigence	Type d'évolution
Portée/périmètre de l'évaluation de la conformité aux exigences PCI DSS	Organisationnelle et technique	Clarification et nouvelle exigence

2. Clarification sur l'introduction de ce chapitre:

Pour garantir la précision et la justesse du périmètre PCI DSS, il est important de respecter ce qui suit:

- **L'entité auditée a inventorié et documenté de manière exhaustive tous les actifs et données bancaires dans son environnement de sorte qu'aucune donnée non déclarée dans cet environnement ne puisse subsister** ;
- Dès que toutes les données bancaires ont été localisées et documentées, l'entité auditée utilise ces résultats pour s'assurer que le périmètre PCI DSS est approprié (par exemple, les résultats peuvent être un diagramme ou un inventaire des lieux où sont les données bancaires) ;
- L'entité auditée doit considérer toute donnée bancaire faisant partie du périmètre de l'audit PCI DSS ou d'une partie de l'environnement CDE. Si l'entité auditée identifie des données qui ne sont pas actuellement incluses dans l'environnement CDE, alors ces données devront être détruites de manière sécurisée, migrées dans l'environnement CDE ou redéfinies pour être incluses dans ce dernier ;
- L'entité auditée doit conserver les documents montrant comment le périmètre PCI DSS a été déterminé. Ces documents serviront lors de la revue documentaire du QSA et/ou de référence lors du prochain audit PCI DSS annuel pour confirmer l'activité.

Pour chaque audit PCI DSS, le QSA doit valider que le périmètre a été très clairement défini et documenté.

3. Clarification relative à la section "Use of Third-Party Service Providers / Outsourcing":

Chaque partie devrait clairement identifier:

- Les services et les composants systèmes qui sont inclus dans le périmètre de l'audit PCI DSS du fournisseur de service ;
- Les exigences spécifiques à PCI DSS couvertes par le fournisseur de service ;
- Toutes les exigences PCI DSS qui sont de la responsabilité des clients de ce fournisseur de service à inclure lors de la revue de leur propre audit PCI DSS.

Par exemple dans le cadre des scans de vulnérabilités trimestriels, un prestataire de services managé devrait clairement définir la liste des adresses IP scannées dont celles qui appartiennent aux clients de ce prestataire et qui sont scannées à cette occasion.

Exigence impactée	Type d'exigence	Type d'évolution
Portée/périmètre de l'évaluation de la conformité aux exigences PCI DSS	Organisationnelle et technique	Clarification et nouvelle exigence

Pour valider leur conformité, deux options s'offrent aux fournisseurs de services tiers :

- Ils prennent l'initiative de réaliser un audit PCI DSS à leur charge puis ils fournissent à leurs clients les preuves de leur conformité ;
- Ils ne souhaitent pas mener leur propre audit PCI DSS, ils devront alors fournir la liste des services revus au cours de chaque audit PCI DSS de leurs clients.

Si la tierce partie mène son propre audit PCI DSS, elle devra fournir les preuves nécessaires et suffisantes à leurs clients pour s'assurer que le périmètre de l'audit PCI DSS couvre bien les services applicables à ses clients et que les exigences PCI DSS pertinentes ont été contrôlées et sont opérationnelles.

Les types de preuves spécifiques fournies par les fournisseurs de services à leurs clients dépendent des accords/contrats en place entre ces parties.

Par exemple, l'AOC et/ou les sections les plus appropriées du ROC dédié à ce fournisseur de service (rédigé pour protéger toute information confidentielle) peuvent aider à fournir tout ou partie des informations.

Contrôle de couverture de l'exigence

Avant de commencer l'audit, le QSA validera le périmètre de l'audit PCI DSS à l'aide des documents fournis par l'entité auditée.

D'autre part, si l'entité auditée utilise des fournisseurs de service, le QSA vérifiera que les mesures mises en œuvre par des fournisseurs sont opérationnelles et conformes aux standards PCI DSS.

Le QSA contrôlera la certification PCI DSS de chacun d'entre eux. Le QSA vérifiera que le périmètre de certification de chaque fournisseur est cohérent avec le périmètre de l'entité auditée pour les exigences couvertes par ce fournisseur.

Tous ceux qui ne sont pas certifiés devront apporter les preuves de leur conformité par rapport aux standards PCI DSS dans le cadre de leur prestation par rapport à l'entité auditée.

Point(s) d'attention ou impact(s) à envisager

L'entité auditée devra fournir au QSA les documents suivants :

- Un inventaire exhaustif de tous les composants de sécurité (notamment les firewalls internes, serveurs d'authentification, DNS et/ou de redirection Web,

Exigence impactée	Type d'exigence	Type d'évolution
Portée/périmètre de l'évaluation de la conformité aux exigences PCI DSS	Organisationnelle et technique	Clarification et nouvelle exigence

…) ;

- Un inventaire exhaustif de tout composant ou périphérique sécurité inclus ou connectés à l'environnement CDE ;
- La localisation précise de toutes les données bancaires dans l'environnement CDE et hors de celui-ci ;
- Les méthodologies utilisées pour qualifier le périmètre de l'audit PCI DSS au fil des différents audits réalisés ;
- La liste de tous les fournisseurs de service de l'entité auditée inclus dans l'audit PCI DSS avec les preuves de leur niveau de conformité par rapport au standard PCI DSS pour chaque fournisseur identifié.

