Stéphane Duproz (TelecityGroup) : « La majorité des points de contrôle PCI-DSS tiennent du bon sens »

Selon le rapport 2012 de l'Observatoire de la Sécurité des Cartes de Paiement (OSCP), les paiements par Internet représentent 61% du montant des fraudes, soit 253 millions d'euros en 2011.

Les consommateurs sont de plus en plus conscients et sensibles face à ces problématiques : nous connaissons tous au moins une personne de notre entourage ayant été victime d'une usurpation d'identité ou d'une utilisation frauduleuse de sa carte bancaire.

Les organismes de cartes de crédit sont désormais passés à la vitesse supérieure. Depuis le 1er janvier 2013, Visa ne couvre plus les transactions non certifiées PCI-DSS (Payment Card Industry Data Security Standard).

Les e-commerçants non conformes aux exigences de ce standard de sécurité international engagent leur responsabilité et s'exposent à des pénalités pouvant s'élever à 385.000 euros, en plus des coûts de remédiations et de remboursement des frais de réémissions des cartes.

Des obligations réglementaires

La norme PCI-DSS définit 12 critères couvrant environ 280 points de contrôle liés à la sécurisation du réseau, la politique de sécurité des informations, la protection des données des titulaires de cartes, la gestion des vulnérabilités, les contrôles d'accès et la surveillance des réseaux.

Elle permet de réduire au maximum les risques d'incidents et engage, par son caractère pyramidal, toute la chaîne du e-commerce : de l'e-marchand à ses fournisseurs de services, de logiciels, d'hébergement et d'infrastructure. Cette chaîne descend jusqu'au datacenter lui-même ! En effet, si le socle qui soutient l'ensemble de l'édifice n'est pas lui-même certifié, quelle chance y a-t-il pour que les couches les plus élevées puissent prouver leur conformité ?

Pour un e-commerçant, il est bien plus facile de répondre aux exigences PCI-DSS si tous les partenaires sous-jacents les satisfont également et sont déjà certifiés. En effet, bien que l'exigence PCI-DSS pèse sur les e-commerçants, les prestataires de la chaîne peuvent également se faire auditer et certifier PCI-DSS afin d'accompagner leurs clients et prospects.

Bien évidemment, l'adoption d'une norme n'est pas, en soi, une garantie d'infaillibilité. Mais elle témoigne d'une exigence de qualité de service, d'un engagement affirmé à protéger ses clients et d'une volonté de lutter contre les fraudes.

Les bénéfices de l'engagement

Adopter et obtenir la certification PCI-DSS peut sembler de prime abord un processus lourd et contraignant que ce soit pour les e-commerçants ou les prestataires IT impliqués dans la chaine.

S'appuyer sur des partenaires déjà certifiés, du datacenter qui héberge les serveurs au fournisseur de la plateforme e-commerce, allège non seulement ce processus, mais témoigne également d'une volonté commune d'offrir le meilleur service possible.

En effet, il n'existe en réalité qu'une seule approche viable pour que la mise en œuvre d'une norme telle que PCI-DSS ne soit pas vécue comme une contrainte, mais comme une opportunité : en faire une culture d'entreprise.

Au fond, l'adoption d'une norme est toujours un processus modelant et structurant. Quand sa philosophie est intégrée, elle n'est plus perçue comme un frein. Son impact doit s'étendre bien au-delà de la multitude des cases de conformité à cocher. Cet engagement pour une amélioration de la qualité devient, au final, un bénéfice pour l'entreprise elle-même comme pour ses clients !

Adopter, c'est aussi anticiper

D'autant que la majorité des points de contrôle PCI-DSS tiennent du bon sens. Ils mènent l'entreprise à définir une politique d'embauche consciencieuse, à définir des droits d'accès, à mettre en place une politique de maintenance vérifiée et vérifiable, à définir des stratégies en matière d'antivirus et de patch des vulnérabilités, etc.

Ces éléments fondamentaux trouvent leur écho bien au-delà de PCI-DSS. Ils témoignent d'une véritable démarche globale de respect de l'entreprise envers ses clients et les données personnelles qu'ils leur confient.

L'adoption de PCI-DSS doit finalement engager chaque acteur du marché. Ne nous y trompons pas, si les organismes de paiement par carte bancaire nous y contraignent aujourd'hui, ils ne sont en réalité annonciateurs que de l'arrivée d'une multiplicité de réglementations toujours plus strictes concernant les données. Ainsi, les CNIL européennes préparent pour 2014 des réglementations qui tendent toutes à renforcer les pénalités encourues.

La mise en conformité est en ce sens une opportunité pour prendre conscience de ces nécessités. Elle permet également d'anticiper l'arrivée de nouvelles règles pour qu'elles ne soient pas vécues, le moment venu, comme autant de freins et contraintes.

Il ne faut pas non plus perdre de vue que les normes sont vivantes : se limiter aujourd'hui au seul cahier des charges actuel de PCI-DSS, c'est l'assurance d'échouer au prochain audit ou à la mise en œuvre de la future version 3.0 de la norme, attendue à l'automne prochain.

À bien y regarder, toute la philosophie de PCI-DSS se résume en un mot : la confiance. Celle que le fournisseur IT peut offrir au marchand et celle que ce dernier peut offrir au consommateur. L'adoption de la norme PCI-DSS prouve alors la valeur de l'engagement d'une société auprès de ses clients.

Stéphane Duproz, directeur général de TelecityGroup France.

Voir aussi

Quiz Silicon.fr – Les temps forts du CES 2013 en dix questions