الجمهورية الجزائرية الديمقراطية الشعبية
REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
وزارة المالية
MINISTERE DES FINANCES
CTRF
CELLULE DE TRAITEMENT DU RENSEIGNEMENT FINANCIER
خلية معالجة الإستعلام المالي
خ م إ

Lettre d'Informations des actualités internationales
en matière de lutte contre le Blanchiment d'Argent
et le Financement du Terrorisme

Opération Tovar : Quand le DoJ démantèle un réseau de pirates international

Le ministère américain de la Justice (DoJ) a annoncé hier lundi 2 juin le démantèlement d'un nouveau réseau de pirates informatiques international étant responsable de plusieurs dizaines de milliers d'attaques ayant permis de voler plusieurs millions de dollars.

Cette opération de grande ampleur intervient quelques jours à peine après les multiples arrestations de pirates informatiques utilisant le maware BlackShades à des fins de fraude bancaire. Pour rappel, 50 perquisitions ont eu lieu en France dans cette précédente affaire, sans compter les dizaines de mules arrêtées pour blanchiment. La aussi, ce sont les renseignements américains qui ont aidé les français après les avoir mis sur la pistes des cybercriminels.

Tovar est le nom de l'opération qui a été menée conjointement par Interpol et plusieurs polices nationales (dont la France, le Japon, l'Italie, la Nouvelle-Zélande, le Luxembourg). Une action d'envergure qui, d'après les dires du DoJ américain, viserait le plus important réseau de cybercriminels au monde, jamais stoppé ! En effet, le réseau baptisé "Gameover Zeus" serait le plus sophistiqué que le FBI et nos alliés ont jamais tenté de démanteler. Mais bon, il faut noter que l'on entend souvent ce genre d'affirmations quelque peu grandiloquentes avec eux…

Les membres de ce réseau international est responsable du vol de millions de dollars sur le sol américain mais aussi à des centaines d'entreprises de par le monde.

Tovar a exploité le climat de tension politique actuel entre la Russie et l'Ukraine et le reste du monde, notamment l'Europe et les Etats-Unis, qui a permis de procéder à un grand nettoyage et donner l'opportunité de "couper des têtes de réseau", dont l'homme le plus important et influent du réseau Gameover Zeus, un russe de 30 ans prénommé *Evgeniy Mikhailovich Bogachev*, inculpé par le tribunal de Pittsburgh en Pennsylvanie au mois d'août 2012. Ce dernier était connu sous divers pseudos tels que Slavik, Pollingsoon, 92829 ou encore lucky12345 et aurait, même si cela semble être tabou, des entrées au Kremlin… Quoi qu'il en soit, l'homme faisait parti des "Most Wanted" publiés par le FBI.

Cet ingénieux russe n'a pas pu résister à l'alliance entre la police ukrainienne, le FBI et l'EC3 européen (Europol), qui ont réussi l'exploit de mettre hors service le centre de commande et de contrôle (C&C) du botnet principal du réseau basé à Kiev et Donetsk. L'architecture était complexe et très sophistiquée : ces nœuds principaux tenaient sous leur emprise des serveurs annexes basés en France, Canada, Allemagne,

Luxembourg, Pays-Bas et au Royaume-Uni tenus par des “lieutenants” de confiance, qui eux-mêmes contrôlaient plus de 320 000 ordinateurs de particuliers et d’entreprises transformés en zombies.
Ci-dessous, un schéma en anglais expliquant le processus de fraude bancaire via le cheval de Troie ZeuS :
Bien entendu, le seul but de tout cela était de dérober un maximum d’argent et le gang mafieux ne reculait devant rien. Bogachev a commencé à intéresser le FBI après la découverte d’une version modifiée du cheval de Troie Zeus, connu sous le nom Gameover Zeus (GOZ), plus perfectionnée et indétectable par rapport à son grand frère plus populaire. Le FBI indique que GOZ serait responsable de plus d’un million d’infections de systèmes informatiques, entraînant des pertes financières de centaines de millions de dollars. Bogachev a également été accusé de complot en avril 2014 en vue de commettre une fraude bancaire liée à son implication présumée dans le fonctionnement d’une autre variante d’un code malveillant connu sous le nom “Jabber Zeus”.
Le réseau est tellement immense que les autorités le soupçonne d’avoir infecté près d’un million de machines partout dans le monde grâce au botnet Gameover Zeus (ou GOZeuS) mais aussi via le ransomware Cryptolocker, qui aurait déjà infecté plus de 234 000 machines. Du coup, les autorités (dont le NCA, National Crime Agency britannique) appellent les internautes du monde entier à renforcer la sécurité de leurs machines et de procéder à un nettoyage poussé des malwares présents sur ces dernières.
*“*Les Botnets infectent généralement leurs victimes de manière opportuniste plutôt que via des attaques ciblées. Le plus souvent, la finalité est de prendre le contrôle des machines afin de perpétrer des attaques par déni de service distribué (DDoS), via des redirections de communications depuis un centre de commande et de contrôle (C&C) et de rassembler des informations personnelles d’identifications et des codes d’accès de haute importance*“,* souligne Olivier Mélis, Country Manager France chez CyberArk.
Bien qu’elles concernent principalement les individus, ces attaques opportunistes sont également en mesure d’atteindre les réseaux d’entreprises afin de détourner les codes d’accès, que ce soit à travers l’infection d’une machine au sein du réseau ou les identifiants VPN. Les cybercriminels peuvent ainsi viser les particuliers mais également les organisations qui leur permettent de faire des bénéfices financiers plus intéressants.
A n’en pas douter, c’est donc un coup d’arrêt pour un très important réseau cybercriminel qui a été réalisé d’une main experte et à l’échelle mondiale.
Néanmoins, il ne faut pas oublier qu’il en reste encore beaucoup qui perpétuent ce juteux business. De plus, la NCA a indiqué le début d’un compte à rebours de 14 jours avant que de nouvelles campagnes de Gameover Zeus et Cryptolocker ne soient de nouveau opérationnelles. D’où l’importance que les victimes nettoient leurs systèmes des malwares avant cette date fatidique à laquelle elles se retrouveront de nouveau sous le joug d’un botmaster pirate… Le US CERT quand à lui a publié une alerte.
Liens : http://www.undernews.fr/hacking-hacktivisme/operation-tovar-quand-le-doj-demantele-un-reseau-de-pirates-international.html

La vidéo pour le KYC, mais pas que...

Le ministre des Finances a confirmé que l'usage de la vidéo était autorisé pour identifier les clients du secteur financier, dans le souci de tirer profit des nouvelles technologies dans le champ de la réglementation.

Les professionnels du secteur financier sont bien autorisés par la Commission de surveillance du secteur financier (CSSF) à identifier leurs clients ou à vérifier leur identité par l'intermédiaire de vidéoconférences.

C'est ce que vient de confirmer le ministre des Finances au député CSV Laurent Mosar qui, par l'intermédiaire d'une question parlementaire, voulait s'assurer de la validité de la procédure.

Une procédure possible depuis le 8 avril dernier, date à laquelle la CSSF a publié son avis sous forme de «questions/réponses», précisant que la nouvelle procédure, autorisée pour tenir compte de l'évolution des technologies, n'enlève rien en matière d'obligations de lutte contre le blanchiment de capitaux et de lutte contre le financement du terrorisme.

«Si le professionnel est amené à considérer que l'entrée en relation d'affaires avec un client au moyen de ce procédé présente un risque particulier, il sera tenu de prendre des mesures de mitigation selon son appréciation de la situation et du risque détecté», rappelle Pierre Gramegna dans sa réponse.

La CSSF a, en autorisant cet usage, devancé la transposition obligatoire pour le 26 juin 2017 d'une directive européenne qui reconnaît ces nouveaux outils: «Les nouvelles technologies offrent aux entreprises et aux clients des solutions rentables et efficaces en termes de temps et devraient dès lors être prises en compte au moment de l'évaluation des risques.»

