Sécurité monétique :
ces mesures à ne pas négliger

Face aux exigences légitimes des clients et à la nécessité de maîtriser les risques, les systèmes de paiement évoluent constamment grâce aux technologies, mais se complexifient aussi en fonction des règlementations et des menaces.

Fraudes à la facture, usurpation de comptes commerçants, utilisation de systèmes d'acceptation non légitimes… les risques monétiques sont nombreux et leurs conséquences peuvent s'avérer importantes pour les commerçants comme pour les banques.
Une chose est sûre, pour éviter les failles, il est nécessaire d'investir dans la sécurité. Cette sécurité à un prix mais la négliger peut coûter encore plus cher, tant d'un point de vue financier qu'en termes d'image, de notoriété, et de confiance.

Cet investissement se fait généralement au travers des passerellistes monétiques dont la mission majeure est de garantir un haut niveau de sécurité. Ces derniers se doivent de respecter plusieurs principes incontournables, en voici quelques exemples.

La certification PCI DSS, le prérequis majeur

Pour traiter et conserver des données bancaires en toute sécurité, la certification PCI DSS, c'est la base !
Elle permet d'assurer que les données cartes bancaires qui transitent par le passerelliste, sont correctement sécurisées, quel que soit le contexte de paiement (proximité, e-commerce ou automate…). Personne ne doit pouvoir accéder à ces données. Leur cryptage est impératif et ce, de bout en bout de la transaction, pour éviter leur circulation en clair sur les réseaux.
Aujourd'hui, certains acteurs exercent sans être certifiés PCI DSS, faisant courir des risques majeurs à leurs clients. D'autres créent une ambiguïté en utilisant des clouds. Même si ces espaces de stockage sont certifiés PCI DSS, l'acteur se doit de certifier également la solution tel que mentionné dans les clauses des acteurs clouds. En effet, il arrive forcément un moment où les informations transitent sur des serveurs, sur des passerelles, avant d'être stockées dans le cloud. Il suffit alors que ces données ne soient pas cryptées pour être récupérées par des pirates positionnés entre le passerelliste et le lieu de stockage. Imaginez les conséquences.

La double authentification, l'atout clé pour tracer les flux

Aujourd'hui, un terminal de paiement classique fait de la simple authentification, c'est-à-dire qu'avant de faire une demande d'autorisation par exemple, il va s'assurer au travers de l'infrastructure de son passerelliste que l'acquéreur (banque du commerçant) est dûment identifié comme autorité de confiance.
Dans le cas d'une double authentification, l'infrastructure du passerelliste va en complément s'assurer que le terminal de paiement qui se connecte est bien légitime pour le faire.
Obligatoire pour les opérations de Transfert de Fonds par carte CB dans le cadre d'une conformité TRACFIN (lutte contre les circuits financiers clandestins, le blanchiment d'argent et le financement du terrorisme), cette double authentification ne l'est pas pour les paiements de proximité en France, contrairement à d'autres pays européens. C'est pourtant une garantie de sécurité importante qui permet la traçabilité des flux, recommandée d'ailleurs par l'ANSSI, l'autorité nationale en matière de sécurité et de défense des systèmes d'information.
Là aussi, la double authentification représente un investissement. Mais pour une banque ou un grand commerçant dont le nom se retrouverait associé au blanchiment d'argent, les répercussions pourraient être catastrophiques !

Réseaux sécurisés et sites redondés

Pour une sécurité accrue, il est important que le passerelliste dispose de liens privés, dédiés à sa plateforme monétique et reliant ses datacenters aux différentes banques acquéreurs. Ces réseaux privés garantissent le transit exclusif des données monétiques. Autre avantage, ils permettent aussi de limiter les intermédiaires et donc les zones de risques sécuritaires.
En complément de ces liens, le fait de travailler avec plusieurs opérateurs internet renforce également la sécurisation des données : si l'un des opérateurs est la cible d'une cyberattaque, un autre peut prendre le relais. Idem avec une infrastructure redondée sur plusieurs sites, qui garantit quotidiennement une continuité de service.
Pour cela, il faut se doter de solutions techniques performantes, mettre les moyens à la hauteur des enjeux et limiter les intermédiaires dans la chaine de liaison en maîtrisant toutes les briques informatiques nécessaires.

On en revient donc comme toujours au coût de la sécurité, qui plus est dans une compétition où nombre d'acteurs jouent sur les ambiguïtés pas toujours simples à décrypter pour l'utilisateur de ces solutions. S'il peut paraître élevé et dissuader certains acteurs, ce coût est à mettre dans la balance avec l'impact que pourrait avoir une faille de sécurité. Faut-il attendre une catastrophe pour comprendre l'importance et le prix de la sécurité ?

Par Anton Bielakoff, Directeur Général de Lyra