Si au cours de l'inventaire des données bancaires, certaines ont été identifiées hors de l'environnement CDE, alors l'entité auditée devra les :

- Détruire de manière sécurisée ;
- Migrer dans l'environnement CDE ;
- Redéfinir le périmètre de l'audit PCI DSS pour être incluses dans ce dernier.

Si l'entité auditée utilise des fournisseurs de service inclus dans le cadre de l'audit PCI DSS, les périmètres devront être clairement identifiés pour déterminer la répartition des rôles et responsabilités de chaque acteur par rapport à chaque exigence du standard PCI DSS (conformément aux exigences 12.8).

La gestion des données sensibles d'authentification par les émetteurs

Exigence impactée	Type d'exigence	Type d'évolution	
3.2	Technique	Précision et nouvelle exigence	

Libellé de l'exigence

3.2.a For issuers and/or companies that support issuing services and store sensitive authentication data, review policies and interview personnel to verify there is a documented business justification for the storage of sensitive authentication data.

3.2.b For issuers and/or companies that support issuing services and store sensitive authentication data, examine data stores and system configurations to verify that the sensitive authentication data is secured.

3.2.c For all other entities, if sensitive authentication data is received, review policies and procedures, and examine system configurations to verify the data is not retained after authorization.

3.2.d For all other entities, if sensitive authentication data is received, review procedures and examine the processes for securely deleting the data to verify that the data is unrecoverable.

Traduction française (à titre informatif)

3.2.a Pour les émetteurs ou entreprises fournissant un service d'émission et stockant des données sensibles d'authentification, revoir les politiques et interroger le personnel afin de prouver l'existence d'un document métier justifiant le stockage des données sensibles d'authentification.

3.2.b Pour les émetteurs ou entreprises fournissant un service d'émission et stockant des données sensibles d'authentification, examiner les données stockées et la configuration des systèmes pour vérifier que les données sensibles d'authentification sont stockées de manière sécurisée.

3.2.c Pour tout autre type d'entité, si les données d'authentification sont reçues, alors revoir les politiques et les procédures et vérifier la configuration des systèmes pour s'assurer qu'aucune donnée est conservée après autorisation.

3.2.d Pour tout autre type d'entité, si les données d'authentification sont reçues, alors examiner les processus de destruction des données afin de vérifier que ces dernières sont irrécupérables (3.2.d).

Contrôle de couverture de l'exigence

Si l'audité est un émetteur ou une entreprise fournissant un service d'émission et stockant des données sensibles d'authentification, alors le QSA devra :

- Identifier la justification métier nécessitant le stockage des données sensibles d'authentification via la revue documentaire des politiques et via les interviews réalisées auprès du personnel ;

Exigence impactée	Type d'exigence	Type d'évolution	
3.2	Technique	Précision et nouvelle exigence	

- Contrôler la configuration des systèmes pour garantir le stockage sécurisé des données sensibles d'authentification.

Pour tout autre type d'entité (non émettrice ou fournissant des services d'émission), si les données d'authentification sont reçues, alors le QSA devra :

- Contrôler qu'après autorisation, aucune donnée sensible n'est conservée à l'aide d'une revue documentaire des politiques et procédures et à l'aide d'un examen de la configuration des systèmes ;
- Vérifier qu'une fois détruite les données ne sont pas récupérables.

Point(s) d'attention ou impact(s) à envisager

Dans la version 2 du standard PCI DSS, l'exigence 3.2 n'exigeait qu'une vérification de l'existence d'une justification métier du besoin de stocker des données sensibles. La méthodologie de vérification n'était pas clairement définie.

La version 3 exige des références documentaires (politiques et procédures) où apparait cette justification métier. De plus, les managers seront interrogés pour valider la connaissance et la nécessité de ce besoin métier.

Enfin, avec cette nouvelle version, le client audité devra mettre à disposition du QSA toutes les configurations des systèmes échantillonnés où sont stockées les données sensibles. De cette manière, le QSA pourra contrôler la robustesse de leur stockage d'une part. D'autre part, il pourra aussi valider leur suppression sécurisée après autorisation.

QUESTIONS EN SUSPENS : (3.2.b) La version 3.0 du standard PCI DSS demande à ce que la conservation des données d'authentification sensibles soit réalisée de manière sécurisée sans préconiser de méthodes particulières, ce qui peut laisser une libre interprétation du caractère « sécurisé ». En effet, le standard précise les méthodes acceptables et acceptées pour le stockage sécurisé des PAN mais pas pour les SAD (« Sensitive Authentication Data »).

Autant il sera possible de contrôler la destruction sécurisée des données SAD une fois la demande d'autorisation déclenchée autant pour les émetteurs de cartes, il n'y aucune recommandation sur les méthodes de sécurisation en fonction des durées de conservation. Le document : Card Production – Logical Security Requirements (PCI SSC) fournit quelques éléments mais n'est pas évoqué ici.

