INTERVIEW

"Le phishing contre les banques en France reste marginal"

Bernard Michel

Directeur
fonctionnement
et logistique
Comité exécutif
Crédit agricole

Les banques françaises sont plus préoccupées des attaques par phishing que leurs clients subissent, que par celles aujourd'hui marginales qui les visent directement.

■ Peut-on mesurer aujourd'hui les effets des attaques de phishing sur les banques françaises, et précisément chez vous, au Crédit agricole ?

Au Crédit agricole, et vraisemblablement pour l'ensemble des banques françaises, les attaques par *phishing* restent marginales pour ne pas dire inexistantes, que ce soit au niveau des plaintes ou au niveau des pertes financières. Les attaques que nous traitons actuellement relèvent majoritairement de l'intrusion dans les postes de travail de nos clients par des programmes espions (*spyware* et *keyloggers*) qui permettent de récupérer les données personnelles présentes sur ces postes ou saisies sur le clavier.

■ Quels sont les moyens de lutte qu'il vous semble important de privilégier ?

Sur le plan général de la sécurité de la banque en ligne, la coordination et la concertation interbancaires sont indispensables pour aboutir à des dispositions communes, et à des dispositifs d'alerte rapides. C'est ainsi que les travaux des banques, au sein du CFONB, en collaboration avec la Banque de France, ont abouti à un référentiel de mesures et de pratiques qui permettront d'améliorer le niveau de sécurité de la banque en ligne. Il s'agit du profil de protection qui a été récemment certifié par la DCSSI (Direction centrale de la sécurité des systèmes d'information). La collaboration se fait aussi avec les services spécialisés du ministère de l'Intérieur et du ministère de l'Économie, des Finances et de l'Industrie.

■ Et vis-à-vis de vos clients ?

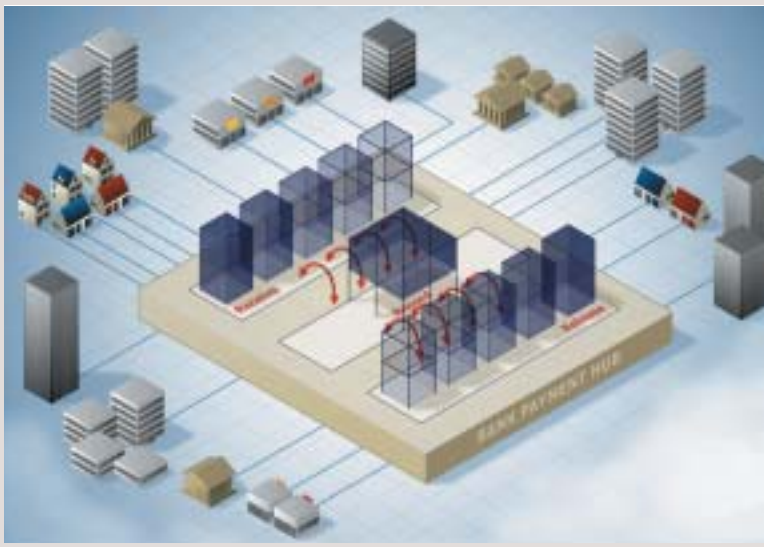
Le problème est en premier lieu celui de l'authentification du client quand il accède à la banque en ligne. Et il faut aussi souligner que la sécurité est un processus dynamique. Les solutions à mettre en place peuvent parfois se révéler antinomiques. Le client exige, par exemple, une ergonomie facile. Il veut prolonger au niveau de la banque en ligne des habitudes de consommation liées à la navigation sur l'internet, mais qui augmentent le risque et occultent les contraintes de sécurité de son poste de travail. Or notre mode opératoire est complexe précisément à cause des exigences de sécurité relatives à la banque en ligne. Et il a un coût. Quoi qu'il en soit, nous disposons déjà d'une panoplie de moyens techniques destinés à compliquer l'action des éventuels attaquants. Nous développons l'information vers nos clients pour qu'ils protègent leurs identifiants, changent fréquemment leurs mots de passe, signalent les anomalies et protègent leur poste de travail.

■ Vos programmes e-Badge et CA certificat vous paraissent-ils s'inscrire dans un mouvement général favorable aux solutions d'authentification fortes ou restent-ils spécifiques à votre groupe ?