L'usage de la vidéo ne doit donc pas être considéré isolément. En amont de l'identification ou de la vérification en vidéo, des procédures complémentaires doivent être mises en place, dont l'élaboration d'un guide pour la conduite de la conférence par vidéo, la réalisation d'une due diligence en matière de sécurité informatique ainsi que de lutte contre le blanchiment de capitaux et de lutte contre le financement du terrorisme, l'exigence de formation adéquate de la personne en charge de cette tâche, l'utilisation de locaux adaptés à la réalisation du procédé, ainsi que l'existence de procédures internes adéquates. 28.06.2016

Liens : http://paperjam.lu/news/la-video-pour-le-kyc-mais-pas-que

L'Inde commercialise des services sécurisés d'authentification « e-KYC »

Les autorités indiennes multiplient leurs actions pour rappeler les efforts accomplis dans le domaine des nouvelles technologies et la mise en œuvre d'un certain nombre de projets, tels que le «make in India», «skill India », « digital India » lancés récemment afin de rendre l'Inde plus compétitive.

L'Autorité d'identification unique de l'Inde (UIDAI) est une agence du gouvernement central. Son objectif est de collecter les données biométriques et démographiques des résidents, de les stocker dans une base de données centralisée, et de délivrer un numéro d'identité unique à 12 chiffres appelé Aadhaar à chaque résident. Il s'agit ici

du plus grand projet d'identification numérique au monde. A la date du 8 Août 2015, plus de 893 millions de cartes Aadhaar ont déjà été émises.
Les autorités gouvernementales indiennes se sont efforcées de répondre aux inquiétudes de la population par une suite d'ordonnances répétant que la carte d'identité électronique n'était pas obligatoire, mais recommandée et utile à tous. L'une des applications les plus spectaculaires est celle de la sécurisation de l'identité du correspondant dans les transactions mobiles (KYC).
Le processus KYC (Know Your Customer) permet à une entreprise de vérifier l'identité de ses clients. Le sigle KYC est également utilisé pour se référer à la réglementation bancaire qui régit ces activités. Les banques, les assureurs et les organismes de crédit à l'exportation exigent que leurs clients fournissent des informations détaillées afin de vérifier leur probité et leur niveau d'intégrité. Le procédé électronique e-KYC est de plus recommandé dans les transactions internationales pour éviter le vol d'identité, la fraude financière, le blanchiment d'argent et le financement du terrorisme.
Plusieurs exploitants de réseau de télécoms indiens, y compris Idea Cellular, Vodafone et Airtel ont ouvert des services e-KYC. Ces derniers devraient permettre aux entreprises de télécommunications de réduire les coûts et le temps passé en vérifications diverses. Les informations fournies par la carte Aadhar permettent le contrôle de l'identité de citoyens indiens en moins de 30 secondes si la personne possède un numéro de carte Aadhar. Des entreprises associées, telles que Suvidha Infoserve envisagent l'ouverture de services e-KYC dans plusieurs dizaines de milliers de points de vente. HDFC Bank a introduit l'e-KYC (Know Your Customer électronique) en collaboration avec la Société nationale des paiements. HDFC a également affirmé que la banque est prête à installer des lecteurs biométriques pour la numérisation des empreintes digitales pour rendre le processus encore plus facile. Avec le procédé e-KYC, il devient plus facile pour un client d'ouvrir un compte ou de souscrire une assurance sans aucune saisie de données, toutes les procédures étant effectuées de façon électronique.
A compter d'aujourd'hui, sur les téléphones Android en Inde, vous pouvez utiliser votre carte bancaire personnelle pour l'application Uber, car cette association permet l'authentification en deux étapes. Uber Inde a conclu un partenariat avec Zaakpay qui gère la passerelle numérique basée à Gurgaon pour la clientèle répartie dans 18 villes. Le projet pilote qui s'est déroulé à Hyderabad a permis d'acquérir une meilleure compréhension du comportement des clients, de leurs préférences et des tendances d'utilisation. D'autres acteurs concurrents en Inde, y compris Ola, Meru et TaxiForSure, ont tous accepté le modèle de paiement à la prestation depuis sa création.
Walmart s'est associé avec Vodafone pour les paiements en M-Pesa dans les magasins. Vodafone M-Pesa est le plus grand de correspondant bancaire en Inde avec 90.000 agents et plus de 3 millions de clients. L'entreprise joue un rôle crucial dans l'élargissement du champ d'application du m-commerce et de divers services financiers. L'exploitant de réseau Airtel a effectué une série de tests de services e-KYC dans plusieurs États, et a constaté une grande économie de temps et d'argent à l'occasion de ces procédures. DoT a choisi Vodafone pour le lancement de ce service d'authentification e-KYC en Inde.
Liens : http://www.smart-webzine.com/linde-commercialise-des-services-securises-dauthentification-e-kyc-5490

Les formes organisées de la Cybercriminalité

Pour les organisations criminelles, les réseaux d'Internet se sont rapidement imposés comme une aide extrêmement efficace pour faciliter leurs activités traditionnelles.
Exploitant sans Etat d'âme et à une échelle bien supérieure le réservoir d'informations et de techniques constitué par les pirates informatiques, nombre d'organisations criminelles se lancent dans la cybercriminalité tandis que d'autres cybergangs naissent, alléchés par les perspectives de gains faciles et rapides.

La pornographie

La diffusion de supports pornographiques a été et reste parmi les premières applications d'Internet. Or, si la pédophilie fut longtemps restreinte à un cercle très fermé, l'arrivée d'Internet a malheureusement provoqué presque instantanément l'expansion brutale du problème en permettant de diffuser ou d'acquérir dans le monde entier du matériel photo ou vidéo par de simples commandes au clavier d'un ordinateur ; d'autant que certains pays comme le Japon ne possèdent aucune législation relative à la publication d'images pornographiques impliquant des enfants.
L'attention des services de sécurité est mobilisée sur cette forme de délinquance en raison notamment de l'émotion légitime que suscite ce type d'affaire dans l'opinion publique. Cependant, la lutte contre cette criminalité est difficile car, pour dissimuler leurs activités aux yeux des autorités, les pédophiles ont recours à des procédés de chiffrement des communications et de stockage des documents pornographiques. Ils restreignent de plus les accès de leurs sites par mots de passe et conditionnent parfois également l'accès à la fourniture d'un nombre de photos à caractère pédophile.
Les investigations menées dans ce domaine ont démontré l'existence de réseaux internationaux structurés. A titre d'illustration, elles ont mis à jour en 1998 un vaste réseau, du nom de "Wonderland Club", qui impliquait 14 pays dans le monde appartenant à l'Europe, l'Amérique du Nord et l'Australie. Son démantèlement coordonné par Interpol a entraîné l'arrestation d'environ 100 personnes et la saisie de plus de 100 000 images.

Le blanchiment d'argent et l'évasion fiscale

Le développement des nouvelles technologies entourant le commerce électronique a largement facilité le blanchiment d'argent et l'évasion fiscale au point que ce procédé n'est plus de nos jours réservé aux seules grandes entreprises criminelles comme la mafia ou encore aux grands groupes industriels soucieux de dissimuler une partie de leurs avoirs pour le compte d'intérêts particuliers.
Désormais, les petites bandes organisées comme les petites sociétés ont les instruments en leur possession pour recycler ou dissimuler au fisc une part de leurs revenus. Les transferts de fonds entre Etats et par conséquent entre systèmes législatifs différents ne nécessitent que quelques secondes.
D'autre part, la constitution d'un réseau d'organismes bancaires non officiels permet d'échapper encore plus facilement au contrôle des Etats, en particulier de celui mis en œuvre par le biais des banques centrales.

Les extorsions ou détournements de fonds

Certains groupes désireux de s'enrichir par la voie la plus rapide s'en prennent directement aux organismes bancaires. Il s'agit en quelque sorte d'une version moderne de l'attaque de banque, à laquelle on pourrait donner le nom de "hold up électronique".

Ils sont pour nombre d'entre eux originaires des Etats-Unis et des autres pays occidentaux, mais pas uniquement. Des pays tels que l'Inde, le Pakistan et même l'Indonésie sont en train de devenir de véritables repaires de pirates. Il faut noter que ces derniers ont souvent été diplômés dans les meilleures universités occidentales et y ont acquis leur expertise en sciences informatiques. La Russie foisonne également de pirates depuis la chute du communisme. Des milliers d'informaticiens de haut niveau se sont en effet brusquement retrouvés sans emploi du jour au lendemain après avoir fait partie des privilégiés du régime et s'être impliqués dans les programmes les plus en pointe de leur pays. Ils ont pu voir alors dans ce type d'activités le moyen le plus simple de retrouver une source de revenus décente.

Parmi les cas répertoriés, la banque du Vatican s'est fait pirater par une vingtaine de personnes qui ont tenté d'extorquer 7 milliards de francs. La technique utilisée fonctionnait avec de petites sommes mais la tentative a échoué lorsqu'ils ont cherché la complicité d'un directeur de banque en Suisse.