La gestion des clés cryptographiques

Exigence impactée	Type d'exigence	Type d'évolution
3.5.2	Organisationnelle et technique	Clarification et nouvelle exigence

Libellé de l'exigence

3.5.2 Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times:

- **Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key ;**
- **Within a secure cryptographic device (such as a host security module (HSM) or PTS-approved ("Pin Transaction Security") point-of-interaction device) ;**
- **As at least two full-length key components or key shares, in accordance with an industry-accepted method.**

Note: It is not required that public keys be stored in one of these forms.

Traduction française (à titre informatif)

3.5.2 Conserver les clés privées et secrètes utilisées pour chiffrer/déchiffrer les données des porteurs sous au moins l'une des formes suivantes, à tout moment :

- **Chiffrées à l'aide d'une clé de chiffrement de clé, au moins aussi robuste que la clé de chiffrement des données, et conservées séparément de celle-ci ;**
- **Au sein d'un module cryptographique sécurisé (tel qu'un « Hardware Security Module (HSM) » ou un périphérique certifié PTS) ;**
- **Sous forme d'au moins deux clés complètes ou parts de clés, conformément à une méthode reconnue par le secteur d'activité.**

Note : il n'est pas requis que les clés publiques soient stockées selon l'un de ces formats.

Contrôle de couverture de l'exigence

Lors de l'audit, le QSA devra vérifier :

- que les clés utilisées pour chiffrer/déchiffrer les données sont conservées en mettant en œuvre au moins l'un des solutions ci-dessus ;
- que les choix d'implémentation et la configuration liés à la méthode retenue sont pertinents et conformes à l'état de l'art ;
- que les clés de chiffrement de clés, si utilisées, sont au moins aussi robustes que les clés de chiffrement de données qu'elles protègent, et sont conservées séparément de celles-ci,

En vérifiant :

- L'existence et la pertinence des procédures documentées ;
- Les emplacements de stockage des clés, ainsi que les configurations des systèmes

Exigence impactée	Type d'exigence	Type d'évolution
3.5.2	Organisationnelle et technique	Clarification et nouvelle exigence

et des HSM associés.

Point(s) d'attention ou impact(s) à envisager

La nouveauté de l'exigence réside dans la conservation des clés sous une forme non lisible à un instant donné par un individu y accédant.

La sécurisation des clés de chiffrement contre les accès frauduleux par des seules mesures organisationnelles ou des « ACL » positionnées sur les fichiers et répertoires n'est donc pas/plus autorisée… ! Cela permet notamment de prévenir le déchiffrement des données chiffrées, par un attaquant qui accéderait au système, et donc à la clé conservée en clair !

Cette exigence s'applique à la partie secrète des clés de chiffrement des données sensibles (« cardholder data »), c'est-à-dire par exemple à la clé privée dans le cas de clés asymétriques.

Cet objectif peut être atteint par l'une des méthodes ci-dessous :

- Le chiffrement par une clé de chiffrement de clés ;
- La conservation au sein d'un module matériel de sécurité (HSM) ou d'un matériel conforme PTS ;
- La conservation sous forme de parts de clés, selon une méthode reconnue.

Il est également possible de combiner plusieurs de ces méthodes.

L'utilisation de chacune de ces méthodes doit s'accompagner d'une organisation adéquate :

- Dans le cas de la solution 1, les clés de chiffrement des clés doivent bien évidemment être elles-mêmes protégées contre la divulgation et l'utilisation non autorisée (exigence 3.5.2c). PCI DSS V3 n'exige pas qu'elles soient elles-mêmes conservées selon l'une des méthodes ci-dessus ; toutefois, appliquer le même niveau de sécurité constitue une bonne pratique à respecter. De plus, les clés de chiffrement de clés doivent être conservées distinctement des clés qu'elles chiffrent (clés de chiffrement de données). Ce cloisonnement peut être physique ou logique (exigence 3.5.2c). De plus, cette clé doit être « plus forte » que les clés qu'elle protège, i.e. plus longue ;
- Les HSM éventuellement utilisés par la solution 2 doivent être mis en œuvre de façon à garantir l'absence d'utilisation et/ou d'export frauduleux des clés qu'ils conservent. Leur initialisation, leur exploitation et la gestion des secrets associés doivent être faites sous contrôle de l'organisme, et doivent être formalisés ;
- Le partitionnement de secrets en parts de clés doit être réalisé selon un algorithme sûr (Shamir…). Les quorums de secrets nécessaires à la reconstitution de la clé (« M of N ») doivent être choisis judicieusement pour éviter la collusion de porteurs de secrets, tout en garantissant la disponibilité dans le temps.

Nouvelle exigence imposant la veille et l'évaluation des menaces de type Malware

Exigence impactée	Type d'exigence	Type d'évolution
5.1.2	Organisationnelle	Nouvelle exigence

Libellé de l'exigence

For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.

