

## Des technologies plus puissantes pour endiguer la fraude

**Conduit par Angelo Caci, du cabinet ADN'Co, l'atelier de Payforum 2011 consacré à la sécurité des paiements et à la lutte contre la fraude, a démontré qu'aujourd'hui, l'industrie des paiements se mobilise afin de lutter contre la fraude sous toutes ses formes. Un sujet difficile qui exige une remise à niveau permanente des infrastructures de protection... et une bonne dose d'imagination.**

*"Lutter contre la fraude constitue aujourd'hui un véritable engagement pour tous les acteurs de la vie économique, des banques aux entreprises en passant par les commerçants et face aux actions des fraudeurs, il faut pouvoir rivaliser d'ingéniosité et d'innovation",* affirme d'emblée Angelo Caci, directeur délégué du cabinet ADN'Co. Prenant la parole, Guy de Felcourt, directeur de CPP France, société d'origine britannique qui a développé une expertise pour aider les particuliers à faire face aux risques engendrés par la vie moderne (cartes de crédit, identité et fraude sur Internet...), assène

quelques chiffres: *"On dénombre plus de 600 millions de 'Facebookiens' dont beaucoup se retrouvent, un jour ou l'autre, dans le collimateur des fraudeurs, au sens large, alors que par ailleurs, on recense quelque 50.000 variétés de codes malicieux tous les mois. Parallèlement, on peut estimer que 25 % des cartes bancaires ont été ou seront fraudées, un jour ou l'autre, et ce à l'échelle de la planète".* Des chiffres qui ont le mérite de faire réfléchir et de montrer l'ampleur des problèmes liés à la sécurité des paiements et la lutte contre la fraude.

Face à ces multiples risques, CPP France a mis au point un système original de contrôle du niveau de sécurité pour les individus. Au travers d'une interface web, une personne peut contrôler le degré d'exposition de ses données sur Internet. Les principaux paramètres sont pris en compte: nom, adresse, adresse de messagerie, pseudo, date

de naissance, numéro de passeport, numéro d'identifiant pour prestations sociales, numéro de cartes de paiement. A partir d'un système d'interrogation, l'utilisateur peut ainsi savoir si son patronyme, par exemple, a été victime de menées frauduleuses. Ensuite, il peut prendre les dispositions qui s'imposent, par exemple changer d'identifiant, pour accéder à telle ou telle application.

*"Plusieurs banques et des opérateurs de téléphonie proposent ce service à leurs clients, ce qui, pour ces entreprises, est une façon de renforcer la qualité de la confiance et le relationnel client",* ajoute

Guy de Felcourt. En règle générale, le service est facturé environ 6 euros par mois à l'utilisateur final. Et manifestement, la formule a trouvé son public car la base CPP compte plus de 2 millions d'adhérents.



Guy de Felcourt, CPP France

### Solution de protection comme un service

Dans la sécurité des paiements, le concept SaaS (Software as a Service) se développe. Ainsi, Léon-Charles Hottier, Directeur Alliances Stratégiques chez Ogone explique: *"Les entreprises recherchent des solutions de protection, par exemple, des infrastructures de cryptographie qui soient accessibles en mode service et capables de conjuguer différentes approches."* Autrement dit, les solutions de prévention de



Léon-Charles Hottier, Ogone



la fraude doivent s'appuyer sur un véritable "panel de solutions", permettant de gérer de manière homogène l'authentification forte, l'analyse comportementale, l'aide à la décision, la géolocalisation, l'ouverture à des bases de données et d'autres fonctions encore.

"Aujourd'hui, de nombreux outils de limitation du risque sont mis à la disposition des sites, poursuit Léon-Charles Hottier, qu'il s'agisse de contrôle manuel ou automatisé, d'outils de scoring ou encore de 3D Secure, l'essentiel étant que chaque commerçant mette en place la bonne combinaison d'outils." Concernant spécifiquement 3D Secure, Léon-Charles Hottier admet que "3D Secure présente aujourd'hui encore, le défaut de ne pas être maîtrisé par tous les utilisateurs sur Internet ce qui interdit l'achat à un grand nombre de personnes." Selon lui, les banques doivent donc continuer de "former les utilisateurs". On le croit sans peine.

## La qualité de cryptage des données, un point essentiel

S'exprimant face à l'auditoire dans la langue de Shakespeare, Mike Bond, directeur sécurité de Cryptomatic développe à sa manière les propos du responsable d'Orgone en évoquant la nécessité de "mutualiser les ressources technologiques de protection et de lutte en déployant un portail complet qui joue le rôle de pivot central et de supervision dans la gestion des processus de détection et de lutte contre la fraude."

En l'occurrence, il s'agit du portail dit HSM (Hardware Security Modules). "Les modules existants sont souvent coûteux à développer et à maintenir, déclare-t-il encore. Le principe général est de mettre en place un serveur unique pouvant gérer aussi bien les ouvertures de session que l'administration des procédures d'authentification forte lors d'une transaction." Il insiste sur un autre aspect, essentiel à ses yeux: "Pour lutter efficacement contre la fraude, il faut pouvoir pister les flux de données et déterminer comment



Mike Bond, Cryptomatic



Guillaume Forget, Cryptomatic



Thierry le Forban, Monext

ces données ont été cryptées. Bien souvent, on s'aperçoit que des données deviennent fragiles du seul fait que le processus de cryptage était insuffisant abouti."

## Assurer des services 24/24

Regrouper les forces, mutualiser les compétences technologiques et le savoir faire métier, tel est, en substance, le message véhiculé par Thierry le Forban, consultant avant-vente chez Monext. Preuve à l'appui : "Notre offre couvre l'essentiel du périmètre de la lutte contre la fraude avec un système couplant prévention, détection et traitement des alertes. Mais pour amplifier nos possibilités d'intervention, nous nous sommes alliés à Isoft une société qui maîtrise les calculs statistiques et dispose à ce titre d'une forte expertise dans le scoring, ce qui est très utile lorsqu'il s'agit de mettre en place des systèmes de traitement des alertes."

A ce sujet, il précise : "Les entreprises manquent de moyens techniques et humains c'est pourquoi nous leur apportons un accompagnement personnalisé grâce à une cellule dédiée. Les traitements des alertes doit être évidemment traité 24/24 et 7/7." Thierry le Forban ajoute que 40 % de la fraude a lieu le week end. "Nous savons par expérience qu'il ne faut jamais baisser la garde", conclut-il. ■

Gilles PROD'HOMME

## Les données d'identification les plus ciblées par les fraudeurs

- ▶ Numéros de cartes de paiement
- ▶ Numéros de comptes bancaires
- ▶ Numéro de sécurité sociale
- ▶ Numéros des documents d'identité
- ▶ Identifiants mots de passe sur Internet
- ▶ Numéros téléphones mobiles

Source : CPP France