Autre détournement mais réussi cette fois, en 1994, un pirate russe Vladimir Levin, opérant depuis St Petersbourg a réussi à accéder au système d'information de la Citibank de New York et à transférer des fonds sur des comptes ouverts par des complices aux Etats-Unis, en Hollande, Finlande, Allemagne et Israël. Ce jour là, ce sont quelques 10 millions de dollars qui se sont volatilisés, détournés vers des comptes personnels. Des milliers d'épargnants américains se sont vus dépossédés du contenu de leur compte. De cet argent, seulement 400 mille dollars ont été récupérés depuis.

Les escroqueries

De même que les sollicitations à caractère frauduleux sont devenues banales par téléphone ou par courrier, le cyberespace foisonne de propositions d'investissements illégales. Il faut reconnaître qu'il se prête particulièrement à ce type de pratique parce qu'il permet d'entrer en contact instantanément avec des millions de personnes, d'afficher une apparence de respectabilité sans gros efforts et de disparaître tout aussi instantanément sans laisser de traces. On y trouve par exemple une foule d'offres de vente, de demandes d'arrhes pour des services qui ne seront jamais honorés, de loteries, de sites d'enchères, de ventes pyramidales, etc.

Un service de réclamations en ligne a lancé en 2000 un avertissement contre un site de petites annonces automobiles du réseau Internet. En échange d'une commission fixe de 399 dollars, ce site offrait de placer sur une page web le descriptif des voitures des particuliers désireux de les mettre en vente. Au cas où le véhicule ne serait pas vendu dans les 90 jours, il promettait de restituer au propriétaire la commission. Evidemment, plusieurs voitures de clients, présentées sur page web, n'ont pas été vendues durant le délai imparti, mais ces derniers n'ont trouvé personne sur le site d'annonces pour leur rembourser leur argent. Ce site Internet a fermé depuis.

Ainsi, l'informatique procure aux entreprises criminelles en plus d'une envergure mondiale des prises de risques moindres car elles peuvent agir sans violence physique et avec un maximum de discrétion.

Liens : http://www.undernews.fr/hacking-hacktivisme/les-formes-organisees-de-la-cybercriminalite.html

Lutter contre la criminalité sur le Net

Au cours des dernières années, l'Internet a connu une croissance explosive. Comparés aux quelque 26 millions d'utilisateurs dénombrés en 1995, ce sont aujourd'hui plus de 200 millions de personnes qui communiquent, font leurs achats, payent leurs factures, font du commerce et consultent même leur médecin sur Internet.

Alors que l'Internet connaissait une grande expansion, le crime en ligne augmentait également. Les cyber-criminels, comme on les appelle, ont largement envahi ou envahiront le monde virtuel, commettant des délits, tels qu'utilisation de codes d'accès confidentiels, piratage, fraude, sabotage informatique, trafic de drogue, commerce pornographique à caractère pédophile et "cyber-harcèlement".

Les criminels informatiques sont aussi variés que les différentes formes de crime qu'ils pratiquent. Il peut aussi bien s'agir d'étudiants, de terroristes ou de membres du crime organisé. En ce qui concerne la criminalité économique, telle que la fraude ou le vol d'informations, ce sont les employés à domicile qui représentent la catégorie la plus importante, tenue responsable de 90% de ces délits, selon le Manuel des Nations Unies sur la prévention et le contrôle de la criminalité informatique.

Les cyber-criminels sont à même de traverser, à toute allure, les frontières en passant inaperçus, cachés derrière d'innombrables "liens" ou en disparaissant tout simplement sans laisser de trace écrite. Ils peuvent faire passer des communications par le biais de "refuges de données" ou y dissimuler les preuves de leurs délits, les pays ne disposent pas des lois ou du savoir-faire nécessaires pour les retrouver.

Dans un effort tendant à réduire cette menace croissante, un atelier spécial sera organisé lors du Dixième congrès des Nations Unies pour la prévention du crime et le traitement des délinquants, à Vienne, du 10 au 17 avril. L'atelier, organisé par l'Institut asiatique et extrême-oriental des Nations Unies pour la prévention du crime et le traitement des délinquants (UNAFEI), basé à Tokyo, et placé sous les auspices du Centre des Nations Unies pour la prévention internationale du crime (CPIC) se concentrera sur la coopération mondiale en matière d'enquêtes sur le crime informatique et de sa poursuite.

"Cet atelier doit servir pour les pays de forum de partage d'informations sur des domaines ayant trait aux techniques d'investigation et aux lois informatiques. Il mettra en présence une grande diversité d'expériences, de savoirs-faire et d'approches relatives à ce problème", déclarait Christopher Ram, responsable de la prévention du crime (crime informatique) au CPIC.

Piratage, sabotage et harcèlement

Le piratage de sites confidentiels, grâce à des techniques sophistiquées permettant d'imiter les codes d'accès ou de contourner les dispositifs de sécurité, est devenu un cyber-délit de plus en plus répandu. Une fois qu'ils ont obtenu un accès, les pirates peuvent "injecter" des virus, envoyer des messages injurieux ou voler des données précieuses, y compris des informations sur les cartes de crédit et des documents confidentiels sur les sociétés.

Les services secrets américains estimaient récemment que les consommateurs perdent environ 500 millions de dollars par an du fait des vols de cartes de crédit ou de la récupération en ligne d'informations sur les cartes, commis par les pirates. Ces codes de cartes peuvent être vendus pour des sommes non négligeables à des faussaires qui utilisent des programmes spéciaux pour les encoder sur les bandes magnétiques des cartes de crédit ou bancaires, note le Manuel de l'ONU.

D'autres cyber-criminels sabotent les ordinateurs pour obtenir un avantage économique sur leurs concurrents ou pour les menacer d'endommager les systèmes à des fins d'extorsion. Les délinquants trafiquent des données ou des opérations de façon directe, ou bien encore utilisent ce que l'on appelle des "parasites" ou des "virus", à même de bloquer complètement les systèmes ou d'effacer les données d'un disque dur. Ciblés au hasard, les virus informatiques qui passaient auparavant d'un ordinateur à l'autre par le biais de disquettes "infectées" sont aujourd'hui transmis par les réseaux et se dissimulent souvent dans des messages e-mail ou des programmes téléchargés à partir d'Internet.

L'Europe a expérimenté pour la première fois, de façon avérée, une opération d'extorsion d'argent menée par le biais d'un virus. En 1990, le monde de la recherche médicale a été menacé par un virus qui devait détruire des sommes croissantes de données si une rançon n'était pas versée pour que ce virus soit "soigné".

Les cyber-harceleurs ont également recours à l'e-mail pour envoyer des messages de menace à d'autres personnes, en particulier aux femmes. On estime qu'environ 200000 femmes sont harcelées chaque année, estimait Barbara Jenson dans le livre qu'elle publiait en 1996, Cyberstalking: Enforcement and Personnal Responsibility in the On-line World.

Une habitante d'Amérique du Nord a été harcelée pendant plusieurs années par les e-mails d'un inconnu qui menaçait de la tuer, de violer sa fille et de faire circuler son adresse sur le réseau, raconte Mme Jenson.

Les délinquants se sont aussi servis des e-mails et des "espaces de discussion" du réseau Internet pour dénicher des proies vulnérables. Les pédophiles, par exemple, gagnent, en ligne, la confiance des enfants et arrangent, ensuite, des rendez-vous dans la vie réelle pour abuser d'eux ou les enlever. Selon le Département de la justice américain, la pédophilie est en progression sur Internet.

En plus de s'attaquer aux pages web privées, les criminels peuvent ouvrir leurs propres sites web pour escroquer des clients ou vendre des biens et des services illégaux, tels qu'armes, drogues, médicaments interdits ou sans ordonnance et documents pornographiques.

CyberCop Holding Cell, un service de réclamations en ligne, a récemment lancé un avertissement contre un site de petites annonces automobiles du réseau Internet. Pour une commission fixe de 399 dollars, le service devait mettre sur une page web un descriptif de la voiture du client et promettait de restituer cet argent, si le véhicule n'était pas vendu dans les 90 jours.

Plusieurs voitures de clients, présentées sur page web, n'ont pas été vendues durant le temps imparti, mais ces derniers n'ont trouvé personne sur le site d'annonces pour leur rembourser leur argent, raconte CyberCop. Le site Internet pour ce "service" a fermé depuis.