Traduction française (à titre informatif)

Pour les systèmes qui ne sont pas considérés comme communément affectés par des logiciels malfaisants, il s'agit de procéder à une évaluation périodique afin d'évaluer l'évolution des menaces inhérentes aux logiciels malveillants dans le but de confirmer si ces systèmes peuvent continuer à être dispensés du déploiement d'une solution antivirale.

Contrôle de couverture de l'exigence

Lors de l'audit, le QSA pourra valider ou non la couverture de l'exigence par le biais de l'interview des personnes en charge des antivirus et/ou de la veille sécurité pour s'assurer que la veille « anti-virale » intègre bien par exemple les bulletins des éditeurs d'antivirus permettant ou non de statuer sur l'exposition de tel ou tel composant.

Il s'agira pour le QSA d'évaluer la performance de la veille sécurité dans le contexte spécifique des logiciels malfaisants.

Point(s) d'attention ou impact(s) à envisager

Dans la version 2.0 comme dans la version 3.0 du standard PCI DSS, l'exigence 5.1 demandait à ce que des solutions antivirus soient déployées sur des environnements considérés comme fréquemment impactés par tout type de logiciels malfaisants.

Au niveau de la communauté on s'accorde aujourd'hui à dire que pour les environnements Windows, Linux, il est nécessaire de déployer un antivirus même si les offres sur ces derniers environnements ne sont pas toujours très étoffées.

Le débat reste ouvert sur les environnements UNIX type AIX/HP UX/SOLARIS.

Au niveau des Mainframe, il est en général acté qu'une solution antivirus n'est pas nécessaire du fait du nombre quasi inexistant de menaces répertoriées.

Le référentiel ne fixe pas de seuils critiques à partir desquels on doit considérer qu'un système est communément impacté par les menaces liées aux logiciels malfaisants.

En l'absence de seuils définis, il pourra sembler pertinent de considérer qu'un système n'est plus exempté du déploiement d'une solution antivirale dès lors qu'au moins une menace critique existe (Au sens PCI DSS du terme, à savoir : associée à une note CVSS supérieure à 4.0 – cf. 11.2.3b).

Exigence impactée	Type d'exigence	Type d'évolution
5.1.2	Organisationnelle	Nouvelle exigence

La responsabilité va désormais reposer sur l'appréciation de l'audité et donc sur l'efficacité de son processus de veille « virale ».

L'une des questions qui se pose immédiatement concerne l'appréciation du QSA lors de l'audit.

Doit-il juger l'efficacité du processus de veille « virale » ou acter que l'absence d'une solution antivirale pour tel ou tel composant n'est pas viable compte tenu d'éléments tangibles à sa disposition ?

Dans le second cas, doit-on considérer que le QSA pourra décider d'invalider la couverture de l'ensemble des exigences du référentiel tant que le déploiement d'une solution antivirus n'aura pas eu lieu ?

Cette nouvelle exigence permet donc de responsabiliser les personnes en charge de l'exploitation des solutions antivirus et de la veille « virale » pour statuer ou non sur le besoin de déployer des antivirus sur certains environnements considérés jusqu'à présent comme « non risqués ».

Toutefois, la dimension subjective de l'interprétation par l'audité du niveau réel d'exposition de son environnement vis-à-vis des logiciels malfaisants, peut engendrer des différences dans le déploiement de solutions antivirus d'un audité à l'autre.

Le point relatif aux environnements qui devront faire l'objet du déploiement d'une solution antivirale et ceux qui pourront continuer à en être dispensés ne semble donc pas être définitivement tranché par cette nouvelle exigence.

Nouvelle exigence sur les techniques de développement

Exigence impactée	Type d'exigence	Type d'évolution
6.5.10	Technique	Nouvelle exigence

Libellé de l'exigence

Broken authentication and session management.

Note: Requirement 6.5.10 is a best practice until June 30, 2015, after which it becomes a requirement.

Traduction française (à titre informatif)

Violation de l'authentification, mauvaise gestion des sessions applicatives

Note : Cette nouvelle exigence fait partie des bonnes pratiques jusqu'au 30 juin 2015. Passée cette date, cela devient une exigence.

Contrôle de couverture de l'exigence

Lors de l'audit, le QSA pourra valider ou non la couverture de l'exigence après avoir examiné les politiques et procédures de développement des applications et interrogé le responsable des développeurs afin de vérifier que l'authentification est correctement implémentée, ainsi que la gestion des sessions applicatives. En particulier, il pourra vérifier a minima que le développement comporte :

- L'utilisation d'un élément aléatoire pour l'identifiant de sessions ;
- La non-divulgation d'IDs de session dans l'URL ;
- L'ajout de time-out appropriés et la rotation des IDs de session après une connexion réussie. Les éléments de sessions et d'authentifications transitent sur des canaux sécurisés (TLS, IPSec, Cookies Secure, …).

Point(s) d'attention ou impact(s) à envisager

L'objectif de cette nouvelle exigence est de limiter la prédictibilité des IDs (identifiants de session) et donc l'usurpation d'identité des utilisateurs connectés.

