Sécuriser la banque sur Internet par une approche collaborative

GAËL BARREZ
Responsable des solutions anti-fraude RSA, La Division Sécurité d'EMC

Jamais le secteur des services financiers n'aura été confronté à une menace technologique aussi bien organisée et sophistiquée que la fraude en ligne. La fraude sur Internet est devenue un véritable marché de plusieurs millions d'euros. Ce n'est plus l'apanage de jeunes surdoués de l'informatique en mal de célébrité ! Aujourd'hui les pirates négocient, sur de véritables « marchés noirs virtuels », des outils technologiques sophistiqués, afin d'industrialiser leurs pratiques frauduleuses.

Au cours des trois dernières années, le *phishing* (ou « hameçonnage ») est devenu la principale arme de fraude en ligne. Les pirates utilisent des systèmes d'ingénierie sociale de plus en plus sophistiqués pour duper les consommateurs. En juin 2007, l'*Anti-Phishing Working Group*[1] recensait 28 888 attaques de *phishing* dans le monde. Pour les banques, il s'agit aujourd'hui de réduire la fraude en ligne et, surtout, de conserver la confiance de leurs clients. Leur capacité à sécuriser l'accès à leurs ressources conditionne la pérennité des accès aux services de banque en ligne.

Une prioritée : le partage des informations

Les établissements financiers ont conscience qu'Internet joue un rôle majeur et croissant dans leur stratégie de distribution de services. Ils souhaitent même amplifier cette tendance en faisant migrer de nouvelles transactions sur le web et en développant leurs sources de revenus en ligne. Cependant, cet essor exige d'apporter des réponses cohérentes aux préoccupations de sécurité des utilisateurs.

Si les établissements n'y parviennent pas, leurs coûts augmenteront. Selon une estimation faite en Grande-Bretagne, l'indisponibilité – pour des raisons de sécurité ou de fraude potentielle – de 10 % des transactions conduites sur Internet vers le téléphone représenterait une augmentation des coûts opérationnels des banques britanniques de 9 millions de livres sterling (soit environ 13,3 millions d'euros) !

Selon une étude réalisée par Infosurv[2] en décembre 2006, 82 % des titulaires de comptes attendent de leur banque qu'elle assure une surveillance de leurs transactions en ligne et par téléphone afin de détecter des signes d'activité ou de comportement anormaux – comme cela existe déjà pour les transactions par carte de crédit. Et 69 % des titulaires de comptes pensent que les établissements financiers devraient remplacer la connexion par identifiant/mot de passe par un système d'authentification renforcé pour leurs opérations bancaires en ligne. Ces chiffres

1. L'*Anti-Phishing Working Group* est une association d'entreprises visant à lutter contre la fraude et le vol de données personnelles sur Internet (*phishing*, *pharming*...) - www.antiphishing.org.

2. Source : 4th Annual Consumer Online Fraud Survey (RSA - Jan. 2007).

« 82 % des titulaires de comptes attendent de leur banque qu'elle assure une surveillance de leurs transactions en ligne et par téléphone afin de détecter des signes d'activité ou de comportement anormaux. »

poussent de nombreux établissements financiers à faire du partage des informations une priorité. Cela exige la construction de relations de confiance entre ces différents acteurs pour assurer une véritable supervision des transactions.

Maximiser la protection collective

Les communautés de lutte collaborative contre la fraude jouent aujourd'hui un rôle essentiel pour aider de multiples institutions financières à contrôler les menaces émergentes et à maximiser la protection collective de tous les participants.

De tels réseaux permettent en effet de mutualiser les observations issues des établissements financiers afin d'identifier les profils et les modes d'action des fraudeurs pouvant s'attaquer à plusieurs établissements bancaires. Les données sur la fraude sont alors partagées en temps réel et, dès qu'une attaque est identifiée sur le réseau d'un des membres, tous les autres membres sont protégés. Aujourd'hui, les principales banques dans le monde (Bank of America, Credit Suisse, LCL, HBOS, ING Direct, Alliance and Leicester ou Washington Mutual) bénéficient d'une protection grâce à l'utilisation de technologies de détection des fraudes. Le réseau RSA eFraudNetwork protège ainsi plus de 500 millions de consommateurs dans le monde, en temps réel. Il s'agit de la première communauté bancaire mondiale de lutte collaborative contre la fraude. La mise en œuvre de fonctionnalités de détection, d'alerte et de blocage a permis de fermer plus de 32 000 sites web de *phishing* et de réduire la durée de vie moyenne des attaques de *phishing* de 115 heures à seulement 5 heures.