Attraper les cyber-criminels

Comme le cyber-crime progressait, de nombreux pays ont adopté des lois pour punir ce nouveau phénomène, tel que le piratage. Ils ont aussi pu adapter les législations déjà existantes, afin que les peines pour délits traditionnels, fraude, vandalisme et sabotage s'appliquent aussi au monde virtuel.

Singapour, par exemple, a récemment amendé son Computer Misuse Act (loi sur les délits informatiques, CMA). Selon CNET Singapor les peines encourues sont aujourd'hui plus sévères pour quiconque trafique des "ordinateurs protégés" - les individus liés à la sécurité nationale, aux banques et aux services financiers, de même qu'aux urgences et à la fonction publique-, cela s'applique aussi à l'accès à des sites

confidentiels, à la modification, à l'utilisation ou l'interception de matériel informatique.
Certains pays disposent de groupes spécialisés dans la recherche des cyber-criminels. Le Service des enquêtes spéciales de l'armée de l'air américaine est un des plus anciens, il fut créé en 1978. Composé de responsables chargés du respect de la loi disposant de formations informatiques très poussées, le groupe des enquêteurs informatiques australiens est un autre organe de ce type. Le groupe australien rassemble des preuves et les communique aux institutions pertinentes chargées du respect de la loi du pays où le délit a été commis.
En dépit de ces efforts, les responsables du respect de la loi sont encore confrontés à de nombreux problèmes. Le problème majeur étant notamment que de tels délits traversent facilement les frontières, ce qui fait des procédures d'enquête sur les délinquants, de même que de leurs poursuites et de l'application de leurs peines, de vrais casse-têtes juridiques et législatifs. Et, une fois qu'un délinquant a été repéré, les responsables doivent décider de l'extrader pour un procès qui se tiendra ailleurs ou de transférer les preuves, et quelques fois les témoins, à l'endroit où les délits ont été commis.
En 1992, des pirates européens ont attaqué un centre informatique californien. L'enquête policière fut bloquée du fait d'un manque de "cocriminalité" -des lois identiques interdisant dans les deux pays de telles pratiques- qui a entravé la coopération officielle, selon le Département américain de la justice. Finalement, la police du pays d'origine des pirates a offert son aide, mais peu de temps après le piratage a cessé, la piste s'est refroidie et le dossier a été fermé.
De la même manière, le Service d'enquêtes criminelles et le Bureau fédéral d'enquêtes américains ont suivi la piste d'un autre pirate jusque dans un pays d'Amérique latine. Le pirate volait des fichiers contenant des mots de passe et modifiait les fichiers d'accès de certains systèmes informatiques militaires, universitaires et privés. Nombre d'entre eux contenaient des études confidentielles sur les satellites, la radiation et la recherche sur l'énergie.
Les responsables du respect de la loi de ce pays sud-américain se mirent en quête de l'appartement du pirate et y saisirent son matériel informatique, au titre de violations potentielles de la loi nationale. Mais aucun accord d'extradition ne liait les deux pays en matière de crime informatique, bien que de telles dispositions existaient entre eux dans le domaine de la criminalité traditionnelle. En fin de comptes, le cas fut résolu, mais uniquement parce que le pirate avait accepté, en échange d'une réduction de peine, de plaider coupable aux Etats-Unis.

Détruire, dissimuler les preuves

Il n'est pas difficile pour les délinquants de faire disparaître les preuves en les modifiant, les effaçant ou les déplaçant. Cela constitue un autre obstacle majeur aux poursuites des cyber-criminels. Si les responsables du respect de la loi sont moins rapides que les délinquants, la plupart des preuves disparaissent. Ou bien les données auront été encryptées; une technique de plus en plus courante visant à protéger les personnes comme les affaires sur les réseaux informatiques.
L'encryptage peut gêner les enquêtes criminelles, mais si les responsables du respect de la loi parviennent à disposer d'un savoir technique trop important, ce sont les libertés individuelles des personnes qui pourraient en souffrir. Le commerce électronique défend l'idée selon laquelle le respect de la liberté est essentiel pour motiver la confiance des consommateurs sur le marché Internet, tandis que les groupes de défense des droits de l'homme réclament une protection concernant les quantités de données personnelles aujourd'hui stockées électroniquement.

Les commerciaux mettent également l'accent sur le fait que l'information est susceptible de tomber en de mauvaises mains, en particulier dans les pays corrompus, dans les cas où les gouvernements auraient accès aux messages encryptés. " Si les gouvernements disposent des clés pour encrypter les messages, cela signifie que des personnes non autorisées, extérieures au gouvernement, peuvent les obtenir et s'en servir,", déclarait le PDG d'une grande société nord-américaine spécialisée dans la sécurité.

Stopper le crime mondial

Les défis qu'affrontent les responsables du respect de la loi, à travers le monde, mettent en évidence le besoin urgent d'une coopération mondiale, en matière d'actualisation des législations nationales, des techniques d'enquête, de l'assistance légale et de l'extradition, afin de suivre le rythme des cyber-criminels. Certains efforts ont déjà été déployés.

Le Manuel de l'ONU de 1997 engage vivement les nations à harmoniser leurs lois et à coopérer pour lutter contre ce problème. Le European Working Party on Information Technology Crime (EWPITC, le Groupe de travail européen sur les informations relatives au crime technologique) a publié un manuel sur le crime informatique, qui dresse la liste des législations pertinentes dans chaque pays et décrit les techniques d'enquête, de même que les moyens de chercher et de sécuriser le matériel électronique.

Le European Institute for Anti-Virus Research (EICAR, l'Institut européen de recherche pour la lutte contre les virus) regroupe le monde universitaire, l'industrie et les médias, de même que des experts techniques en dispositifs de sécurité, des spécialistes du respect de la loi et des organisations privées de protection pour lutter contre les virus informatiques ou chevaux de Troie. L'Institut travaille également dans le domaine de la lutte contre la fraude et l'exploitation de données personnelles.

En 1997, les pays du G-8 ont adopté une stratégie pionnière de lutte contre le crime technologique de pointe. Le groupe s'est entendu pour développer des moyens de repérer rapidement les attaques informatiques et d'identifier les pirates, en utilisant des liens vidéo pour procéder aux auditions de témoins transfrontaliers et s'entraider dans le domaine de la formation et des équipements. Il a également décidé de se joindre à l'industrie concernant la mise en place d'instituts à même de sécuriser les technologies informatiques, développer des systèmes d'information pour stopper les délits sur le réseau, rechercher les délinquants et rassembler les preuves.

Le G-8 a, à présent, mis en place des groupes de contact auxquels peuvent s'adresser les responsables du respect de la loi, 24 heures sur 24, sept jours sur sept. Ces groupes activent une enquête menée par un autre pays en fournissant des informations essentielles ou en aidant par le biais de procédures légales, telles qu'auditions de témoins ou regroupement des données informatiques, servant de preuves.

L'obstacle majeur à la mise en place au niveau international d'une stratégie du type de celle du G-8 est que certains pays ne disposent pas d'un savoir-faire technique ou d'une législation qui permettraient aux responsables du respect de la loi de rechercher rapidement les preuves dans le domaine électronique avant qu'elles ne se perdent ou de les déplacer dans un lieu où les délinquants sont mis à l'épreuve.

Réseau : les méchants

Espionnage industriel

Les pirates peuvent entreprendre des opérations sophistiquées d'espionnage pour des sociétés ou à leur compte, en copiant des données commerciales confidentielles, allant des stratégies marketing aux renseignements techniques ou sur des produits.

Sabotage des systèmes

Des attaques, tel les que le "bombardement de courriers", sont à même d'envoyer de façon répétitive des messages à une même adresse e-mail ou sur un même site Internet, empêchant les utilisateurs légitimes d'y accéder. Le flux d'e-mails est susceptible de surcharger le compte personnel du receveur et de détruire le système dans son ensemble. Une pratique si dangereusement préjudiciable n'est pourtant pas nécessairement illégale.

Sabotage de données et vandalisme

Les intrus accèdent aux sites Internet ou aux bases de données, endommageant, effaçant ou modifiant les données, altérant les données elles-mêmes et causant davantage de tort dans les cas où les données sont ensuite utilisées à d'autres fins.