Les programmes e-Badge et CA certificat sont des programmes CA spécifiques élaborés par le Crédit agricole, liés à des problématiques particulières : offres ciblées en direction d'une clientèle d'entreprise, ou accompagnant le domaine de la Télé-TVA. Au-delà de ce marché, et en attendant un déploiement de solutions renforcées d'authentification auprès du grand public, on peut imaginer que les solutions basées sur la PKI (*Public key infrastructure*) se déploieront plus rapidement sur certains segments de particuliers utilisant les services de la banque en ligne de manière intensive ou sensible. ■

Propos recueillis par Yvon Avenel

Traitement des paiements : vers une plate-forme unique mais flexible



La plate-forme permet de réutiliser des composants existants et d'en ajouter de nouveaux sans perturber le système.

■ Le centre de paiement **PayPak** annoncé par la société Clear2pay offre aux banques et aux fournisseurs d'infrastructure de marché une voie de migration vers une plate-forme de paiement unique. Bâtie sur une architecture J2EE (Java), cette plate-forme très orientée services utilise un moteur (Business processes engine) qui distribue les tâches à des composants sous-jacents au système, et rend ces derniers indépendants des processus fonctionnels proprement dits. Un avantage qui permet de réutiliser des composants existants et d'en ajouter de nouveaux sans perturber le système. Ce dernier peut, du coup, s'adapter au plus vite à l'évolution de la réglementation et de l'offre commerciale associée, ou encore offrir une gestion proactive des fraudes et risques liés au paiement.

Flexibilité, capacité à évoluer rapidement, optimisation des STP (*Straight through processing*) et des coûts de traitement en général... c'est une philosophie similaire qui est au cœur de l'accord conclu à l'occasion du dernier Sibos, le congrès annuel consacré à Swift, entre l'intégrateur LogicaCMG et Dovetail systems. La plate-forme de paiement de ce dernier (Q5 STP Application platform), choisie par le premier pour s'intégrer à son offre LPA (Logica payment architecture), est elle aussi bâtie sur une architecture J2EE. Elle offre en outre une interface web et une panoplie d'outils de développement et d'interfaces de façon à intégrer de nouveaux composants et à valoriser les applications existantes.

Cette plate-forme tourne dans les environnements Unix et Microsoft, et s'interface aux bases de données Oracle, DB2, ou SQL server.

Protéger les distributeurs de billets contre les vers internet

■ La généralisation des réseaux TCP-IP et leur déploiement pour connecter des distributeurs de billets, des terminaux de paiement ou des kiosques de self-service a une contrepartie : une vulnérabilité de ces appareils et de leurs équipements de communication aux virus, et en particuliers aux "vers internet". En 2003, le ver SQL Spammer avait ainsi bloqué les retraits d'argent sur le réseau de distributeurs de billets d'une banque américaine. Dans bon nombre de cas, ces vers qui s'installent sur les machines du réseau n'utilisent ce dernier que pour se reproduire et générer une surcharge d'activité qui dégrade vite la qualité des services proposés par ces machines. Depuis quelque mois, Trend Micro, l'un des plus importants éditeurs de logiciels de sécurité, propose une solution pour résoudre ce problème. Il s'agit d'un boîtier autonome (**Network VirusWall 300**) qui se connecte sur tout type de réseau IP et permet d'en contrôler le trafic (analyse des paquets IP), voire, le cas échéant, de détruire les trames infectées. Ce boîtier est relié à une console d'administration. La détection est basée sur une analyse de la signature logique des vers.

Les services de paiement sans fil GPRS se développent

■ **Transactions network services (TNS)** a conclu à la fin de l'année 2004 des accords avec les principaux opérateurs de téléphonie mobile en Europe, de façon à pouvoir offrir des services GPRS dans cinq pays européens. Ces services seront accessibles aux terminaux de paiement équipés de modules GPRS et de cartes SIM, fournies par TNS ou ses partenaires. CardPoint, par exemple, l'un des principaux gestionnaires indépendants de distributeurs de billets au Royaume-Uni, a pu augmenter son réseau de 3 000 automates et en placer sur des sites de manifestations et de festivals en plein air jusque-là inaccessibles à ce type de services. Le réseau privé de TNS sert d'interface entre les terminaux et les banques. En particulier, il convertit les données transactionnelles nativement organisées en trames en IP sur les terminaux, au format X25 utilisé encore par la plupart des serveurs bancaires.

