Les banques musclent la sécurité des données

Pour protéger leurs clients, les établissements de crédit accroissent leurs investissements. Les tentatives d'effraction demandent toujours plus de vigilance.

www.agefi.fr/actualite-eclairages

PAR YVES RIVOAL

Les vols de données clients survenus ces derniers mois chez Target aux Etats-Unis et chez trois émetteurs de cartes en Corée du Sud amènent à se poser la question de la sécurité des données au sein des banques françaises. Quand on l'interroge sur le sujet, Raymond Bunge, directeur des systèmes d'information (SI) des réseaux France du groupe Société Générale, joue la carte de la transparence. « *Rien qu'en janvier, nous avons identifié quatre nouveaux virus et paré à deux attaques lourdes en déni de service. A cela, il faut ajouter la centaine de robots qui, chaque jour, essaient de repérer des failles dans notre système.* »

La menace est donc bien réelle et permanente. L'intrusion dans le SI des banques, pour y récupérer des listings de clients ou de numéros de cartes bancaires, a toujours constitué une forme de Graal pour les cybercriminels. « *En matière de sécurité, il faut toujours rester modeste,* reconnaît Raymond Bunge. *Les hackers disposent de moyens considérables. Vouloir les défier serait une erreur. En revanche, nous devons tout mettre en œuvre pour les empêcher de nuire.* » En 2014, la direction des réseaux France de Société Générale a d'ailleurs décidé de multiplier par cinq ses investissements en matière de sécurité… Pour parer aux intrusions extérieures, les banques ont déployé des batteries de pare-feux qui ne constituent pourtant pas une garantie de

protection absolue, comme le confirme Raymond Bunge. « *Edifier une muraille devant l'entrée d'un SI complique la tâche des hackers, mais ne les empêchera pas d'entrer. Nous avons donc décidé de renforcer nos investissements sur la sécurité des applications, en mettant l'accent sur les zones sensibles car si un hacker parvenait à pénétrer dans l'une de nos applications clés, il pourrait alors entrer en dialogue direct avec notre serveur central et, par exemple, procéder à des virements, ce qui nous mettrait en position de fragilité maximale.* »

Le péril intérieur

Pour Yves Le Roux, administrateur de l'Association française de l'audit et du conseil informatiques (AFAI), les agressions venues de l'extérieur ne constituent pas le principal péril pour les banques. « *Elles ont en effet mis en place depuis longtemps des protections qui fonctionnent bien. En revanche, il est beaucoup plus compliqué pour elles de se prémunir contre le risque intérieur.* » Un constat corroboré par l'exemple coréen. C'est en effet un salarié du Korea Credit Bureau (KCB), qui collaborait avec trois sociétés émettrices de cartes afin de renforcer la protection des données, qui aurait copié les données de 105 millions de clients pour les revendre à des sociétés de marketing !

Pour se prémunir contre cette menace intérieure, Société Générale a déployé un système d'habilitation avec des annuaires centraux qui vérifie que chaque personne est authentifiée et habilitée à entrer dans une application. « *Nous sommes également en mesure de tracer toutes les actions de nos collaborateurs afin d'identifier ceux qui tenteraient d'accéder à des applications sans autorisation. Car si nous ne pouvons pas empêcher un très bon ingénieur système de prendre à défaut notre protection, nous sommes aujourd'hui en mesure de le repérer immédiatement et de l'empêcher d'agir,* assure Raymond Bunge. Des solutions de Data Leak Prevention (DLP) existent également pour empêcher toute copie intempestive d'informations sur une clé USB, un disque externe ou un Smartphone. « *Ces solutions sont efficaces sur un périmètre maîtrisé, mais elles sont difficilement exportables sur un périmètre externe non maîtrisé* », explique Loïc Pillant, consultant expert sécurité chez Steria.

Or, le risque de piratage des données clients ne se limite pas aux SI des banques, il concerne aussi l'ensemble des prestataires de services de paiement (PSP) et les e-commerçants. « *La plupart des banques s'assurent dans les contrats signés avec leurs prestataires que ces derniers ont mis en œuvre, eux aussi, des plans de sécurité informatique,* souligne Olivier Perrin, responsable des activités conseil moyen de paiements chez Steria. *La protection des données bancaires est également encadrée par diverses réglementations et normes, comme PCI DSS, qui apportent une réelle protection des données de cartes bancaires. Cependant, certaines données bancaires telles que les Iban, utilisées pour les virements et les prélèvements Sepa, ne sont pas visées par cette norme PCI DSS alors que la fraude se déploie sur ces nouveaux moyens de paiements.* »

Le véritable maillon faible reste l'ordinateur du client

Mais le véritable maillon faible pour les banques reste le poste de leurs clients, comme le reconnaît Raymond Bunge. « *Quand vous avez 8 millions de clients qui accèdent à votre site Internet bancaire avec des systèmes d'exploitation parfois obsolètes et qui ne sont plus protégés par les antivirus, il est très facile pour un hacker de prendre le contrôle de l'ordinateur et, avec des virus comme Zeus, Torpig ou Citadel, d'effectuer des opérations sans que le client s'en aperçoive.* » Société Générale mène donc régulièrement des campagnes d'information afin de sensibiliser ses clients à la protection de leur ordinateur. « *Nous avons également déployé le logiciel Trusteer Rapport qui permet de lutter contre les virus bancaires. A ce jour, près de 25 % de nos clients l'ont téléchargé et je conseille à tout le monde de le faire* », conclut Raymond Bunge. ■

L'AVIS DE...


DR

Marc Andries, inspecteur Banque de France et chef de mission de l'Autorité de contrôle prudentiel et de résolution (ACPR)

« *Le risque zéro n'existe pas* »

Quelles sont les obligations des banques en matière de protection des données de leurs clients ?
C'est le règlement n°97-02 du CRBF du 21 février 1997 qui fixe le cadre à respecter par les établissements bancaires en matière de sécurité et de confidentialité des données. Même s'il a été complété depuis par toute une série de mesures adaptées à chaque profil de risques, le régulateur a choisi de rester sur les grands principes. Il revient à l'APCR de veiller, à travers des contrôles ciblés, à ce que les mesures prises correspondent à la réalité des risques auxquels les banques doivent faire face.

Sur quoi portent les contrôles de l'ACPR en matière de sécurité ?
Jusqu'à présent, nos attentes ont principalement porté sur la sécurité de l'environnement de la banque, mais nous étendons de plus en plus cette préoccupation à la bonne sécurité de l'environnement du client. Pour le système d'information de la banque, nous vérifions que les données sensibles sont correctement identifiées. Nous analysons également les mesures de protection prises pour lutter contre les risques de fraudes internes et externes à travers des mesures de chiffrement des données ou de limitation des droits d'accès aux données sensibles. Nous nous assurons en outre que la banque effectue régulièrement des tests d'intrusion et qu'elle prend bien en compte les recommandations formulées à l'issue de ces tests.

Quel regard portez-vous sur l'efficacité des dispositifs de sécurité mis en place par les banques ?
Les grandes banques ont aujourd'hui parfaitement pris conscience des risques et engagé des mesures de protection globalement satisfaisantes. Mais la difficulté en matière de sécurité, c'est que le risque zéro n'existe pas, et qu'il faut donc rester en permanence à un niveau de vigilance élevé. Ce qui suppose de mobiliser énormément de ressources.