" Pêcheurs ", " découvreurs " de codes d'accès

Les trafiquants trompent souvent les nouveaux utilisateurs ou les moins expérimentés en se faisant passer pour des responsables du respect de la loi ou des employés de leur service de connexion à Internet. Les "découvreurs" de code d'accès utilisent des logiciels pour découvrir l'identité des utilisateurs des codes d'accès, qui leur servira ensuite à se cacher sous leur nom et à commettre d'autres délits, qui peuvent aller de l'utilisation de systèmes informatiques confidentiels à des fins de crime économique, au vandalisme ou à des actes terroristes.

Parodie

Les individus qui pratiquent la parodie ont recours à diverses techniques qui leur permettent de déguiser un ordinateur afin que celui-ci prenne, électroniquement, l'apparence d'un autre ordinateur. Ils peuvent ainsi accéder à un système dont l'utilisation est normalement limitée et commettre des délits. Le pirate bien connu, Kevin Mitnick, a eu recours à cette technique de la parodie, en 1996, pour accéder à l'ordinateur personnel de l'expert en sécurité, Toutomu Shimomura, et communiqua ensuite, sur Internet, de précieuses données sécuritaires.

Pornographie à caractère pédophile

La circulation de documents pornographiques à caractère pédophile à travers le monde par le biais de l'Internet est en plein essor. Au cours des cinq dernières années, les inculpations, dans un pays d'Amérique du Nord, pour circulation ou possession de documents pornographiques à caractère pédophile sont passées de 100 à 400 par an. Le problème se trouve exacerbé par les nouvelles technologies, telles que l'encryptage, qui peut être utilisé pour dissimuler la transmission ou le stockage de documents pornographiques ou d'autres matériaux " choquants ".

Les jeux d'argent

Les jeux d'argent électroniques ont augmenté tandis que le commerce fournissait des moyens de contracter des crédits ou de transférer des fonds par Internet. Des problèmes ont vu le jour dans des pays où les jeux d'argent sont interdits ou dans les pays où le jeu ne peut se pratiquer sans licence. On ne peut garantir aux joueurs aucune partialité, étant donné les contraintes techniques et juridiques de contrôle du jeu.

Fraude

Des offres frauduleuses ont déjà été faites à des consommateurs dans différents secteurs du commerce électronique, tels que l'achat et la vente d'action ou d'obligation ou l'achat et la vente d'équipements informatiques.

Blanchiment d'argent

On pense que le commerce électronique est susceptible d'offrir de nouvelles opportunités au transfert électronique de biens et d'argent utilisé pour blanchir l'argent sale, surtout s'il est possible de dissimuler les transactions.

Liens : http://www.un.org/french/events/10thcongress/2088hf.htm

Le blanchiment des fonds de la cybercriminalité : cryptomarchés et cryptomonnaies

Si le cybercrime devient de plus en plus accessible, les gains – souvent financiers – demeurent difficiles à monétiser lors de leur passage du virtuel vers l'économie réelle et licite. Par contre, les monnaies numériques dont le développement soulève de nombreuses questions tant au niveau de leur utilisation que de la législation, peuvent-elles représenter de nouvelles opportunités pour le cybercriminel ?

L'essor des cryptomonnaies

Lors de cette dernière décennie, les systèmes de monnaies virtuelles se sont non seulement multipliés mais également imposés en tant que véritable devise avec un taux de change de plus en plus intéressant.

Au «cours» actuel, certaines de ces monnaies numériques vont de 2 euros l'unité (Litecoin, BanxShares, SuperNet, etc.) jusqu'à dépasser les 210 euros le Bitcoin qui est devenu l'une des cryptomonnaies les plus populaires et utilisées dans le monde depuis 2009.

Ces nouvelles méthodes de paiement, pensées initialement comme solution alternative et à des fins légales, s'accompagnent de nombreux services facilitant les transactions mais également renforçant l'anonymat de leurs utilisateurs.

Attractivité des devises virtuelles : cible et moyen

Alors que peu de juridictions reconnaissent ces monnaies virtuelles comme de réelles devises, et certains Etats en interdisent leur utilisation (Thaïlande, Russie, etc.), on assiste de plus en plus à l'émergence d'importants réseaux de change (ZipZap, etc.) mais également à l'apparition de distributeurs de monnaie similaires aux traditionnels ATM.

Pour les (cyber)criminels, les disparités légales en la matière, la polyvalence, la popularité et les taux de conversion intéressants font de ces devises virtuelles un moyen efficace d'échapper aux services de paiement traditionnels – déjà régulés – où les risques de détection sont plus importants.

Dès lors, la monnaie virtuelle peut être non seulement une cible de la cybercriminalité (vol, mining, etc.) mais également permettre de réaliser des transactions illicites (marchés noirs, etc.) et de blanchiments grâce à l'anonymat et aux vides juridiques actuels propres à ces devises.

Blanchiment d'argent : un processus délicat, de nouvelles solutions

Les cybercrimes ont souvent pour finalité un gain financier. Profiter du butin induit généralement une transaction financière. C'est précisément l'une des étapes les plus dangereuses pour le cybercriminel car le passage du virtuel au réel l'expose inéluctablement aux risques d'être identifié.

La cryptomonnaie combinée aux modes opératoires traditionnels de blanchiment d'argent offre aux (cyber)criminels de nouvelles opportunités d'échapper à la détection et aux poursuites judiciaires :

– Le recours au *commerce électronique licite* : dans le cas de petits larcins virtuels, les cybercriminels opèrent à travers l'achat de produits sur les e-commerces licites notamment via des paiements en monnaie virtuelle. Afin de minimiser la traçabilité, les produits sont acheminés vers des dropzones (intermédiaires logistiques) ou house drop (maison/appartement vides).

– Les *casinos en ligne* : à travers les dépôts/jeux/retraits, le cybercriminel peut transformer sa cryptomonnaie en argent réel mais également blanchir ces fonds en les changeant en gains. De plus, ces casinos/sites de jeux en ligne sont souvent situés

dans des pays offshore ou, à tout le moins, bénéficiant d'une législation financière plus légère faisant obstacle à toute remontée d'informations auprès des autorités financières et judiciaires.
– Le recours aux *«mules»* : les transactions bancaires sont souvent risquées puisque plus régulées. Afin de blanchir des gains illicites de manière sécurisée, les cybercriminels recourent le plus souvent aux mules. Ces intermédiaires sont enrôlés – de manière volontaire ou à leur insu (spam, fausses annonces d'emploi, etc.)– et ont pour mission de recevoir le butin illicite et de le transférer par la suite sur plusieurs comptes bancaires afin de blanchir les fonds du commanditaire ; les mules reçoivent en retour une commission significative qui contraste avec le peu de travail qu'ont nécessité ces opérations
Liens : https://tetedansleguidon.com/2015/11/16/le-blanchiment-des-fonds-de-la-cybercriminalite-cryptomarches-et-cryptomonnaies/

Les services de paiement digitaux et lutte contre le crime financier

La tendance grandissante du commerce sur internet et l'émergence de prestataires de services de paiement (PSP) non issus du secteur bancaire, conjuguées à l'évolution des moyens de transactions (tels que les bitcoins) comportent un risque de crime financier non négligeable.
En effet, à ce jour, les prestataires non bancaires ne sont pas soumis à des exigences réglementaire aussi lourdes que les banques, notamment en matière de lutte contre le blanchiment d'argent, de lutte contre le financement du terrorisme, d'embargos et de sanctions. Le défi est de taille pour les banques car elles doivent être capables d'identifier les titulaires bénéficiaires ou finaux de chaque relation établie. Elles doivent connaître les raisons pour lesquelles un compte est ouvert.
Dans le cas d'une banque correspondante, l'identification d'un titulaire bénéficiaire repose sur le fait que la relation est établie avec une autre banque. Toutes les banques sont soumises aux mêmes types de législations en matière de lutte contre le blanchiment d'argent et le financement du terrorisme ainsi qu'aux règles Know Your Customer. Dans le cas des banques correspondantes, les institutions travaillent avec des clients en qui elles ont une confiance absolue. La mise en place d'une collaboration avec de nouveaux PSP nécessite que les banques réajustent leur niveau de vigilance afin de garantir que le titulaire bénéficiaire de la relation est légitime et ne conduit pas d'activité susceptible d'enfreindre la législation en matière de lutte contre le blanchiment, le financement du terrorisme ou des sanctions. Les paiements effectués pour des prestataires de paiement tiers comportent un risque relativement élevé pour les banques dans la mesure où les PSP procèdent eux-mêmes à des paiements pour une tierce partie. A l'heure actuelle, il n'existe aucun cadre réglementaire à l'égard de ce qui est considéré comme une forte zone de risque pour les banques.
Les banques doivent avoir une parfaite confiance dans leurs relations avec les clients.
Les processus *Know Your Customer*
et *due diligence* forment les bases de la lutte contre le crime financier. Si ces derniers ne sont pas correctement suivis ou si les politiques et procédures ne sont pas régulièrement réévaluées, une banque peut être confrontée à d'importants défis en matière de réglementations liées à la lutte contre le blanchiment d'argent et les sanctions.