Dans le cas d'une attaque par MITM (« Man-in-the-Middle »), les cookies ne comportant pas l'attribut « secure », peuvent transiter sur un canal réseau non sécurisé. Il est donc possible de les intercepter et de les rejouer pour accéder aux sites sur le compte de la personne sans authentification.

Dans le cas d'une injection de code javascript sur le client (XSS par exemple), il est possible de récupérer le cookie et de le rejouer.

Par ailleurs, si aucun timeout de session n'est mis en place, la validité de la session peut permettre dans le cas de la récupération de l'ID de session dans un log de se faire passer pour l'utilisateur.

Exigence impactée	Type d'exigence	Type d'évolution
6.5.10	Technique	Nouvelle exigence

Par conséquent, il est vivement recommandé aux clients souhaitant être conformes aux standards PCI DSS de prendre en compte les points de contrôle suivants :

- Non divulgation des infos dans les URLs : analyse des logs des serveurs web pour contrôler qu'aucun IDs de session n'apparait dans les URLs ;
- Marquage de jetons de session : Vérifier dans l'entête Set-Cookie, que le cookie dispose de l'attribut « secure », ou via l'analyse de code source l'utilisation de la méthode/fonction de cookie dite « Secure » ;
- Timeout : revue de code faisant apparaître une classe ou une méthode contrôlant le temps imparti après une connexion réussie ;
- Aléa des IDs de session : Vérification dans le code source de l'utilisation d'une classe ou une méthode permettant d'obtenir des IDs de session suffisamment aléatoires pour ne pas être prédictibles. Vérification sur un nombre important d'ID de sessions de la distribution aléatoire de cet ID. Note : certaines API de randomisation disponibles sur Internet manquent d'entropie. Après avoir généré un grand nombre d'IDs, il est possible de retrouver les mêmes IDs de manière cyclique.

Nouvelle exigence de sécurité physique / inventaire concernant les POS (« Point-of-Sale »)

Exigence impactée	Type d'exigence	Type d'évolution
9.9, 9.9.1, 9.9.2, 9.9.3, 9.10	Organisationnelle et technique	Précisions et nouvelles exigences

Libellé de l'exigence

9.9: Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.

9.9.1: Maintain an up-to-date list of devices.

9.9.2: Periodically inspect device surfaces to detect tampering or substitution.

9.9.3: Provide training for personnel to be aware of attempted tampering or replacement of devices.

9.10: Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties.

Traduction française (à titre informatif)

9.9 : Protéger les périphériques utilisés dans les interactions physiques directes avec la carte contre les risques de compromission et de substitution des terminaux.

9.9.1 : Maintenir à jour une liste des périphériques.

9.9.2 : Inspecter régulièrement les périphériques pour détecter les éventuelles compromissions ou substitutions des terminaux.

9.9.3 : Former le personnel aux risques de substitution ou de compromission des terminaux.

9.10 : S'assurer que la politique de sécurité et les procédures opérationnelles pour restreindre les accès physiques aux données cartes soient clairement documentées, connues et bien appliquées par le personnel concerné.

Contrôle de couverture de l'exigence

Lors de l'audit, le QSA devra :

- S'assurer de la présence dans les politiques de sécurité et des procédures opérationnelles de la mise en œuvre d'un inventaire des périphériques, du contrôle des périphériques et de la sensibilisation des personnels vis-à-vis des risques de compromission et de substitution des périphériques ;
- s'assurer de la disponibilité d'un inventaire à jour des périphériques ;
- s'assurer qu'un contrôle périodique a lieu au niveau des périphériques pour rechercher des traces éventuelles de compromission ou de substitution ;
- S'assurer que le personnel a été sensibilisé vis-à-vis des comportements suspects et de pouvoir notifier en cas de compromission ou de substitution des

Exigence impactée	Type d'exigence	Type d'évolution
9.9, 9.9.1, 9.9.2, 9.9.3, 9.10	Organisationnelle et technique	Précisions et nouvelles exigences

périphériques.

Point(s) d'attention ou impact(s) à envisager

Dans la version 2.0 du standard PCI DSS, l'exigence 9.9 se focalisait sur l'existence d'une procédure de gestion des médias physiques dans laquelle il fallait préciser les modalités de stockage et de maintenance des médias physiques et demander la réalisation périodique d'un inventaire. L'exigence 9.1 précisait la nécessité de tenir à jour un inventaire des médias physiques et que cet inventaire soit réalisé au moins une fois par an.

La version 3.0 du standard PCI DSS précise les attentes par rapport à l'exigence 9.9 en s'inspirant fortement des exigences P2PE (« Point-to-Point Encryption ») où les principes se basent sur :

- Un contrôle régulier de l'état physique des périphériques ;
- Un inventaire précis à l'aide d'outils de gestion des actifs (également appelé asset management) ;
- Une formation adaptée du personnel pour que ce dernier soit capable de détecter les vols ou les violations d'intégrité physiques des périphériques.

Les clients audités devraient donc mettre en place des outils de gestion des actifs pour simplifier la gestion de leurs terminaux de paiement.

