Sécurité sur les cartes bancaires : une nouvelle norme obligatoire pour les entreprises du tourisme

Par David Savary19 janvier 2018

Depuis le 1er janvier 2018, tous les acteurs marchands ou intermédiaires détenant des cartes de paiement entre les mains doivent appliquer la norme PCI DSS (Payment Card Industry Data Security Standard). L'industrie du tourisme et ses nombreux commerces n'échappe bien évidemment pas à cette obligation. Avec l'avènement d'Internet et du e-commerce, la norme PCI DSS vise à éviter ou minimiser les fraudes sur les cartes de crédit.

« C'est une norme très ancienne. Simplement elle a été renforcée de manière drastique » explique Christophe Suleski, responsable technique chez Bdv.fr A l'initiative d'un consortium de cartes bancaires (Visa, Mastercard, American Express…), le PCI DSS entend réduire la fraude en ligne et sécuriser les paiements. Toute organisation (agence de voyages physique, en ligne, hôtel…) qui traite les données des titulaires de cartes bancaires doit s'y conformer.

Pour Christophe Suleski, de cette norme découle quatre grands principes :

- **Obligation de sécuriser le stockage et le transport des numéros de cartes bancaires selon des normes drastiques.**
- **Interdiction dorénavant de stocker les CVV (cryptogrammes).**
- **Obligation de sécuriser physiquement les personnes ayant accès à des numéros de carte bancaire, notamment au téléphone.**
- **Obligation d'informer et de former le personnel sur les normes de sécurité liées à l'accès aux numéros de cartes bancaires.**

« Chez Bdv.fr par exemple, on ne stocke rien. Nous avons décidé de ne plus faire transiter les numéros de carte par notre serveur. Nous renvoyons directement le client sur la banque » souligne le directeur technique. En résumé, chaque entreprise doit assumer la responsabilité et faire le nécessaire sur la sécurité des données de ses clients.

Quels risques ?

Dans la pratique, aucune loi n'oblige à se conformer à la norme PCI DSS.
« Cependant, explique Christophe Suleski, la conséquence majeure si les investissements technologiques ne sont pas faits est que les banques peuvent aller jusqu'à interdire aux marchands la possibilité de faire des transactions via les cartes bancaires ». « De même, poursuit le responsable, les commissions mises en place par les opérateurs bancaires peuvent varier. Ainsi, une entreprise qui ne serait pas suffisamment sécurisée pourrait voir sa commission augmenter ».

Par ailleurs, si l'on prend l'exemple d'un billet d'avion acheté en agence physique, le vendeur devant son écran passe par un GDS (Travelport, Amadeus…), lequel est certifié PCI DSS ce qui garantit la sécurité de la transaction.

« Cela représente des investissements informatiques à réaliser » reconnait Christophe Suleski, « **mais ce n'est rien à côté de la norme relative au Règlement Général sur la Protection des Données (GDPR)** et qui doit entrer en vigueur au cours de l'année 2018. Là encore les entreprises devront s'y conformer ». Le but du jeu étant de simplifier et harmoniser la protection des données dans les 28 pays de l'Union Européenne.