AVIS D'EXPERT

Agences de voyage : PCI DSS devenu obligatoire au 1er mars 2018 !

par Julien Soudée, Project Expert Information Security
et l'équipe Provadys Nantes

a. Introduction - Quelles obligations applicables ?

En 2017, l'**Association internationale du transport aérien** (en anglais International Air Transport Association, ou **IATA**) a annoncé une obligation de se conformer au **standard PCI DSS pour le 1er mars 2018**. Cette obligation concerne toutes les entreprises accréditées auprès de l'IATA.

À compter de cette date, les agences qui n'ont pas transmis leur certificat recevront une demande écrite de la part de l'IATA puis, sans réponse de la part de l'agence, une notification de non-conformité.

Les agences non conformes **ne pourront plus utiliser le code commerçant de la compagnie aérienne**, ce qui entraînera une **augmentation du tarif des transactions** et une **dépréciation d'image auprès des compagnies aériennes**.

La date butoir vient juste d'être dépassée ! Est-ce la fin des haricots ? Rassurez-vous, la France (comme plusieurs autres pays) bénéficie d'un délai supplémentaire comme l'indique le planning fourni par l'IATA (http://www.iata.org/whatwedo/airline-distribution/Documents/NGISS-TIP-Timelines.pdf).

Les **sanctions** ne seront prises **qu'à compter de 2019**.

Il faut néanmoins profiter de ce temps supplémentaire pour réaliser les travaux de mise en conformité, qui peuvent potentiellement être significatifs.

b. Mais PCI DSS, qu'est-ce que c'est ?

PCI DSS est un standard de protection de la **confidentialité des données cartes bancaires (CB)**, résultant d'une analyse menée par les marques de cartes suite à diverses compromissions massives de données CB qui ont défrayé la chronique.

PCI DSS vise à **réduire le risque de vol de données CB**, via la mise en place de mesures **techniques, documentaires, organisationnelles et juridiques** afin d'éviter une perte de confiance dans ce moyen de paiement aujourd'hui très massivement utilisé.

c. Qui est concerné ?

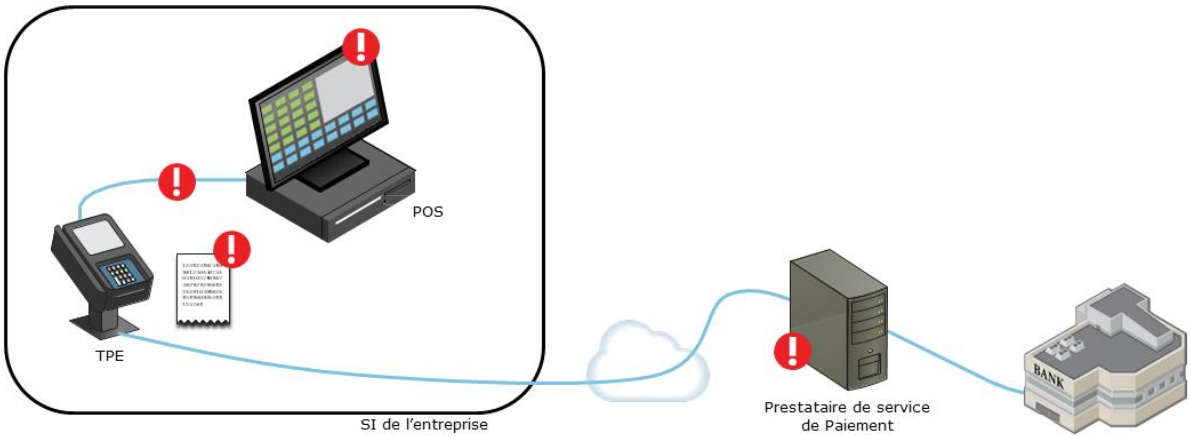
Le standard PCI DSS s'applique à toutes les entités juridiques impliquées dans **le stockage, le traitement et la transmission des données des cartes de paiement**, notamment les commerçants, les banques et les prestataires de services.

Les données CB peuvent donc se retrouver à de multiples endroits au sein d'une entreprise, en fonction des activités et des canaux de ventes proposés :

d. Quelles sont les difficultés ?

En fonction de l'architecture monétique de l'entreprise, la mise en conformité PCI DSS peut être plus ou moins longue et complexe.

Prenons un exemple concret (le paiement de proximité avec terminal de paiement et point d'encaissement) et estimons les risques potentiels. Sur le schéma suivant, les principaux risques sont représentés par une pastille rouge :



Dans cette configuration spécifique, il faudra vérifier la conformité PCI DSS de plusieurs éléments :

- Les processus de gestion des terminaux (inventaire, inspection régulière)
- La relation avec le prestataire de paiement
- Les habilitations des utilisateurs afin que seules les personnes qui en ont besoin dans le cadre de leur activité puissent accéder aux données sensibles (numéros de cartes, etc.)
- La sécurité physique des lieux de stockage des facturettes papiers
- Etc.

En fonction des canaux de vente (e-commerce, VAD MOTO, …) et l'architecture informatique, les problématiques ne seront pas nécessairement les mêmes.

e. Comment s'y prendre ?

La liste précédente n'est (malheureusement) pas exhaustive. Il est donc important de suivre une méthodologie précise afin de réaliser un projet de mise en conformité efficace.

Parmi tous les travaux qu'il va falloir mener, voici quelques exigences emblématiques :

- Protéger les données
- Durcir les systèmes
- Contrôler les accès
- Sensibiliser les utilisateurs
- Documenter (formaliser sa démarche)

f. Conclusion

Bien que les agences de voyage françaises bénéficient d'un délai de grâce (3e trimestre 2019) pour leur mise en conformité PCI DSS, le Règlement Général sur la Protection des Données (RGPD), lui, entre en application dès le mois de mai prochain.

Les données des cartes bancaires sont une des nombreuses données à caractère personnel. Réaliser sa mise en conformité PCI DSS dès à présent peut donc aider à aller vers un respect du RGPD.

Provadys propose des approches concrètes, efficaces, pragmatiques et adaptées aux entreprises pour les aider dans cette aventure de mise en conformité, à la fois sur PCI DSS et le RGPD.

Provadys vous accompagne sur PCI DSS

Provadys est une société de conseil, d'audit et de formation, spécialiste des technologies de l'information, et qualifiée par l'ANSSI.

Nous accompagnons les organisations en matière de Cybersécurité, Infrastructure & Cloud, Transformation du système d'information.

Nous mettons nos savoir-faire au service des DSI et des RSSI pour traiter les défis liés à la sécurisation ou aux mutations des Systèmes d'Information.

Provadys est certifié en tant que « QSA Company », ce qui lui permet de se positionner en tant qu'entité habilitée à réaliser les audits de certification PCI DSS. Les consultants experts de Provadys vous apportent également tout leur retour d'expérience pour vous accompagner dans votre projet de mise en conformité, que ce soit sur PCI DSS ou sur d'autres référentiels de sécurité (ISO 27001, ARJEL, LPM, GDPR, ISAE …).

Provadys rayonne partout en France, possède des bureaux à Paris, Sophia-Antipolis et Nantes et compte plus de 500 clients.

Contacts
Paris : +33 (0)1 46 99 93 80
Sophia-Antopolis : +33 (0)4 28 27 03 16
Nantes : +33 (0)2 55 59 01 10