Heureusement, la situation devrait changer car les régulateurs ont pris conscience du problème. Des réglementations visant ces PSP seront déployées mais, dans cette attente, les banques ne peuvent pas uniquement se reposer sur des mesures externes pour être rassurées quant au développement de relations avec ces prestataires. En l'absence d'un cadre réglementaire, il revient par conséquent aux banques de s'assurer de la solidité de leurs processus KYC lors de l'établissement de nouvelles relations avec ces prestataires. Le programme d'approbation est un élément essentiel de ce processus. Il requiert un fort degré de vigilance pour garantir que tout revendeur d'un produit bancaire respecte un certain nombre de règles et que le contrat fait état de toutes les clauses protectrices.

Les banques doivent mettre en œuvre des politiques détaillées qui régissent l'approbation de ces nouveaux PSP. Elles doivent avoir une parfaite connaissance des types de services offerts par ces prestataires et connaître les profils de leurs clients. Des politiques et procédures doivent être déployées pour régir la relation et garantir le respect des exigences en matière de lutte contre le blanchiment d'argent, le financement du terrorisme et de KYC. Il est devenu essentiel, dans tous les aspects de la banque correspondante, de connaître le client final. Et par conséquent de connaître également le client de son client. Cela s'avère toutefois difficile lorsque le PSP intervient en tant qu'entité relativement anonyme.

Une fois l'approbation obtenue pour une relation, le compte doit être régulièrement surveillé afin de détecter toute activité suspecte ou illégale. Les banques doivent s'assurer que les flux d'entrée et de sortie de compte sont conformes aux volumes préalablement déclarés par le PSP. Les relations avec les PSP doivent également faire l'objet de revues régulières dans la mesure car elles sont considérées comme une forte zone de risque. La documentation doit être à jour et les politiques et procédures renouvelées. La technologie joue un rôle important et les outils de suivi des comptes permettent aux banques de détecter toute transaction suspecte.

Les programmes de conformité des banques ont été mis en place pour empêcher que des comptes ou produits soient utilisés dans le cadre de transactions illégales. Il est de notre devoir de nous assurer que ces comptes ne sont pas utilisés à des fins illégales. Le principe général de réglementation des banques veut que nous appliquions une approche centrée sur le risque à l'égard de nos clients et que nous déployions les politiques et procédures nécessaires.

Les banques seront moins réticentes à l'idée d'établir des relations avec des PSP tiers lorsque ces derniers seront soumis à des réglementations. Ces prestataires deviendront plus nombreux à mesure que le commerce sur internet se développe, et la mise en place de réglementations sera par conséquent inévitable.

Liens : https://www.societegenerale.com/fr/connaitre-notre-entreprise/responsabilite/maitrise-des-risques/les-services-de-paiement-digitaux-et-lutte-contre-le-crime-financier-1

Banques : Comment la blockchain va révolutionner la connaissance client.

La technologie derrière les monnaies virtuelles permettra aux acteurs bancaires de partager leurs informations sur les individus.

La blockchainisation du secteur de la finance est en marche. « Nous observerons les premiers usages à grande échelle sur certains marchés dans les deux ans à venir, assure Frédéric Dalibard, responsable du digital de la banque de grande clientèle

deNatixis, filiale du groupe BPCE. Et la technologie sera diffusée au plus grand nombre dans les cinq à dix ans. »
Déjà, les banques testent différentes blockchains et applications. A l'international, au sein du consortium R3, qui regroupe 42 acteurs. En France, grâce à l'initiative de la Caisse des Dépôts et Consignations, lancée en décembre dernier avec une quinzaine de partenaires. Et des applications concrètes se dessinent. A commencer par le KYC, acronyme de Know Your Customer, au coeur de la démarche des banques.

Le KYC, fondamental pour lutter contre la fraude

Le KYC est en effet l'un des grands chantiers sur lequel travaillent aussi bien R3 que l'initiative CDC. Cette démarche légale obligatoire à toutes les banques consiste à réunir des informations sur leurs clients pour mieux les identifier et se prémunir des usurpations d'identité, de la fraude, du blanchiment d'argent… « Le KYC est fondamental, assure Philippe Denis, CDO de BNP Paribas Securities Services. Sans KYC sur la blockchain, il sera compliqué d'y réaliser des échanges et transactions. »
Enregistrer les documents sur la blockchain pour éviter la redondance
Aujourd'hui, le processus de KYC est lourd et long : le client doit remplir des documents, la banque les vérifie et apporte la preuve de leur véracité, stocke et surveille les informations… Pour le simplifier, les acteurs bancaires étudient un moyen d'inscrire sur une blockchain infalsifiable et auditable les connaissances authentifiées des contreparties (papiers numérisés, signatures, vérifications…). « Une base de données partagée pourrait permettre aux banques et acteurs financiers de partager les documents de KYC en étant sûrs qu'ils sont légitimes et valides », décrit Frédéric Dalibard, de la banque de financement Natixis, membre du consortium R3. Une telle initiative engendrerait un gain de temps énorme en évitant à chaque banque d'effectuer le processus de vérification d'un client déjà effectué par une autre et réduirait aussi le risque réglementaire.
Le KYC ne serait ainsi plus centralisé au sein de chaque banque. « L'individu aura la main sur ses données dans un environnement distribué et il n'y aura plus de redondance des informations », décrit Philippe Denis. Par exemple, BNP Paribasinscrirait sur la blockchain qu'il a vérifié les documents de tel client et l'information pourra être connue par les autres banques. « Le client aurait accès à ses informations personnelles plus facilement, pourrait rajouter des documents au fil de l'eau, choisir quelles informations il souhaite partager avec tel ou tel acteur… », ajoute Nicolas Châtillon, directeur du développement chez BPCE. Reste à savoir quelle forme prendra le réseau et quels acteurs y participeront ensemble…26/05/2016
Liens : http://fr.wabiness.com/blog/fr/2016/05/26/banques-comment-la-blockchain-va-revolutionner-la-connaissance-client/

Malware Blackshades
50 perquisitions réalisées en France

UnderNews vous rapportait il y a quelques jours une vague d'arrestation de pirates informatiques en France. Une cinquantaine de perquisitions ont **été** menées dans le cadre d'une vaste affaire de piratage informatique dont l'enquête avait débuté aux États-Unis, liée au trojan bancaire Blackshades.
Les perquisitions, menées par des services spécialisés de la police judiciaire (PJ) chargée de lutter contre la cybercriminalité, ont visé de présumés possesseurs d'un

malware bancaire nommé "*Blackshades*", destiné au piratage bancaire à distance des victimes infectées.
Blackshades a été diffusé à grande échelle il y a environ trois ans sur des forums clandestins underground, surtout en Inde, en Grande-Bretagne et aux Etats-Unis. Fin 2012, à Tucson en(Arizona, selon les mêmes sources, le FBI avait mené une série d'interpellations car des données financières avaient été piratées par le biais de cet ingénieux programme malveillant. Le FBI avait poursuivi ses investigations sur ce logiciel "malveillant" et récemment alerté plusieurs pays, dont la France.
La Direction centrale de la PJ (DCPJ) a effectué plus de 50 perquisitions partout en France le 14 mai, opérations dont les résultats sont en cours d'analyse. Elles ont visé de présumés utilisateurs de Blackshades figurant sur une liste fournie par les Américains après l'interpellation d'un revendeur.
La DCPJ se dote progressivement d'une sous-direction spécialisée dédiée à la lutte contre la fraude informatique, les piratages, les dérapages sur les réseaux sociaux et tout ce qui relève de la cybercriminalité plus généralement afin de contrer un "phénomène en pleine expansion".
C'est donc bien une affaire de carding à l'échelle mondiale, dont les principaux instigateurs sont en train d'être mis hors d'état de nuire, y compris en France.
Liens : http://www.undernews.fr/malwares-virus-antivirus/malware-blackshades-50-perquisitions-realisees-en-france.html

