La cybersécurité, entre défense et opportunités

L'accélération du numérique, la multiplication des canaux, des usages, et le développement des réseaux informatiques représentent des risques mais aussi des opportunités pour les banques.

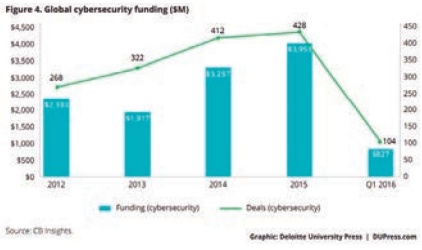
Le volume d'attaques contre certaines institutions financières françaises progresse jusqu'à 10 fois chaque année. A l'échelle mondiale, l'industrie financière subit jusqu' à 300 % d'attaques de plus que tout autre secteur ! Depuis 2013, plus de 100 banques dans 30 pays différents ont été soumises à des attaques informatiques qui sont à ce jour toujours actives. Selon Kaspersky Lab, chaque raid peut atteindre jusqu'à dix millions de dollars.

« Le secteur bancaire est particulièrement exposé au développement exponentiel des cyberattaques opérées par menace persistante avancée, hameçonnage ou déni de service principalement », alerte la Banque de France dans son rapport intitulé « Evaluation des risques du système financier francais ». « Il devient par conséquent urgent que les dirigeants de banques prennent la pleine mesure des risques en matière de cybersécurité et que les dispositifs de sécurité soient renforcés », préviennent les auteurs. Bien que les banques aient renforcé leurs dispositifs, « les systèmes de détection des banques permettent de déjouer de nombreuses attaques, mais plusieurs incidents récents de grande ampleur montrent le caractère évolutif, de plus en plus sophistiqué et protéiforme de ces attaques : vol des données personnelles liées à 76 millions de comptes utilisateurs de la banque JP Morgan Chase en juin 2014, blocage de sites de banques en ligne européennes en 2014, rançonnage de banques grecques avec menaces d'attaques en déni de service en 2015, transfert frauduleux de 81 milliards USD au détriment de la Banque centrale du Bangladesh en février 2016 », résume la Banque de France.

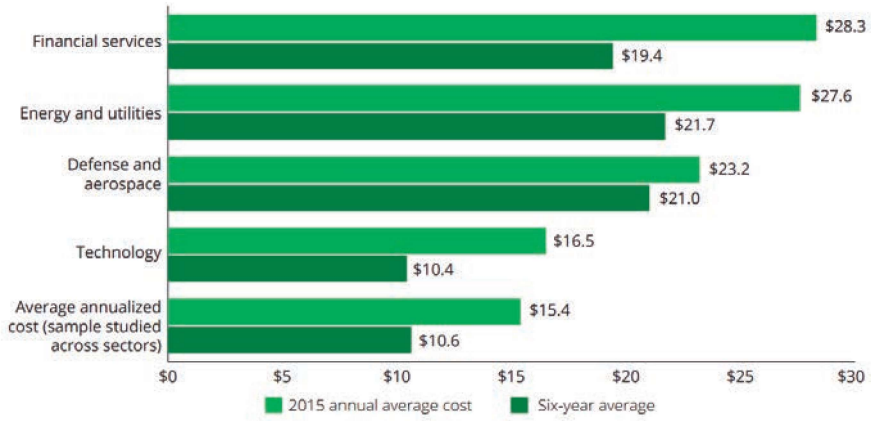
Des opportunités en constante construction

Obligées de se protéger et pouvant être tenues légalement responsables, les

FONDS DE LA CYBERCRIMINALITÉ



COÛT DE LA CYBERCRIMINALITÉ



Source: Ponemon Institute and Hewlett Packard Enterprise, *2015 Cost of cyber crime study—United States*, October 2015.

Graphic: Deloitte University Press | DUPress.com

banques en font un axe prioritaire. Parallèlement, elles en font également une nouvelle activité commerciale pour répondre aux attentes et nouer la confiance. Un récent sondage de la Commission européenne montre que 80 % des Français et Européens jugent important et prioritaire la lutte contre la cybercriminalité. De la même manière, 60 % des Français et 56 % des Européens font confiance aux établissements financiers pour protéger leurs informations personnelles.

Les établissements se positionnent ainsi sur le marché de la cybersécurité, qui est colossal. A titre d'illustration, les attaques généreraient des pertes pouvant atteindre 2 200 milliards d'euros d'ici à 2020.

Elles ont créé de nouvelles offres s'appuyant sur les besoins informatiques de leurs clients (services sécurisés sur mobile et tablette, signature électronique, solutions de dématérialisation, authentification forte, coffre-fort électronique…). Elles mettent également à disposition leurs infrastructures, technologies, savoir-faire, informations et formations. Ces offres leurs permettent à la fois d'abaisser les coûts et risques, d'aseptiser leur écosystème avec les parties prenantes, et de bénéficier de revenus.

Reste que le marché n'est pas sans risques. Par exemple, les technologies clés telles la biométrie sont devenues populaires. Cette dernière peut être compromise. A l'image du Bureau de gestion du personnel américain qui s'est vu voler 5,6 millions d'empreintes digitales. Les « fingerprints », à l'inverse des mots de passe ou autres dispositifs de sécurisation, ne peuvent pas être modifiés. L'enjeu est alors de trouver une sécurité proportionnée. ■ PR