Banques : 2006, année authentification ?

Les banques européennes planchent sur les systèmes d'authentification de leurs clients.

En 2006, certaines adopteront des systèmes de mot de passe générés à chaque connexion ou à chaque transaction. Mais elles se pencheront également sur les mécanismes de prévention de la fraude, comme l'utilisation des outils d'analyse de risque en temps réel. Telles sont les conclusions du rapport daté de mars 2006 de Forrester Research. **Les raisons du choix** Pour les analystes, les choix des établissements en matière d'authentification vont être dictés par différents critères : Tout d'abord, la sophistication croissante des attaques de phishing, dont les mails sont traduits en différentes langues, et qui ne ciblent plus uniquement les établissements importants. Au regard de ce phénomène, la vulnérabilité effective des systèmes demeure un aspect essentiel de la question. Mais les établissements vont également prendre en compte le coût, la complexité des solutions à mettre en place, la tendance ou pas du consommateur à accepter certaines contraintes, et la cohérence des solutions avec l'image de la banque. Par exemple, un établissement qui se veut à la pointe sera tenté d'adopter les solutions les plus « high tech » du moment. **Double authentification** Pour l'essentiel, c'est la méthode d'authentification basée sur la génération de mots de passe dynamiques, ou une signature digitale, qui convainc les établissements, signalent les analystes. Avec un débat sur le moment opportun pour mener l'opération : lors de la connexion, de la transaction, à chacune de ces deux étapes ? L'attitude du client pèsera lourd, lorsqu'il s'agira de trancher. **Pas à pas** En tout cas, d'après les distributeurs de solutions d'authentification, expose l'étude, si les banques se préparent à renforcer leur système d'authentification, c'est sans hâte. Certaines ne prévoient pas d'agir avant 2007. D'aucunes adoptent une stratégie par étapes. Par exemple, elles offriront des solutions avancées, comme un outil de génération de mot de passe à la volée, à une sélection seulement de leurs clients. Pour un investissement limité, cette option permet d'expérimenter ces outils. Avec l'inconvénient toutefois de devoir gérer la complexité de la gestion de différents systèmes d'authentification en parallèle. **Surveillance globale** Au delà de l'authentification, soulignent les analystes, les banques vont revoir leurs règles de surveillance et de détection de la fraude. Aujourd'hui, certains établissements se révèlent incapables de repérer l'adresse IP du client qui se connecte. Mais d'autres ont déjà commencé à mettre en place des solutions, ou à faire appel à des services anti-phishing. Mieux, les plus avancés se préparent à proposer à leurs clients de personnaliser les règles de sécurité appliquées à leur compte, par exemple en fixant un plafond pour les transferts internationaux.