Il existe une corrélation directe entre le volume des attaques de *phishing* et le montant des pertes liées aux fraudes en ligne. Les banques ont tout intérêt à réduire le nombre d'attaques pour améliorer le niveau de confiance – qui conditionne directement l'accroissement du nombre

Glossaire

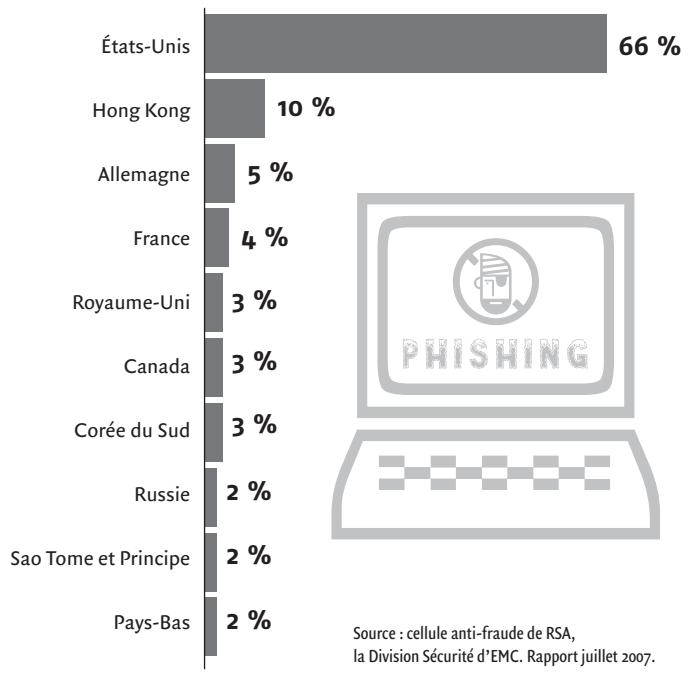
■ **Le *phishing*.** Forme d'usurpation d'identité par laquelle, un pirate utilise un e-mail d'allure authentique afin de tromper son destinataire pour que ce dernier donne de manière consentante ses données personnelles, telles qu'un numéro de carte de crédit, de compte bancaire ou de sécurité sociale.

■ **Le *pharming*.** Installer un site factice contenant des copies de pages d'un site officiel dans le but de recueillir des informations confidentielles sur les utilisateurs du site officiel. En piratant les serveurs DNS (*Domain Name Server*) et en changeant les adresses IP, les utilisateurs sont dirigés automatiquement sur des sites fictifs.

■ **Un cheval de Troie.** Programme apparemment sans danger contenant un code malveillant qui permet la récupération, la falsification ou la destruction de données.

Source : Rapport mensuel sur la fraude en ligne – Juillet 2007, RSA – Division Sécurité d'EMC.

Principaux pays hébergeant des sites de phishing



Source : cellule anti-fraude de RSA, la Division Sécurité d'EMC. Rapport juillet 2007.

La cellule anti-fraude de RSA, basée en Israël, travaille 24h/24 pour neutraliser les attaques de *phishing*.

de clients. En outre, les fraudeurs potentiels s'attaquent moins volontiers aux établissements qu'ils savent bien protégés contre le *phishing* pour leur préférer des victimes plus faciles à pirater.

Redonner confiance aux clients, un impératif économique

Les effets induits par la fraude en ligne sont considérables. Selon le Gartner, environ 15 millions d'Américains auraient été victimes de vols de leurs données personnelles sur Internet entre juillet 2005 et juin 2006 et la perte moyenne par victime s'élevait à 3 257 dollars. Ramené à 15 millions d'individus, ce seraient plus de 48 milliards de dollars qui auraient été détournés par des cyber-criminels. Ces données démontrent sans conteste que la collaboration, l'authentification, l'intégration de nouvelles technologies de sécurisation des transactions et la formation des utilisateurs à des pratiques de sécurité actives sont les seuls remèdes pour déjouer des attaques de *phishing* et développer de nouveaux avantages concurrentiels pour les banques.

Certes, cette collaboration existe déjà à certains niveaux en France. Les banques savent échanger des informations quand cela s'avère nécessaire (tentatives de cavalerie, fraudes au chèque…). Cependant, ces échanges seront plus complexes, voire très difficiles à mettre en œuvre en raison de la mutation du secteur bancaire : fusions, acquisitions, changements du cadre législatif et réglementaire.

Le 1er janvier 2008, un nouvel environnement bancaire va officiellement voir le jour : le SEPA (ou *Single European Payments Area*). Il s'agit d'un espace européen à l'intérieur duquel tous les acteurs économiques seront dotés de moyens de paiement scripturaux communs, permettant de réaliser, dans des conditions identiques (facilité, vitesse, sécurité), des transactions de paiement en euro. Comment feront les banques de la place lorsqu'elles souhaiteront collaborer avec une banque au fin fond de la Pologne ? Est-ce que nos banquiers vont devoir apprendre le Polonais ? Dans ce cas, la technologie sera une réponse plus efficace et plus simple à mettre en œuvre.

> *« La collaboration, l'authentification, l'intégration de nouvelles technologies de sécurisation et la formation des utilisateurs sont les seuls remèdes pour déjouer des attaques de phishing. »*

Redonner confiance aux clients dans la sécurité de leurs services bancaires en ligne est un impératif économique pour tous les établissements financiers qui souhaitent les fidéliser. La collaboration offre ainsi aux banques un moyen efficace de réduire la fraude en ligne, en s'appuyant sur un réseau de détection partagé avec leurs pairs au niveau européen et international. Plus les établissements bancaires adopteront cette approche collaborative, plus ce système de protection sera efficace. ■