Pour garder une longueur d'avance face à des fraudes de plus en plus sophistiquées

Une nouvelle approche tenant compte de l'analyse du big data et du comportement des utilisateurs est nécessaire contre la cyberfraude.

Frédéric Viard
Marketing Director, Financial Messaging
Bottomline Technologies

Les exemples de fraude dans l'industrie financière sont légion, et de nouvelles affaires apparaissent chaque jour. La fraude est partout. Les modèles sont de plus en plus sophistiqués, les fraudeurs toujours plus créatifs, et les pertes colossales. Des analyses récentes montrent que les coûts d'une violation de données se situent entre 4 et 20 millions de dollars en fonction du type d'entreprise concernée[1]. Et cela sans compter les dégâts d'image et de réputation lors de fuite de données ou de fraude avérée.

La protection physique (firewall, anti-malware, anti-virus, chiffrage des données) combinée avec des identifiants robustes (log in, mot de passe, sms ou numéro additionnel de sécurité) restent bien évidemment des éléments clé de la protection contre la fraude. Mais avec des attaques de plus en plus sophistiquées et des méthodes de fraude conçues pour contourner ces couches de sécurité traditionnelles, ce type de protection ne suffit plus. Les responsables de sécurité optent désormais pour une approche plus holistique (formation, procédures, technologies) qui prend en compte notamment l'analyse des données de masse (big data) et le comportement des utilisateurs. Et il y a de quoi, lorsque l'on sait que les pertes liées à la fraude sont estimées à plusieurs billions (!) de dollars par année et que des utilisateurs habilités (ou leurs identifiants usurpés) sont impliqués dans plus de la moitié des cas[2].

En plus d'assurer la sécurité physique des données, il faut donc désormais être en mesure de monitorer les activités en temps réel afin de mettre en évidence les écarts entre un comportement habituel et un comportement suspect. Bien que ce type d'analyse puisse s'étendre à la fraude externe ou à d'autres types de contrôles, le profilage des comportements est particulièrement adapté à la prévention de la fraude interne,

En effet, dans la plupart des cas, une fraude interne s'accompagne d'un comportement inhabituel de l'utilisateur ou de l'entité impliquée (un compte, un système, un flux, un montant, un client, etc.): connexion à un système depuis une adresse exotique ou via un canal insolite, accès inaccoutumé à une application ou à un compte, ou encore nombre de transactions anormal ou montants suspects. En s'attaquant à la modélisation du comportement des utilisateurs et des données – la manière dont elles sont accédées, visualisées, utilisées, manipulées et transportées, l'approche de profilage permet de repérer des anomalies ou des comportements suspects pour ensuite lever des alertes voire bloquer les activités en cours. Très efficace, ce type d'analyse peut être effectué à plus ou moins grande échelle, soit en se concentrant sur le monitoring des données significatives pour la protection de la fraude – en ciblant des applications sensibles, des données confidentielles, certains profils d'utilisateurs, soit de manière massive (big data) en y ajoutant le plus souvent des analyses d'autres types permettant une meilleure planification et la mise à disposition d'informations stratégiques allant jusqu'au comportement des consommateurs – comment ils interagissent habituellement avec votre entreprise et votre offre – afin de mieux profiler et cibler leurs attentes.

LES PERTES LIÉES À LA FRAUDE SONT ESTIMÉES À PLUSIEURS BILLIONS (!) DE DOLLARS PAR ANNÉE.

Dans un monde en pleine digitalisation, les nouveaux canaux d'échanges et de communication génèrent de nouvelles brèches potentielles de sécurité. En outre, avec le nombre croissant de solutions offertes en mode cloud, une attention particulière doit être apportée aux options proposées par les fournisseurs de solutions en termes de prévention de la fraude. Dans ce contexte, une approche pluridisciplinaire à plusieurs niveaux incluant un monitoring avancé des comportements semble la mieux adaptée pour se prémunir de la fraude. Mais les risques restent importants et seule une prise de conscience à tous les niveaux de l'entreprise combinée avec des procédures et des outils efficaces et un plus large partage d'expérience pourraient faire mentir Robert Muller, Directeur du FBI en 2012, qui disait[3]: «Il y a deux types d'entreprises; celles qui ont été piratées et celles qui le seront. Et la tendance est au regroupement en une seule catégorie: celles qui l'ont été et qui le seront à nouveau». ■

(1) Ponemon Institute, 2014 Cost of Cyber Crime Study: United States, October 2014, http://www.ponemon.org/library/2014-global-report-on-the-cost-of-cyber-crime.
(2) Association of Certified Fraud Examiners, Report to the Nations on Occupational Fraud.
(3) Federal Bureau of Investigation, «RSA Cyber Security Conference» March 1, 2012, http://www.fbi.gov/news/speeches/combating-threats-in-the-cyber-worldoutsmarting-terrorists-hackers-and-spies.

