PAYS : France
PAGE(S) : 1,2
SURFACE : 93 %
PERIODICITE : Bimensuel
DIFFUSION : (200)
Systèmes de Paiemen
► 25 mars 2016 - N°553

interview

Thierry le Forban, Monext : « PCI DSS devient le socle pour la conformité aux prochaines régulations européennes sur la protection des données »

Opérateur de paiements certifié PCI-DSS depuis 2008, Monext a développé une expertise reconnue en matière de conformité pour tous ceux qui doivent traiter et stocker des données de cartes bancaires. Dans cette interview, Thierry le Forban, product manager chez Monext, fait le point sur les toutes récentes évolutions de PCI DSS.

Y aura-t-il des évolutions de PCI DSS en 2016 ?

Il n'y aura pas de version majeure du standard cette année mais des évolutions importantes qui seront regroupées dans la version PCI-DSS 3.2, à paraître en Novembre. Cette version, entre autres, officialisera le changement de calendrier de la migration SSL vers TLS. Cette migration, rendue indispensable par les vulnérabilités découvertes dans le protocole SSL, avait été initialement demandée pour mi-2016. Le feed-back des acteurs concernés était que le délai était trop court : dans l'état de la version 3.1, certaines organisations risquaient de perdre leur certification uniquement à cause de ce point. Le PCI-SSC a repoussé l'échéance de fin de migration à juin 2018, en demandant aux QSA de vérifier qu'un plan d'action de migration est bien en cours et en imposant que toute nouvelle prestation utilise TLS et non plus SSL.

Une autre évolution importante concerne l'authentification forte à deux facteurs pour les administrateurs ayant accès au CDE (Cardholder Data Environment), périmètre réputé sensible puisqu'il contient les PAN des cartes. Les entreprises auront un an pour mettre en œuvre cette disposition qui cherche, entre autres, à éviter les cas de malveillances internes. Certaines études estiment à 40 % les cas de vols de données de tous types ayant origine du personnel de l'entreprise. Cette mise en œuvre de l'authentification forte rejoint les démarches de SecurePay et de l'association européenne des banques EBA qui étudie actuellement ses modalités de mise en œuvre dans le cadre de la DSP2. Cette réflexion est menée en concertation avec les tous les acteurs du paiement, de sorte à éviter certaines erreurs commises lors de la mise en œuvre du 3D Secure.

Le second facteur d'authentification pourra être, par exemple, un « selfie animé» sur mobile ou la reconnaissance de la voix qui viendraient ainsi renforcer l'identifiant et le mot de passe initial. Les solutions biométriques sont, pour la plupart, encore en phase préindustrielle : elles vont certainement encore évoluer, de sorte à prendre en compte, notamment, tous les as-

PAYS : France
PAGE(S) : 1,2
SURFACE : 93 %
PERIODICITE : Bimensuel
DIFFUSION : (200)
Systèmes de Paiemen
► 25 mars 2016 - N°553

pects liés à l'irrévocabilité des données biométriques.

Où en est le standard PCI DSS sur le marché européen ?

Le contexte général pour PCI DSS est favorable dans la mesure où la protection des données devient une préoccupation majeure des instances européennes avec le règlement européen sur la protection des données personnelles (GDPR), dont la parution est attendue pour les semaines à venir. Il comportera des aspects opérationnels et juridiques importants pour les entreprises. On y retrouve des bonnes pratiques communes avec le référentiel PCI DSS comme, par exemple, « pseudonymiser » les données, autrement dit, ne pas les stocker en clair. Cette technique, maîtrisée par Monext, depuis plusieurs années, est équivalente à la tokenisation réversible pour les données cartes. Si PCI DSS est le socle de sécurité reconnu pour le paiement par cartes, au niveau européen, les DSP2 et GDPR généralisent, par la loi, la nécessité d'appliquer un référentiel de sécurité commun aux données de tous types, pour renforcer la confiance du consommateur.

Qu'en est-il de la solution de cryptage P2PE ?

Comme la tokenisation, P2PE reste la méthode préconisée par PCI DSS dans la chaine de paiement de proximité, pour protéger les données entre les systèmes d'acquisition et les terminaux de paiement, y compris mPOS. Leur mise en œuvre permet de réduire le scope de certification et donc les charges et coûts afférents.

Quid de la tokenisation ?

Il y a, à ce jour deux technologies de tokenisation. La première, introduite par ApplePay, est en train de se généraliser pour le paiement mobile. Le mobile ne contient pas les données de la carte mais un jeton de paiement, en général à usage unique. La seconde est l'utilisation d'un alias pour remplacer une donnée sensible au sein d'un système d'information, ce qui le rend insensible aux pertes de données critiques en cas d'attaques.

PCI DSS va-t-il suivre l'évolution du marché vers le cloud ?

Cette évolution vers le cloud devient incontournable. Le PCI SSC propose sur son site des documents en rapport avec l'usage du Cloud. Il ne peut toutefois pas réguler un tel environnement dans son ensemble et je ne pense pas que ce soit sa vocation. Les systèmes sont de plus en plus ouverts, de nouvelles technologies apparaissent tous les jours, les solutions de paiement sont de plus en plus nombreuses sur de multiples canaux : seules de bonnes pratiques, tenant compte de l'usage, permettrons de renforcer la confiance du consommateur. Le référentiel PCI DSS est un socle reconnu sur lequel les différents acteurs peuvent s'appuyer et le PCI SSC a ainsi renouvelé sa communication pour accompagner les entreprises pour atteindre cet objectif et combattre la cybercriminalité dans son ensemble.•