Prestations bancaires et financières en ligne : vers un référentiel de sécurité

Conformément aux recommandations du Livre Blanc, la profession bancaire élabore un référentiel de sécurité des sites financiers de transactions, appelé profil de protection. Ces normes vont s'inscrire dans un cadre international.

JEAN-LOUIS FORT
Secrétaire général
Commission bancaire

Le Livre blanc de la Banque de France et du secrétariat général de la Commission «Internet, quelles conséquences prudentielles ?» présenté par le Gouverneur en janvier dernier, est un recueil de bonnes pratiques [1]. Conçu en collaboration avec des représentants de la profession, il est également source de propositions.

En matière de sécurité, une des recommandations essentielles qu'il formule est la définition au sein du Comité français d'organisation et de normalisation bancaire (CFONB) d'un référentiel de sécurité des sites financiers transactionnels, appelé «profil de protection». Il s'agit d'une initiative importante, visant à élever le niveau de sécurité des systèmes d'information et des transactions sur internet, et je me félicite de l'état d'avancement des travaux, auxquels sont associés depuis le mois de juillet la profession réunie au sein du CFONB, le Conseil des marchés financiers, la Banque de France et la Commission bancaire assistés d'une société de service, sélectionnée à l'issue d'une procédure d'appel d'offre.

«Les enquêtes sur place menées par la Commission bancaire, s'agissant des courtiers en ligne, ont montré diverses insuffisances dans les dispositifs de sécurité.»

LES TROIS VOCATIONS DU PROJET DE «PROFIL DE PROTECTION» DÉFINI AU SEIN DU CFONB

Un «profil de protection» est un référentiel de sécurité de nature fonctionnelle, fondé sur l'analyse des menaces qui peuvent porter atteinte aux clients et au service. Conçu pour être reconnu au niveau international, il peut être utilisé aussi bien à titre de référentiel de contrôle interne que comme support d'une évaluation menée par une société externe ou par un laboratoire spécialisé d'évaluation de la sécurité.

1. Élever le niveau de sécurité au niveau de chaque établissement

Les menaces sont nombreuses : l'atteinte à la vie privée des clients, l'usurpation d'identité d'un utilisateur, la répudiation des transactions, la perte d'intégrité des flux d'information, l'indisponibilité des systèmes, les risques d'intrusion, le risque de détournement de sites… Elles appellent une réponse adaptée de chaque établissement. Telle est la vocation première du référentiel de sécurité. Les enquêtes sur place menées par la Commission bancaire ainsi que les audits menés pour le compte du Conseil des marchés financiers [2], s'agissant des courtiers en ligne, ont en effet montré diverses insuffisances dans les dispositifs de sécurité.

2. Promouvoir l'appropriation des meilleures pratiques au niveau de la place

Au niveau de la place dans son ensemble, la définition d'un «profil de protection» vise à promouvoir un niveau satisfaisant de sécurité des sites web financiers transactionnels, car un établissement n'offrant pas de bonnes garanties de sécurité court un risque pour lui-même et fait courir un risque d'image à la communauté bancaire et financière. Il n'existe pourtant pas actuellement de référentiel pour mener à bien une évaluation de la sécurité des sites transactionnels bancaires et financiers, alors même que les établissements sont de plus en plus nombreux à faire appel à des sociétés externes pour auditer et évaluer leurs systèmes.

Le profil de protection n'a pas vocation à être sanctionné réglementairement : certes, une évaluation de la sécurité des systèmes d'information des établissements de la place conformément à ce référentiel s'inscrit pleinement dans le cadre de l'article 14 du Règlement n° 97-02 du Comité de la réglementation bancaire et financière relative au contrôle interne, qui dispose notamment que «*le niveau de sécurité des systèmes d'information est périodiquement apprécié*». L'évaluation selon ce référentiel ne constituera qu'un élément complémentaire intégré au dispositif global de sécurité, lequel doit rester, bien entendu, sous l'entière maîtrise de la direction générale des établissements, chargés de déterminer le niveau de sécurité jugé souhaitable par rapport aux exigences de leurs métiers. Cependant, une évaluation par un laboratoire spécialisé et reconnu peut apporter une garantie supplémentaire s'agissant de la partie technique du référentiel.

«Une réponse possible aux inquiétudes des consommateurs réside dans une labellisation de la sécurité des sites concernés.»

3. Accroître la confiance des consommateurs

Le développement des services bancaires et financiers sur internet, porteur de nombreuses opportunités pour les établissements, suppose une plus grande confiance des consommateurs dans ce nouveau canal de distribution. Une réponse possible aux inquiétudes des consommateurs réside dans une labellisation de la sécurité des sites

concernés. Des réflexions supplémentaires devraient être menées afin de permettre une graduation des labels selon les exigences de sécurité couvertes. A cette fin, le Livre Blanc recommande aux organisations professionnelles de se prononcer sur ce sujet.