La directive PSD2 provoquera l'un des plus importants bouleversements du secteur bancaire depuis des décennies

Alors que les autorités de régulation sont de plus en plus soucieuses d'assurer la protection des consommateurs, de nouveaux cadres réglementaires tels que la Directive révisée concernant les services de paiement (PSD2) contraignent actuellement les acteurs du secteur des paiements à repenser leur mode de fonctionnement dans un marché qui s'ouvre rapidement à de nouvelles formes de concurrence. En effet, face à l'apparition de nouvelles solutions de paiement digital, telles qu'Apple Pay, et à l'essor des services d'agrégation de comptes proposés par les fintechs, cette réglementation qui se trouve actuellement dans la phase ultime de négociation, entraînera des bouleversements et ouvrira la voie à d'autres changements encore plus significatifs.
La directive PSD2 constitue un prolongement de la première Directive sur les services de paiement (PSD) adoptée par la Commission européenne en 2007. L'objectif est de réguler les activités des prestataires de services de paiement et de créer un cadre harmonisé à travers toute l'Europe. Cette réglementation devrait accroître le nombre de prestataires au sein de l'écosystème et renforcer la concurrence, en vue de proposer aux consommateurs un choix élargi et une transparence accrue.
La directive précise que toute entreprise qui fournit et conserve des informations sur des comptes clients doit rendre ces dernières accessibles à des tiers, notamment à des prestataires de paiement mobile, sous réserve que le client leur en ait donné l'autorisation. Une telle mesure contraindra les banques à ouvrir à des tiers l'accès aux données de leurs comptes clients via des interfaces de programmation applicative (API). Pour les banques traditionnelles, une telle évolution entraîne à terme un danger important de désintermédiation, étant donné que de nouveaux acteurs pourront

accéder à une base de clientèle bien plus large. En réponse, les banques devront réinventer l'expérience paiement et devront trouver des moyens innovants pour fidéliser la clientèle : cela s'imposera comme un impératif stratégique. De plus, certains critères fondamentaux tels que la sécurité, la responsabilité en matière de défaillances et de fraudes, la connaissance du client (le « KYC ») et les contrôles de lutte contre le blanchiment d'argent (AML) gagneront en importance à l'heure où l'univers des paiements s'ouvre à de nouveaux prestataires.

Quelles conséquences pour les banques traditionnelles ?

Si la directive PSD2 entend éliminer les obstacles auxquels sont confrontés les nouveaux entrants sur le marché, elle implique aussi de règlementer les fournisseurs tiers (les « Third Party Providers » ou TPP) qui proposent des services de paiement. A l'instar des banques, ces derniers devront en effet satisfaire aux exigences imposées par PSD2, comme n'importe quel autre établissement de paiement (agréé, enregistré et contrôlé). Autrement dit, ils seront soumis à leurs propres exigences en matière d'information, de transparence et de sécurité des paiements.

Fournir une infrastructure sécurisée aux TPP constitue un défi majeur pour les banques. Elles doivent en effet créer un cadre pour le KYC et empêcher que la lutte contre le blanchiment d'argent ne gère les risques opérationnels liés aux incidents de paiements ou aux paiements frauduleux, ainsi que les risques pour la sécurité. C'est aux acteurs traditionnels qu'il reviendra de supporter la charge liée à la mise à jour des anciens systèmes pour répondre aux impératifs des paiements internationaux. À cet égard, la transparence et la sécurité accrues des données de paiement constituent des problématiques majeures. Mais, pour les banques, cette charge n'est pas simplement financière. La multiplication des fournisseurs tiers et des nouveaux entrants sur le marché des paiements pourraient également s'accompagner de pertes de recettes et impacter leurs marges. Compte tenu par ailleurs du règlement sur les commissions d'interchange de l'UE (visant au plafonnement de ces commissions), les modèles commerciaux traditionnels se trouvent donc soumis à une forte pression. Avec l'ouverture de la chaîne de valeur, il existe peut-être même de nouvelles opportunités liées à la désintermédiation du consommateur final, qui peut accéder à ses comptes via des outils tels qu'Appel Pay, sans avoir à traiter directement avec sa banque.

Comprendre le client, une condition sine qua non pour survivre

Le fait de savoir si les banques continueront à exister sous leur forme actuelle dans dix ans a alimenté de nombreux débats. En effet, l'émergence des technologies digitales et des autres technologies qui y sont associées, ainsi que l'évolution des préférences des clients, exercent une pression sur les structures et les méthodes de travail traditionnelles. Avec l'adoption de la directive PSD2, les banques seront contraintes de se métamorphoser au risque de rester à la traîne face à de nouveaux prestataires visionnaires et innovants, de tisser des relations plus étroites avec leurs clients et de développer de nouveaux flux de revenus. La tactique ne suffit plus ; les banques doivent adopter une approche stratégique différente si elles veulent conserver leurs clients et en attirer de nouveaux.

Le secteur bancaire est sur le point de connaître une mutation majeure engagée par la PSD2, qui encourage la concurrence et l'innovation dans les services financiers. La seule façon pour les banques de s'assurer que les agrégateurs ne leur dérobent pas de parts de marchés est de nouer des liens véritables, authentiques et émotionnels avec leurs clients. Autrement dit de revenir aux fondamentaux, de comprendre les besoins des consommateurs et de proposer à ces derniers des offres et des services de valeur leur permettant de réaliser plus simplement leurs opérations financières.

Liens : http://www.finyear.com/La-directive-PSD2-provoquera-l-un-des-plus-importants-bouleversements-du-secteur-bancaire-depuis-des-decennies_a36367.html

La révision de la Directive Services de Paiement (DSP2)

Le 24 juillet 2013, la Commission européenne a publié un paquet législatif comprenant, entre autres, une proposition de révision de la directive sur les services de paiement (DSP2)(1).

Ce nouveau cadre législatif modernisé doit permettre de prendre en compte les évolutions technologiques et les nouveaux usages apparus sur le marché des paiements depuis l'adoption de la DSP1 en 2007 (croissance continue du e-commerce, développement du m-commerce...).

La confiance, que les Français placent dans leur banque, repose sur la sécurité des moyens de paiement qu'elle met à leur disposition. Pour cette raison, les établissements bancaires investissent massivement et en permanence dans la sécurisation des moyens de paiement. Cette sécurité ne doit en aucun cas être remise en cause.

La proposition de révision de la DSP encadre de nouveaux acteurs

La DSP2 a pour objet d'encadrer juridiquement les nouveaux acteurs intervenant sur le marché des paiements en ligne, et non régulés à ce jour, les tiers de paiement (third party provider ou TPP). En proposant d'accorder un agrément à ces nouveaux entrants, la Commission européenne poursuit l'objectif d'accroître la concurrence et l'innovation sur ce marché.

La FBF approuve l'entrée dans le champ d'application de la DSP2 de ces nouveaux acteurs.

- La proposition de la Commission européenne va dans le sens de ce que la FBF a toujours souhaité : l'obtention préalable d'un agrément, délivré par une autorité compétente pour offrir de tels services, et la supervision de ces nouveaux acteurs à l'instar de tout prestataire de services de paiement.
- La FBF ne conteste pas non plus l'objectif visé par la DSP2 d'accroître la concurrence sur le marché des paiements.

Toutefois, la FBF s'interroge sur les modalités pratiques de mise en œuvre qui seront définies par l'Agence Bancaire Européenne (ABE) pour assurer la sécurité nécessaire au bon fonctionnement des moyens de paiements. Ces nouveaux entrants proposent, en effet, des services, qui nécessitent l'accès aux données bancaires de leurs clients.

La sécurité des paiements, un enjeu majeur pour les banques

Les banques sont responsables de la sécurité et de la protection des données de leurs clients. Celle-ci ne doit pas être amoindrie par l'émergence de nouveaux services. La FBF considère que la sécurité fait défaut dans la DSP2 à plusieurs niveaux :

- Les exigences prudentielles relatives à l'obtention par ces prestataires tiers de l'agrément d'établissement de paiement sont insuffisantes**.**
- L'accès aux comptes via les identifiants bancaires, pose un problème grave de sécurité. Cette manière de se connecter aux banques représente un risque systémique. De plus, elle remet en cause le message de sécurité transmis aux clients par leurs banques sur le caractère strictement confidentiel de leurs identifiants.
- Pour la FBF :

- Tous les acteurs des moyens de paiement doivent être soumis à un même niveau d'exigence sécuritaire concernant la sécurité des données et la supervision.
- Tous les acteurs des moyens de paiement doivent assumer les mêmes devoirs et bénéficier des mêmes droits.
- Les acteurs des moyens de paiement doivent se partager équitablement les responsabilités dans l'utilisation des données bancaires de leurs clients.

