Et si la conformité PCI était une source d'opportunités business ? (Tribune)

Il devient essentiel que les entreprises considèrent la sécurité PCI comme un élément fondamental de leur stratégie plutôt que comme un enjeu technique. Face au renouvellement permanent des menaces et à la croissance exponentielle des volumes de données, elles se trouvent confrontées à toujours plus de difficultés et de responsabilités : plus elles stockent de données sensibles, plus elles s'exposent aux risques de failles de sécurité et de compromissions de leurs données.

Or un trop grand nombre d'entreprises, après leur évaluation annuelle d'attestation de conformité au standard PCI-DSS (Payment Card Industry Data Security Standard), relà¢chent leur attention et s'exposent alors à des risques majeurs de compromissions de données, de préjudice financier et de réputation. De plus, bon nombre d'entreprises continuent d'envisager la conformité PCI comme une obligation annuelle, alors que le maintien de la conformité exige une attention de tous les jours.

Plus encore : **une entreprise conforme à PCI y trouvera des opportunités business**

Le PCI SSC (PCI Security Standards Council) a expliqué que les changements apportés au standard DSS 3.0 ont pour objectif « d'aider les entreprises à adopter une approche proactive de la protection des données des porteurs de cartes de paiement, davantage centrée sur la sécurité que sur la conformité, pour les inciter à intégrer la sécurité PCI DSS à leurs activités courantes ».

Bien menée, une politique de maintien de la conformité peut aboutir à des améliorations des processus, permettre d'identifier des potentiels de consolidation de l'infrastructure et générer des recettes supplémentaires. Par exemple :

- **Meilleure efficacité de fonctionnement** : les démarches de sécurité PCI sont l'occasion de faire un audit complet des opérations internes et d'améliorer ce qui doit l'être : optimisation des processus, amélioration de la communication interne et sensibilisation accrue de la direction aux questions de sécurité et aux dépenses associées.
- **Gains d'efficacité des services IT** : le maintien de la conformité au standard de sécurité PCI suppose autant de changements IT que stratégiques et fonctionnels. C'est l'occasion de reconsidérer les systèmes, qui sont le fruit d'années voire de dizaines d'années d'investissements,de consolider et moderniser l'infrastructure pour en retirer des avantages multiples en termes de sécurité, de continuité de l'activité, de simplicité d'administration et de performance des systèmes.
- **Diminution des risques** : au début d'un programme de conformité PCI, l'entreprise s'intéresse en profondeur à la protection de l'information à l'échelle de toute l'organisation, parfois pour la première fois. Pour renforcer la sécurité d'ensemble et limiter l'exposition aux risques, elle peut appliquer à d'autres systèmes et d'autres types de données les contrôles de base préconisés pour l'environnement des porteurs de carte bancaire.
- **Innovation accrue** : en plus de combler des lacunes, la conformité au standard de sécurité PCI peut être un moteur d'innovation : adoption de nouvelles technologies

(mobiles, Cloud, etc.), de nouvelles pratiques de travail, de nouveaux business models. Certains commerçants qui ont déployé de nouveaux systèmes point de vente pour se conformer à PCI en ont retiré de multiples bénéfices, de rendement notamment, et des recettes publicitaires.

- **Confiance du client** : les clients vont devenir sans cesse plus exigeants. Certes les technologies d'analyse du Big Data vont permettre de mieux décrypter leur comportement, mais à condition qu'ils aient envie de vous confier leurs données. Leur apporter les garanties que leurs opérations sont protégées selon le standard PCI peut aider à gagner leur confiance dans la marque.

La conformité aide à réduire les risques, mais est-ce que ça rend l'entreprise plus « efficace » pour autant ?

Il faut comprendre que c'est l'ensemble du périmètre de sécurité de l'entreprise qui doit être surveillé constamment, et toutes les règles de protection des données, pas uniquement le degré de conformité au standard de sécurité PCI. Etre 100 % conforme à PCI DSS à un moment donné sur un périmètre PCI donné ne présage pas de la sécurité globale et durable de l'entreprise. Cette conformité n'est qu'une étape.

Limiter les risques et la diffusion des données des porteurs de cartes dans l'organisation présente des avantages importants. Dans le périmètre d'un environnement PCI DSS conforme, le risque de vol ou de fuite de données est limité, de même que l'ampleur de la faille si elle devait se produire. En créant des « compartiments » entre les différents réseaux internes oà[1] stocker les données sensibles, classées par catégories, on réduit nettement la probabilité qu'une brèche s'étende à toute l'infrastructure IT.

Une entreprise qui réduit ses risques avec PCI peut devenir plus efficace, mais ça ne signifie pas qu'une fois qu'elle est conforme elle peut négliger ses autres contrôles de sécurité ! Le fait de mieux intégrer la gestion et la mesure du Risque ne doit pas dispenser les entreprises des contrôles requis mais doit les amener au contraire à mieux appréhender la pertinence et la quête d'efficacité du standard PCI DSS.

En un mot, installer des contrôles ne suffit pas à garantir la sécurité d'une entreprise, et se contenter du minimum, c'est s'exposer à de graves dangers. Quand l'infraction sera avérée, avoir coché trop rapidement les cases d'une checklist de conformité ne vous sera pas d'un grand réconfort.