Pour que les inventaires réalisés soient représentatifs, il s'agit pour le marchand de s'assurer qu'une information unique comme le numéro de série de chaque terminal (élément de référence) ne soit pas aisément falsifiable compte tenu des environnements dans lesquels les terminaux peuvent être déployés.

Faute de disposer d'un élément d'identification fiable, les marchands pourraient être amenés à s'orienter vers des solutions de sécurisation/verrouillage physique des terminaux qui font sens dans des environnements accessibles librement au public et/ou sans présence humaine constante (guichets automatiques…). Parmi les solutions possibles on trouve :

- utilisation de scellés ;
- mise en place d'un support fixe enchâssant le TPE, avec utilisation de câble de sécurité ;
- une combinaison de solution logique permettant le contrôle de la chaine de paiement et de vidéo-surveillance… .

Ces solutions du marché ont certes fait leurs preuves mais restent onéreuses encore

Exigence impactée	Type d'exigence	Type d'évolution
9.9, 9.9.1, 9.9.2, 9.9.3, 9.10	Organisationnelle et technique	Précisions et nouvelles exigences

aujourd'hui et ne pourront donc pas être envisagées par la plupart des marchands dès lors qu'un volume important de terminaux est impacté.

Pour permettre au personnel impacté de répondre à ces exigences, le référentiel impose le suivi d'un programme de sensibilisation sur les techniques de corruption des périphériques (skimming….) dans ce que l'on pourrait considérer comme une forme d'extension du programme de sensibilisation demandé actuellement.

La méthode envisagée, pour assurer l'identification des périphériques et faciliter ainsi le contrôle périodique, doit prendre en compte le fait que le personnel en charge du contrôle ne disposera pas d'expertise technique pour attester de la compromission ou de la substitution d'un terminal. L'objectif de la mise à niveau du programme de sensibilisation est de faciliter la tâche d'inspection.

D'ailleurs, les supports de formation ou les certificats de formation seraient une excellente preuve pour le QSA pour montrer que le personnel a bien été formé.

Toutefois, le programme de sensibilisation devra être mis à jour dès lors qu'une nouvelle technique permet d'agir sur la sécurité des terminaux ; ce qui impose d'intégrer ces considérations dans le processus de veille sécurité.

Cette évolution du référentiel est légitime et répond à une véritable problématique. Il s'agit maintenant pour les constructeurs de terminaux d'intégrer des fonctionnalités pour assurer l'identification fiable de ces derniers au travers de moyens difficilement contournables et ainsi faciliter la détection des tentatives de compromission ou de substitution des terminaux.

Ces modifications seront nécessaires pour proposer des solutions adaptées aux écosystèmes des différents marchands.

Nouvelle exigence sur les méthodologies de tests d'intrusion

Exigences impactées	Type d'exigence	Type d'évolution
11.3, 11.3.1, 11.3.2, 11.3.3, 11.3.4	Organisationnelle et technique	Ajout d'une exigence et clarification

Libellé de l'exigence

11.3: Implement a methodology for penetration testing.

11.3.1: Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operation system upgrade, a sub-network added to the environment, or a web server added to the environment).

11.3.2: Perform internal penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operation system upgrade, a sub-network added to the environment, or a web server added to the environment).

11.3.3: Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.

11.3.4: If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from in-scope systems.

Traduction française (à titre informatif)

11.3 : Mettre en place une méthodologie de tests d'intrusion.

11.3.1 : Réaliser des tests d'intrusion externes au moins tous les ans ou après une mise à jour ou modification significative d'une application ou de l'infrastructure (ex : mise à jour de système d'exploitation, ajout d'un sous-réseau ou d'un serveur web dans l'environnement).

11.3.2 : Réaliser des tests d'intrusion internes au moins tous les ans ou après une mise à jour ou modification significative d'une application ou de l'infrastructure (ex : mise à jour de système d'exploitation, ajout d'un sous-réseau ou d'un serveur web dans l'environnement).

11.3.3 : Les vulnérabilités exploitables identifiées pendant les tests d'intrusion doivent être corrigées et de nouveaux tests doivent être réalisés pour vérifier les corrections.

11.3.4 : Si la segmentation est utilisée pour isoler le CDE des autres réseaux, alors des tests d'intrusion doivent être réalisés annuellement ou après une modification des méthodes/contrôles de segmentation pour vérifier que les méthodes de segmentation sont

Exigences impactées	Type d'exigence	Type d'évolution
11.3, 11.3.1, 11.3.2, 11.3.3, 11.3.4	Organisationnelle et technique	Ajout d'une exigence et clarification

opérationnelles et efficaces et qu'elles isolent correctement tous les composants inclus dans le périmètre de l'audit par rapport aux autres composants.

Contrôle de couverture de l'exigence

Lors de l'audit, le QSA devra :

- Vérifier le contenu de la procédure d'encadrement des tests d'intrusion incluant la méthodologie qui doit être utilisée ;
- Vérifier que des tests d'intrusion internes et externes sont menés annuellement et après chaque modification significative/mise à jour de l'infrastructure ou des applications ;
- Obtenir les rapports des tests d'intrusion interne et externe ;
- Vérifier que les vulnérabilités exploitables ont été corrigées et qu'une nouvelle vérification a été menée pour valider la correction ;
- Vérifier que les méthodes de segmentation des réseaux permettant d'isoler le CDE des autres réseaux ont bien été testées avec succès.