La lutte contre la fraude gagne en précision

■ Huit fois moins de fausses alertes… et trois fois et demi plus performant ! C'est, selon Visa, le diagnostic établi par les banques qui ont remplacé, depuis le début de l'année 2004, CRIS (Card risk identification service) par Visor (Visa intelligent scoring of risk). Depuis son adoption par quelque 80 banques en Europe, plus de 3,5 millions de transactions ont été identifiées comme des tentatives de fraude sur une période d'observation de 130 jours. **Visor** utilise un moteur à base de réseaux de neurones (système expert avec autoapprentissage, reconnaissance de formes) qui établit des scores à partir d'une analyse de chacun des comportements combinés des porteurs de cartes et des marchands. Ces analyses sont effectuées à partir de 240 paramètres comme l'heure et la date de la transaction, le pays où elle est réalisée, etc. Le logiciel est capable d'analyser ainsi jusqu'à environ 300 000 transactions à l'heure.

Vers une carte de débit paneuropéenne

■ Un pas de plus vers la prise en compte du projet Single european payments area (SEPA), dont la réalisation est souhaitée par la Banque centrale européenne et l'European payment council : Visa Europe lance une carte de débit paneuropéenne baptisée **V Pay**. Il s'agit d'une carte EMV, donc utilisable avec un code confidentiel. Elle est compatible avec les systèmes nationaux de numérotation des comptes cartes (13 et 19 chiffres commençant par 4,5 ou 6), ce qui n'induira pas de coûts d'adaptation aux systèmes de traitement et aux infrastructures en place. Elle pourra être cobadgée avec des marques de systèmes domestiques durant toute la période de transition vers la carte SEPA unique.

Une carte EMV à contact et sans contact

■ MasterCard, qui a récemment franchi le cap des 200 millions de cartes à puce émises dans le monde, a annoncé l'une des premières cartes EMV offrant des moyens de réaliser des transactions rapides pour de petits montants. Baptisée **OneSmart PayPass**, cette carte à puce embarque une antenne qui lui permet de communiquer sans contact, d'un simple geste, avec un lecteur idoine selon les protocoles ISO 14443. L'application embarquée dans la carte est une implémentation de la technologie M/Chip de MasterCard, appelée à se développer dans toute une famille de cartes (et même de cartes à piste magnétique). Ce type de transaction qui a l'avantage d'être bien plus rapide que le paiement en liquide est particulièrement

adapté aux péages autoroutiers, à la restauration rapide et aux stations-service. Pour des dépenses présentant ainsi un faible risque et un faible montant, l'authentification du porteur et de la carte ne réclame ni signature ni frappe d'un code personnel. La transaction est acceptée soit on-line par l'émetteur de la carte, soit off-line par la carte elle-même.

Oberthur card systems a récemment annoncé de son côté une carte homologuée par **MasterCard, MoneytIC OneSmart PayPass**, tandis qu'**Ingenico** et **Sagem Monetel** proposent déjà des terminaux conformes à ces spécifications, et des modules sans contact permettant d'adapter les terminaux existants à cette technologie sans contact. Dans son utilisation à contact, la carte se comporte comme une carte EMV classique avec des capacités d'authentification fortes on-line et off-line, et des possibilités mutiapplicatives (fidélité notamment).

Sécuriser les transactions en ligne

■ Récompensé à la fin de l'année dernière par le Trophée de l'innovation lors du Forum européen des tiers de confiance, le service en ligne **Webank**, développé par la banque OBC (Odier Bungener Courvoisier), filiale du groupe ABN Amro, est le premier à tirer parti de la signature électronique et de son environnement légal établi depuis la loi du 13 mars 2000, complétée par son décret d'application du 30 mars 2001. L'utilisation par les entreprises clientes d'un certificat numérique X509 de classe 3 (niveau de vérification d'identité en face à face) délivré par Certinomis pour signer tous les mandats dématérialisés, assure l'authentification du signataire de la transaction, mais également l'intégrité et la non-répudiation de la transaction signée. OBC prévoit d'élargir dès cette année l'utilisation de la signature numérique pour l'appliquer à d'autres services que ceux qui sont ouverts depuis déjà dix-huit mois, afin de réaliser des ordres de virement domestiques ou étrangers, de paiement et de prélèvement.

