Marc Andries

Chef du service de la surveillance des moyens de paiements scripturaux
Banque de France

BANQUE EN LIGNE

“Nous souhaitons voir l’usage des mots de passe non rejouables se généraliser”

La Banque de France a défini des objectifs de sécurité pour le paiement sur Internet, qui valent aussi pour la banque et la Bourse en ligne, et elle vérifie que les banques s’y conforment.

La sécurité des services de banque en ligne fait-elle l’objet d’un traitement particulier dans le cadre de votre mission de surveillance des systèmes et moyens de paiement ?

Non, elle s’inscrit naturellement dans le cadre de notre mission : veiller à la sécurité et à la bonne exécution des paiements. Nous sommes vigilants à la sécurité des sites de banque en ligne car on y trouve les informations nécessaires à l’exécution de paiements et de virements. Nous sommes également vigilants à la sécurité des paiements par carte sur Internet. Dans les deux cas, il est essentiel de s’assurer que celui qui effectue le paiement est bien l’utilisateur légitime. Pour cela, il faut l’authentifier de façon suffisamment sûre. Nous procédons sur ces sujets de la même manière que pour les autres instruments de paiement : nous avons défini des objectifs de sécurité à atteindre et nous vérifions que les banques s’y conforment. Nous le faisons au titre de nos missions nationales auprès des banques françaises, comme le font les autres Banques centrales de l’Eurosystème sur leur territoire. Pour les systèmes transfrontaliers, comme certains systèmes de paiement par carte, la surveillance est exercée en commun par plusieurs Banques centrales de l’Eurosystème.

Quelles sont les recommandations de la Banque de France pour répondre aux exigences de sécurité en ligne ?

En collaboration avec la Commission bancaire, nous avons formulé très tôt un certain nombre d’exigences pour renforcer l’authentification des utilisateurs des services de banque en ligne. Dès fin 2000, il y a eu un livre blanc sur la sécurité des opérations bancaires sur Internet [1]. Cela nous a conduits à élaborer, en collaboration avec le Centre français d’organisation et de normalisation bancaires (CFONB), un profil de protection dédié aux sites bancaires et de Bourse en ligne. Ce document, certifié en octobre 2004, par la Direction centrale de la sécurité des systèmes d’information (DCSSI), sert désormais de référentiel pour la définition des architectures et des règles de sécurité des sites de banque en ligne. Nous avons, dès cette époque, demandé aux banques de mettre en œuvre des solutions d’authentification dite “non rejouable” : le mot de passe ou le code d’authentification ne peut servir qu’une seule fois afin d’éviter tout risque de réutilisation par un fraudeur. Les mesures qui ont été prises par les banques vont dans ce sens.

[1] Internet : quelles conséquences prudentielles ? http://www.banque-france.fr/archipel/publications/cb_livbl/cb_livbl_internet.pdf

Nous souhaitons que l’essor des paiements à distance s’accompagne d’une généralisation de l’usage de mots de passe ou de codes non rejouables, pour les opérations de virement et pour les paiements par carte sur Internet. Il est également essentiel de protéger par ce type de solutions, les informations nécessaires à l’exécution de paiements, comme le RIB, lorsqu’elles sont disponibles dès l’accès au site.

Ce qui est assez loin d’être le cas, au moins pour l’accès aux sites de banques en ligne “grand public”…

Les choses évoluent dans le bon sens. Ces solutions peuvent être combinées à la fois pour la banque en ligne et le paiement par carte afin d’en simplifier l’usage par les clients. De telles évolutions sont particulièrement importantes dans le contexte de la concurrence accrue entre banques européennes qui résultera de la mise en œuvre du marché européen des paiements SEPA. Certaines banques françaises diffusent déjà des codes d’accès à usage unique par SMS, d’autres s’apprêtent à distribuer à leur clientèle des lecteurs d’authentification forte. D’autres sont encore en phase de tests auprès de certains segments de clientèle. Bien évidemment, cela n’est pas sans difficultés dans des environnements multicanaux, multi-établissements, au sein de grands groupes. Mais c’est sans doute l’occasion de réfléchir aux services que les banques pourront offrir à l’avenir avec ces nouveaux moyens d’authentification – on pense aux virements SEPA à partir des sites de banques en ligne. ■