Point(s) d'attention ou impact(s) à envisager

Dans la version 2.0 du standard PCI DSS, la manière dont devaient être réalisés les tests d'intrusion était peu précise. En revanche dans la version 3.0, il est indiqué qu'une méthodologie de tests d'intrusion doit être mise en œuvre.

Il est évident que cette méthodologie requiert des compétences précises sur le sujet et qu'elle n'est pas à la portée de toutes les entreprises. Si l'entreprise auditée ne dispose pas des compétences en interne pour créer cette méthodologie, elle peut se faire accompagner par une société spécialisée.

Cette méthodologie est considérée comme une bonne pratique jusqu'en juin 2015 où elle deviendra une exigence.

Certes, la nature de la prestation et des livrables est très variable en fonction des prestataires qui réalisent les tests d'intrusion. Toutefois, cette exigence a pour objectif d'obliger les audités à formaliser leur propre méthodologie de tests d'intrusion en s'appuyant sur des guides de bonnes pratiques tels que OWASP (https://www.owasp.org/index.php/OWASP_Testing_Project) ou NIST (http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf).

La méthodologie doit comporter a minima les éléments suivants :

- Etre basée sur référentiel reconnu (ex : NIST SP800-115) ;
- Couvrir l'ensemble du périmètre et les systèmes critiques ;
- Inclure des tests depuis l'intérieur et l'extérieur du réseau ;

Exigences impactées	Type d'exigence	Type d'évolution
11.3, 11.3.1, 11.3.2, 11.3.3, 11.3.4	Organisationnelle et technique	Ajout d'une exigence et clarification

- Inclure la validation de l'efficacité de la segmentation mise en place pour réduire le périmètre ;
- Définir les tests applicatifs à inclure avec au minimum la couverture de l'exigence 6.5 ;
- Définir les tests réseaux à effectuer et inclure aussi bien les composants réseaux que les systèmes d'exploitation ;
- Inclure une revue des menaces et vulnérabilités identifiées durant les 12 derniers mois ;
- Spécifier la durée de rétention des résultats de tests et des activités de remédiation.

Un point qui n'est pas traité directement dans le référentiel et qui devrait faire partie de cette méthodologie est la description de la méthodologie d'évaluation des vulnérabilités. En effet, cette évaluation de la sévérité des vulnérabilités est souvent variable selon les prestataires utilisés. Par conséquent, il semble essentiel que cette évaluation soit précisée dans la méthodologie et communiquée aux prestataires lors de l'appel d'offre.

Par ailleurs, la version 3.0 a introduit la notion d'approche par les risques. Contrairement aux versions précédentes il est clairement indiqué que le type, la profondeur et la complexité des tests d'intrusion dépendent des spécificités de l'environnement et de l'analyse de risques de la société.

Enfin, la version 3.0 a introduit une nouvelle exigence concernant la nécessité de valider la segmentation mise en place pour réduire le périmètre. Cette vérification, qui était implicite dans les versions précédentes, est maintenant une exigence à part entière.

Nouvelles exigences dans les relations contractuelles avec les fournisseurs de services

Exigences impactées	Type d'exigence	Type d'évolution
12.8.2, 12.8.5, 12.9	Organisationnelle	12.9, 12.8.5 Nouvelle exigence 12.8.2 Clarification – Évolution

Libellé de l'exigence

12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.

12.8.5 Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.

12.9 Additional requirement for service providers: Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.

Traduction française (à titre informatif)

12.8.2 Maintenir un accord écrit qui inclut que les fournisseurs de services reconnaissent être responsables de la sécurité des données cartes qu'ils possèdent, ou qu'ils stockent, utilisent ou transmettent pour le compte de leur client, ou par extension, qui peuvent impacter la sécurité de l'environnement des données cartes de leur client.

12.8.5 Pour chaque exigence PCI DSS, expliciter celles qui sont gérées par chaque fournisseur de services et celles qui sont gérées par l'entité auditée.

12.9 Exigence additionnelle pour les fournisseurs de services : Les fournisseurs de services acceptent d'écrire à leurs clients qu'ils sont responsables de la sécurité des données cartes que les fournisseurs de service possèdent, ou qu'ils stockent, utilisent ou transmettent pour le compte de leur client, ou par extension, qui peuvent impacter la sécurité de l'environnement des données cartes de leur client.

Contrôle de couverture de l'exigence

12.8.2 Inspecter les accords écrits et confirmer qu'ils comprennent une partie spécifique des fournisseurs de services explicitant qu'ils sont responsables de la sécurité des données cartes que les fournisseurs de services possèdent ou stockent, traitent ou transmettent pour le compte de leur client, ou dans la mesure où ils pourraient avoir un impact sur la sécurité des données cartes de l'environnement client.