Le téléphone mobile comme moyen de paiement

■ MasterCard, qui a déjà expérimenté avec succès à Dallas avec Nokia, AT & T Wireless et JP Morgan Chase, l'utilisation de sa technologie de paiement sans contact PayPass à partir d'un téléphone mobile, poursuit, cette fois-ci avec **Motorola**, l'exploration technique et marketing de ce nouveau moyen de paiement. Des pilotes sont en effet en préparation dans plusieurs villes des États-Unis pour utiliser des téléphones Motorola équipés de puces sans contact de type NFC (Near field communication) et réaliser des transactions pour des montants de faible valeur (moins de 20 dollars). Cette technologie basée sur l'ISO 14443 est sensiblement différente de la simple technologie PayPass, puisqu'elle permet au mobile de se comporter non seulement comme un portemonnaie électronique utilisable avec un lecteur adapté, mais aussi comme un lecteur, ce qui ouvre la voie à des applications nouvelles d'*e-ticketing* ou de fidélité, liées ou pas au paiement lui-même.

La sécurité " réseau " à 10 Gbit/s

■ **SafeNet**, l'un des premiers fournisseurs mondiaux de solutions de sécurité, propose désormais une version Sonet et SDH de ses boîtiers de chiffrement déjà conçus pour IP, ATM et Frame relay. Ces boîtiers offrent des débits de 10 Gbit/s en duplex sur des distances qui peuvent varier de 2 à 40 km. La gestion des clés est entièrement automatique, grâce à l'utilisation de certificats numériques X509.

Optimiser l'administration de la sécurité

■ La solution **ExtraProtect advanced software (EAS)** développée par la société ExtraProtect technology, spécialisée dans l'infogérance de sécurité dans le monde bancaire, a été conçue pour simplifier et optimiser l'administration de la sécurité. Elle s'adresse aussi bien aux responsables de la sécurité des systèmes d'information qu'aux directions générales. Elle vise en premier lieu à résoudre les problèmes posés par la volumétrie des données à traiter (quelques centaines d'événements à la seconde, par exemple) et leur hétérogénéité, puisque souvent issues de sources très diverses (pare-feu, antivirus, sonde de détection d'intrusions, IPS, système d'exploitation, applications, etc.). Le logiciel, qui est embarqué dans des équipements dédiés (biprocesseur Dell), agrège les formats de données différents (*logs*), puis procède à leur analyse, grâce à un moteur intelligent de corrélation baptisé Incident Care, le cœur d'expertise de la société. Les règles utilisées et les outils de filtrage fonctionnent à partir de bases de connaissance aussi bien interne qu'externe. Elles peuvent ainsi s'adapter à chaque entreprise, à chaque périmètre préalablement défini et à chaque projet de Security information management (SIM). Certaines règles de corrélation peuvent être définies par les administrateurs. Les alertes sont administrées au travers d'une console unique. ■

La "communication événementielle" enrichit la CRM

■ Les outils de CRM (*customer relationship management*) ne cessent de se perfectionner pour gagner en précision, en puissance et en réactivité. La notion de temps réel dans l'interaction devient centrale. SAS, premier éditeur mondial d'informatique décisionnelle, vient ainsi d'annoncer l'implémentation du concept de "communication événementielle" (*event trigger*) dans un outil de CRM baptisé **SAS interaction management**. Très lié aux concepts de "conversation" et de carte de comportement, cet outil se distingue des systèmes classiques de CRM basés sur l'utilisation de profils et de modèles mathématiques prédictifs portant généralement sur de larges segmentations de clientèle et des stéréotypes. Autant le profil offre une image statique toujours périmée parce que mise à jour selon des périodicités qui sont parfois mensuelles, autant la carte de comportement propose une sorte de film personnalisé dont la compréhension continue autorise des réactions en temps réel, et, du coup, des taux de réussite des messages bien plus élevés que ceux atteints par les campagnes classiques. De l'ordre de 20 % contre 3 % selon une étude du Gartner Group. Cette capacité à réagir immédiatement à un changement de comportement permet ainsi d'optimiser la détection des opportunités de vente (*cross selling*) ou des risques de fuite à la concurrence (*attrition*). SAS signale le cas d'une grande banque américaine qui, en utilisant cet outil à la place d'un traditionnel moteur de règles, a pu augmenter de 30 à 35 % la rétention de ses comptes clients. SAS interaction management est paramétrable. Il permet d'assurer toute la chaîne des opérations qui vont du suivi et de l'analyse de l'historique du comportement de chaque client, jusqu'à l'automatisation et la génération des actions marketing individualisées, en passant par la détection des changements clés de comportement, le déclenchement des alertes, l'intégration des données contextuelles toujours essentielles à la bonne compréhension des changements de comportement, et à l'élimination des "faux positifs" au niveau des alertes.