EN DROIT

Dr. Thierry Amy, Associé
BCCC Avocats Sàrl, Genève-Lausanne

Banque digitale: les contraintes réglementaires

Les progrès de la technologie et sa grande démocratisation permettent aujourd'hui aux acteurs du monde bancaire et financier d'envisager à la fois de nouveaux services, une nouvelle manière d'interagir avec le client, mais aussi une automatisation croissante des outils de back-office. Ces nouvelles opportunités doivent toutefois se fondre dans un cadre réglementaire de plus en plus contraignant et qui, sans être véritablement monolithique, peine à s'adapter à l'évolution rapide de la technique. Ainsi, les banques qui désirent moderniser leurs infrastructures et proposer à leurs clients des services axés sur les nouvelles technologies se heurtent à plusieurs problématiques, parmi lesquelles nous pouvons notamment mentionner – outre l'entrée en relation d'affaires en ligne et/ou par vidéo, qui a déjà fait l'objet de nombreux commentaires suite à l'entrée en vigueur de la nouvelle Circulaire FINMA 2016/7 – l'évaluation du risque en lien avec l'offre et le développement de nouveaux produits, la sécurité du traitement des données et la vérification de la validité et de l'authenticité des instructions du client.

S'agissant de l'évaluation des risques liés aux nouvelles technologies, à l'occasion de la révision de l'OBA-FINMA, la FINMA a introduit un nouvel article 22 OBA-FINMA consacré aux nouveaux produits et à la gestion des nouvelles technologies. En vertu de cette disposition, l'intermédiaire financier est tenu de «réfléchir» aux risques de blanchiment d'argent et de financement du terrorisme susceptibles de résulter du développement de nouveaux produits ou pratiques commerciales et de l'utilisation de technologies nouvelles ou perfectionnées. Cette réflexion, qui doit avoir lieu avant que les changements ne surviennent, doit également conduire l'intermédiaire financier à saisir la portée, limiter et contrôler les risques générés par de nouvelles pratiques. Le cas échéant, des règles et processus internes nouveaux doivent être élaborés. Pour les banques et négociants en valeurs mobilières, ces dispositions ne constituent pas une réelle nouveauté, la Circulaire FINMA 2008/24 Surveillance et contrôle interne prévoyant déjà que la fonction compliance doit évaluer le risque de compliance lié à l'activité de l'établissement, ce qui englobe déjà l'évaluation du risque lié aux nouveaux produits et aux nouvelles pratiques.

En ce qui concerne la sécurité des données, l'article 7 LPD dispose que « [l]es données personnelles doivent être protégées contre tout traitement non autorisé par des mesures organisationnelles et techniques appropriées». Les articles 8ss OLPD prévoient diverses mesures que l'auteur du traitement de données doit mettre en œuvre, en vue d'une part d'assurer la confidentialité, la disponibilité et l'intégrité des données (destruction accidentelle, erreurs, falsification, vol ou utilisation illicite) et d'autre part, d'introduire des contrôles à l'entrée des installations où sont traitées des données, des contrôles des transports de supports de données et des contrôles de l'accès aux données. De même, le droit de la surveillance, en particulier les articles relatifs à l'exigence d'une organisation adéquate, à la garantie d'une activité irréprochable et au secret bancaire, les circulaires de la FINMA qui les concrétisent (Circulaires 2008/7, 2008/24 et Annexe 3 à la Circulaire 2008/21, actuellement en cours de révision dans le cadre de la Circulaire 2016/X: Gouvernance d'entreprise – banques) et les décisions rendues par la FINMA fixent clairement le principe que la banque doit maîtriser son infrastructure informatique (en termes d'architecture, de confidentialité, d'externalisation ainsi que d'identification et d'évaluation des cyberrisques). A noter cependant que la FINMA n'a à ce jour pas encore élaboré de règles précises en ce qui concerne la maîtrise par la banque de la partie de son infrastructure informatique tournée vers l'extérieur et rendue accessible à ses clients ou à l'ensemble des internautes.

Enfin, la question de la vérification de l'authenticité des instructions du client relève exclusivement du rapport contractuel entre la banque et son client (article 398 CO); la banque doit faire preuve de l'attention que les circonstances permettent d'exiger d'elle. Il convient toutefois de garder à l'esprit que la vérification de l'authenticité des ordres du client n'est pas uniquement une question liée à la technologie. En effet, la pratique démontre que les criminels savent utiliser la ruse (par exemple en se faisant passer pour le client ou pour un employé de la banque) pour parvenir à leurs fins sans avoir à pénétrer les défenses informatiques de la banque (social engineering). Ensuite, il n'existe pas de standard technologique minimal ou approuvé. Il ne s'agit pas là d'une omission du législateur: cela résulte au contraire d'une volonté délibérée d'élaborer une réglementation «neutre» d'un point de vue technologique.

La banque est donc libre de prévoir contractuellement par quel biais les ordres doivent lui être transmis. Ce faisant, elle se devra toutefois non seulement d'attirer l'attention de ses clients sur les risques inhérents à l'utilisation de certains outils technologiques, mais aussi d'acquérir ou de développer une infrastructure informatique à la hauteur des exigences de la FINMA, d'élaborer des procédures adéquates et de surveiller leur application pratique. ■