12.8.5 Vérifier que l'entité auditée maintient l'information à propos des exigences PCI DSS

Exigences impactées	Type d'exigence	Type d'évolution
12.8.2, 12.8.5, 12.9	Organisationnelle	12.9, 12.8.5 Nouvelle exigence 12.8.2 Clarification – Évolution

qui sont gérées par chaque fournisseur de services et de celles gérées par l'entité auditée.

12.9 Procédure de test additionnel pour les fournisseurs de services: Revoir les politiques et les procédures du fournisseur de service et observer les modèles d'accord écrits pour confirmer que le fournisseur de service accepte d'écrire à ses clients qu'il maintiendra les exigences PCI DSS applicables aux données cartes ou aux données sensibles d'authentification, qu'il gère, a accès, stocke, utilise ou transmet pour le compte de leur client.

Point(s) d'attention ou impact(s) à envisager

Des clarifications ont été apportées à l'exigence **12.8.2** concernant les relations entre les fournisseurs de services et l'entité auditée, et deux nouvelles exigences **12.8.5** et **12.9** sont apparues. Ces clarifications concernent la partie contractuelle entre les fournisseurs de services et l'entité auditée et permettent d'identifier clairement les zones d'implications et les domaines de responsabilités de chacun dans la poursuite du but global de sécurisation des données cartes en conformité avec PCI DSS.

La clarification de l'exigence 12.8.2 apporte un nouveau degré de responsabilisation. En effet, dans la version 2, il était seulement spécifié que les fournisseurs de services devaient maintenir un accord écrit, explicitant qu'ils étaient responsables des données cartes qui leur étaient confiées. Dans cette nouvelle version, en ajoutant « ***ou qu'ils stockent, utilisent ou transmettent pour le compte de leur client, ou par extension, qui peuvent impacter la sécurité de l'environnement des données cartes de leur client*** », l'exigence est plus claire. Il n'est plus possible pour un fournisseur de services d'ignorer la sécurité et les exigences PCI DSS de son client, et ce, même si les données cartes ne lui appartiennent pas. Cette clarification empêche désormais les fournisseurs de services ou les audités d'interpréter à leur avantage une zone floue des exigences PCI DSS.

De plus, la nouvelle exigence 12.8.5 poursuit le même but de clarification des responsabilités, afin de s'assurer que toutes les exigences PCI DSS sont traitées (par l'entité auditée elle-même, par le fournisseur de services, ou par les deux). L'entité auditée doit être capable d'identifier à quel moment la sécurité des données cartes peut être mise à mal et par qui, régulièrement, même si les contrats entre les entités et les fournisseurs de services peuvent évoluer dans le temps.

Un simple contrat explicitant que le fournisseur de services doit être conforme PCI DSS n'est plus suffisant. Tous les acteurs pouvant impacter la sécurité des données cartes doivent être identifiés et leurs domaines de responsabilités, ainsi que les exigences PCI DSS qui leur incombent explicités et maintenus à jour. Les entités auditées sont désormais forcées de s'intéresser de près à la sécurité de leurs données cartes et ne peuvent plus ignorer PCI DSS, même si elles ont totalement externalisé la gestion de leurs données cartes.

Exigences impactées	Type d'exigence	Type d'évolution
12.8.2, 12.8.5, 12.9	Organisationnelle	12.9, 12.8.5 Nouvelle exigence 12.8.2 Clarification – Évolution

En complément, une nouvelle exigence 12.9 a été ajoutée. Elle constitue avec l'exigence 12.8.2, le complément de la déclaration de responsabilité des clients, mais pour les fournisseurs de services. Elle leur impose de s'engager formellement à se déclarer responsables vis-à-vis de leurs clients, de la sécurité des données cartes qui leur sont confiées (qu'il s'agisse de données auxquelles le fournisseur peut accéder, ou de données stockées, traitées ou transmises) ou dont ils peuvent impacter la sécurité.

En conclusion, ces clarifications et nouvelles exigences imposent essentiellement des engagements écrits de la part des fournisseurs qui ne semblent pas avoir été clairs sur ce qu'ils faisaient des données de leurs clients. Elles vont principalement impacter d'une part les entités auditées qui souhaitaient externaliser la responsabilité de la conformité PCI DSS à leurs fournisseurs de service, sans se soucier de la manière dont le fournisseur de service se préoccupait de ces données ; d'autre part, les fournisseurs de services qui sont désormais forcés de prendre en compte la sécurité des données cartes dans leur globalité (qu'ils possèdent, ou qu'ils traitent, utilisent ou transmettent pour le compte de leurs clients). Elles devraient permettre de valider contractuellement l'absence d'éventuelles ruptures dans les chaînes de responsabilités établies entre un client et ses fournisseurs.

Pour les entités auditées cela clarifie les limites de responsabilités car l'intégralité de celles incombant aux fournisseurs sont clairement écrites : il ne subsistera donc aucune zone d'ombre sur les exigences contractuelles PCI DSS entre les entités auditées et leurs fournisseurs de service.

L'ESPRIT DE L'ÉCHANGE

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS

11 rue Mogador
75009 Paris
✆ 01 53 25 08 80
clusif@clusif.fr

Téléchargez les productions du CLUSIF sur

www.clusif.fr