UNE PRÉOCCUPATION PARTAGÉE PAR TOUS LES SUPERVISEURS BANCAIRES

De nombreuses initiatives se sont développées visant à élever le niveau de sécurité des services bancaires et financiers sur internet.

■ Les initiatives internationales

Le Comité de Bâle a publié un certain nombre de recommandations relatives à la maîtrise des risques des banques électroniques [3]. Ces recommandations portent sur le contrôle interne des activités des banques électroniques, sur la sécurité de ces activités et sur la maîtrise des risques juridiques et de réputation. Un certain nombre d'établissements de la place, ainsi que des sociétés de services, avaient été associés à ce travail du groupe Electronic Banking du Comité de Bâle.

«Le développement des opérations transfrontalières en ligne sera facilité par la conformité de ces services à des normes internationalement reconnues en matière de sécurité.»

■ Les initiatives à l'étranger

La Bundesbank et le Bundesaufsichtamt für das Kreditwesen, le superviseur bancaire allemand, ont mandaté l'organisme en charge de la sécurité des systèmes d'information [4] (le BSI), en janvier dernier, pour mener des inspections conjointes de l'activité internet dans les grands établissements allemands.

Aux Etats-Unis, les superviseurs bancaires participent avec la profession à la définition de référentiels de sécurité. Le projet est développé par le Banking Industry Technology Secretariat (BITS) qui offre des recommandations en matière de sécurité des sites agrégateurs [5] ainsi que plusieurs types de profils de protection.

Les autorités financières britanniques viennent de lancer le débat sur la place de Londres [6].

La communauté des superviseurs partage la même analyse : la définition par l'industrie de référentiels de sécurité flexibles et fondés sur une analyse des risques doit être encouragée. L'initiative française s'inscrit dans cette logique : le profil de protection revêt un caractère souple et s'adapte aux différentes technologies utilisées. Il ne s'agit pas d'une obligation réglementaire mais d'une démarche d'autorégulation des établissements de crédit et des entreprises d'investissement.

L'INTÉRET DES «CRITERES COMMUNS» DANS LA DÉFINITION D'UN RÉFÉRENTIEL DE SÉCURITÉ

La définition d'un référentiel de sécurité doit s'inscrire dans le cadre des «Critères communs» [7], déjà largement utilisés et reconnus au plan international. De nombreux profils de protection [8] existent déjà et l'utilisation des critères communs est en plein développement, encouragée notamment par la Commission européenne. En outre, la Banque centrale européenne procède actuellement à une analyse des objectifs de sécurité des transactions sur internet et de la monnaie électronique.

La nature transfrontalière des services bancaires et financiers en ligne plaide en faveur de ce référentiel fonctionnel, qui permet d'évaluer la sécurité à partir de critères internationalement reconnus. Si les opérations transfrontalières en ligne sont actuellement peu nombreuses, leur développement à l'avenir sera grandement facilité par la conformité de ces services à des normes internationalement reconnues en matière de sécurité. ●

[1] Disponible sur le site de la Banque de France www.banque-france.fr
[2] Une synthèse des résultats de cette enquête a été publiée par le CMF, «Contrôle de la réception d'ordres par internet», *revue CMF*, n° 35, février 2001.
[3] Risk management principles for electronic banking, mai 2001, disponible sur le site de la Banque des règlements internationaux, www.bis.org.
[4] Bundesamt für Sicherheit in der Informationstechnik.
[5] BITS voluntary guidelines for aggregation services, avril 2001 en consultation sur www.bitsinfo.org.
[6] The FSA's approach to the regulation of e-commerce, Discussion paper, juin 2001, disponible sur le site du FSA, www.fsa.gov.uk
[7] Il s'agit de la norme ISO 15408. Dans les pays parties aux Critères communs, une autorité publique (en France la Direction centrale de la sécurité des systèmes d'information (DCSSI) dépendant des services du Premier ministre) est chargée de présider à la certification sur des bases communes. 14 pays sont parties aux Critères communs et connaissent le même schéma d'évaluation : Allemagne, Australie, Nouvelle-Zélande, Canada, Espagne, Etats-Unis, Finlande, France, Grèce, Italie, Pays-Bas, Norvège, Royaume-Uni et Suède. Dans chacun de ces pays existe une structure semblable à la DCSSI : Allemagne (BSI), Royaume-Uni (CESG), Australie (DSD), Canada (CSE), Etats-Unis (NIST/NSA)…
[8] A titre d'exemple, il existe des profils de protection pour le porte-monnaie électronique, les lecteurs transactionnels avec carte à puce, les DAB, les firewalls à exigences élevées et réduites…