

La stratégie des banques face à leur sécurité

Les nouvelles difficultés que doivent affronter les établissements financiers sont omniprésentes.

PIERRE-HENRY BADEL

S'il est vrai que les préoccupations sécuritaires ne sont pas nouvelles dans le monde bancaire et financier, la crise économique a relégué cette question à un niveau de priorité moins élevé. Et parallèlement, de nouveaux risques apparaissent, en particulier liés à l'émergence des réseaux sociaux. «Dans le cas particulier de la Suisse, sa situation géo-économique particulière et les contraintes auxquelles doivent faire face ses places financières constitue l'une des cinq grandes préoccupations auquel doit faire face le secteur de la banque et de la finance», a relevé Jean-Pierre Therre lors de la conférence débat annuelle de l'Union des intérêts de la place financière lémanique qui s'est tenue à Palexpo le 18 novembre dernier. «Ceci est d'autant plus préoccupant qu'une très grande partie du patrimoine informationnel et du savoir-faire des entreprises se retrouve souvent en ligne, que ce soit sur Internet ou dans ce que l'on désigne sous le nom d'Internet profond», a-t-il relevé. «Le pillage de ce savoir, son détournement ou sa mauvaise utilisation constituent des risques omniprésents», précise Jean-Pierre Therre.

Pour cet ingénieur EPFL spécialisé dans les télécommunications et responsable de la sécurité à la banque Pictet, le défi majeur que les établissements financiers doivent relever réside dans le fait que ces attaques ont un caractère diffus, souvent ignoré des personnes et entreprises qui en sont l'objet. Face à ce fléau, la principale réponse des banques est de lancer des campagnes de prise de conscience des risques et des dangers auprès de son personnel. Elles éviteront aussi par tous les moyens de le mécontenter, de peur qu'il ne cherche à se venger. De plus, chaque licenciement devra être réalisé en prenant toutes les précautions indispensables.

L'autre défi majeur des banques réside dans le fait que les clients recherchent toujours plus de simplicité dans le déroulement des opérations. Les questions qui se posent réellement aux établissements financiers ont trait à la manière d'accéder à l'information, tout en garantissant l'intégrité des données de même que leur disponibilité. «Comment est-il possible de concilier l'exploitation des données personnelles avec l'accès à la sphère privée de ses clients», se demande Jean-Pierre Therre. «Et enfin quel prix accorde-t-on à la valeur ajoutée économique de la sécurité», enchaîne-t-il. La réponse à cette question s'avère sur ce point-là extrêmement politique pour les banques. Car aujourd'hui on est de plus en plus confronté à une consolidation du marché de la cybercriminalité. «Le crime organisé découvre qu'il court moins de risques en déployant ses activités dans le monde virtuel», admet volontiers Jean-Pierre Therre. «Cette consolidation est actuellement essentiellement le fait des pays de l'ex-bloc de l'Est, de l'Asie et de l'Amérique du Sud», témoigne-t-il en l'occurrence.

La disparition de la frontière entre le lieu de travail et domicile grâce aux appareils nomades facilitent grandement ce type d'intrusion, d'autant plus que le recrutement à l'échelle internationale et la mondialisation du monde bancaire vont de pair avec une perte de la notion d'appartenance par rapport à son employeur. Le vol et l'usurpation d'identité ainsi que le Hacking sur les réseaux sociaux sont aussi autant de nouveaux défis que les banques devront affronter au cours de ces prochaines années. Tout comme l'intégration de l'ensemble des partenaires et fournisseurs dans la chaîne de sécurité des établissements. ■

LE DÉFI MAJEUR QUE LES ÉTABLISSEMENTS FINANCIERS DOIVENT RELEVER RÉSIDE DANS LE FAIT QUE CES ATTAQUES ONT UN CARACTÈRE DIFFUS.