Définitions

- Les services d'agrégation d'informations permettent aux clients multibancarisés de bénéficier d'une vision consolidée de l'ensemble de leurs comptes sur une seule interface.
- Les services d'initiation de paiement permettent au client de demander à un tiers de présenter et d'exécuter des opérations de paiements aux banques en son nom

Liens : http://www.fbf.fr/fr/espace-presse/fiches-reperes/la-revision-de-la-directive-services-de-paiement-%28dsp2%29

Comment les banques peuvent-elles suivre la cadence imposée par les Fintech ?

Lorsque l'on demande à un « millénial » à quelle fréquence il se rend dans une agence bancaire ou téléphone à son conseiller, sa réponse est en général « jamais ». Les consommateurs passés à l'âge adulte au tournant du 21e siècle voient en effet la banque d'une façon différente des générations précédentes.

L'époque des clients fidèles est révolue : les consommateurs d'aujourd'hui recherchent une expérience de service agréable, des services numériques innovants à tarifs toujours plus attractifs. Un nombre croissant de consommateurs passent désormais à des services bancaires disponibles sur terminaux mobiles, Internet et objets connectés. La nouvelle directive européenne sur les services des paiements (PSD2) va dans ce sens pour ouvrir le marché à de nouveaux fournisseurs de services financiers et offrir de nouveaux services aux consommateurs. La banque de détail n'a plus d'autres choix que de se réinventer si elle ne veut pas se faire « uberiser » à son tour. La disparition des intermédiaires rendue possible grâce aux services numériques bouleverse en effet les modèles traditionnels de ces banques et offre de nouvelles opportunités dans l'économie des applications.

Croissance exponentielle des investissements

Les Fintech, ces start-ups de services financiers qui font frémir les banques, révolutionnent aujourd'hui tous les secteurs des paiements mobiles, des transferts de fonds, des prêts, des levées de fonds, et même de la gestion de patrimoine. Selon la société Accenture, les investissements mondiaux dans ces entreprises sont passés de 930 millions de dollars en 2008 à 12 milliards de dollars début 2015. C'est en Europe que ce taux de croissance a été le plus fort, avec une hausse de 215 % permettant d'atteindre 1,48 milliard de dollars en 2014.

Le classement annuel Fintech 100 de KPMG identifie également les entreprises du secteur financier qui ont su tirer parti des nouvelles technologies à leur avantage et bouleverser ce secteur.

Prêt d'Union, par exemple, est le premier établissement de crédit entre particuliers sur Internet en France. La banque berlinoise Number26 est en train de développer en

Europe le concept de « banque sans frontières ». Elle propose à ses clients de gérer un compte sur smartphone lié à une carte de crédit et a déjà lancé son service un peu partout en Europe. Ou encore Slimpay qui propose des alternatives à la carte bancaire et qui la rendra peut-être à terme totalement obsolète.

Une "force irrésistible"

Ces nouvelles sociétés de services financiers axées sur les nouvelles technologies agissent rapidement pour devancer le manque de réactivité des banques traditionnelles. L'ancien directeur de Barclays Bank au Royaume-Uni décrit ces nouvelles technologies comme une « force irrésistible » qui permettra d'améliorer le service client et voir émerger de nouvelles enseignes bancaires.

L'essor des Fintech doit effectivement être vu comme une formidable opportunité pour les banques de changer définitivement la façon dont elles proposent des services et des produits. Il ne suffit plus aujourd'hui de baser ses arguments de vente sur des horaires d'ouverture étendus ou sur un service de relevé de compte détaillé sur le web. Les clients veulent des services numériques innovants et une expérience plus complète et attrayante, que ce soit sur Internet, sur appareil mobile ou même par téléphone ou en agence.

Services en ligne innovants

Pour accompagner la transition vers ce modèle, les banques doivent s'appuyer sur des solutions leur permettant de planifier, construire, gérer et sécuriser ces nouvelles applications. Prenons l'exemple de la phase de planification d'un nouveau service : les Fintech mettent une pression immense sur les banques en lançant des services en ligne innovants avec des délais plus courts et des budgets réduits. La gestion de projet et de portefeuille aide les banques à faire face à cette menace en leur permettant de transformer la planification, l'exécution et la gestion d'activités critiques afin d'assurer la création d'applications innovantes pour leur métier.

Les logiciels peuvent également aider à développer de nouveaux services, comme « Pingit » de Barclays, qui permet d'effectuer des transactions sur des téléphones mobiles. Enfin, la mise en place d'une méthode intelligente et agile de développement de nouveaux services permet de réduire le délai de lancement d'innovations et de s'assurer que les nouveaux services sont axés sur les besoins des clients, y compris en les proposant à faible coût.

Les banques peuvent donc rivaliser en s'appuyant sur des logiciels optimisant le cycle de vie de leurs applications (la planification, le développement, les tests, le déploiement et la mise à jour des applications). Les banques peuvent ainsi proposer des services numériques disponibles 24h/7j, s'adaptant à la demande, et offrant la réactivité exigée par leurs clients.

Rendre les paiements plus sûrs

Les logiciels assurent aussi la sécurité des nouveaux services bancaires numériques en les protégeant des menaces internes et externes et en créant un climat de confiance facilitant la fidélisation des clients.

Enfin, les logiciels vont permettre aux banques de respecter la révision de la directive sur les Services de Paiement (PSD2) par la Commission européenne afin de normaliser le partage de services, de rendre les paiements plus sûrs, de renforcer la protection des clients et d'élargir leurs offres de services.

En utilisant les technologies logicielles adéquates, les banques ont l'opportunité de réagir et créer des services innovants pour fidéliser les clients nouvelle génération.

15/06/2016

Liens : http://www.latribune.fr/opinions/tribunes/comment-les-banques-peuvent-elles-suivre-la-cadence-imposee-par-les-fintech-578962.html

Banques : les américains craignent un Armageddon informatique dans la prochaine décennie

Signe des craintes des autorités américaines, le département du Trésor et les autres régulateurs fédéraux ont fait de la cyber-sécurité dans la finance une priorité, a indiqué Benjamin Lawsky, dont les services contrôlent les banques et assureurs opérant dans l'Etat de New York. « Nous craignons un Armageddon informatique dans la prochaine décennie, si ce n'est plus tôt, qui entraînerait une interruption longue du système financier. C'est ce que certains nomment déjà le '11-Septembre du Cyber«, *a* déclaré M. Lawsky, lors d'une conférence à l'université Columbia à New York.

Renforcer la sécurité

Pour éviter cette éventuelle « *attaque massive*« , le régulateur new-yorkais envisage de demander aux établissements financiers de mettre en place de nouvelles mesures de sécurité pour accéder à leur système informatique. Outre leurs noms d'utilisateurs et mots de passe, les employés des banques devraient par exemple répondre à une question supplémentaire envoyée par SMS à leur téléphone portable pour se connecter à leur écosystème professionnel.

Le régulateur veut également que les établissements financiers exigent de leurs fournisseurs de services qu'ils appliquent des mesures de sécurité identiques.

Attaques répétées

Enfin, Benjamin Lawsky, réputé pour être particulièrement dur avec les banques étrangères, comme la française BNP Paribas, a en projet de noter les systèmes de protection contre les attaques informatiques de ces dernières. « Nous n'éliminerons pas complètement le risque de cyber-attaque mais nous ferons tout ce qui est en notre pouvoir pour éviter qu'on se demande dans quelques années après un piratage dévastateur 'pourquoi ne l'avons-nous pas vu venir? Et pourquoi n'avons nous pas fait assez pour le prévenir?' », plaide M.Lawsky.

Ces craintes du régulateur new-yorkais interviennent après que des institutions financières et entreprises américaines ont été victimes d'intrusions dans leurs systèmes informatiques, avec vol des données de leurs clients. Dans plusieurs cas, les auteurs ont été soupçonnés d'être basés en Chine.

Source: RTLInternational

Liens : http://www.koldanews.com/2015/02/26/banques-les-americains-craignent-un-armageddon-informatique-dans-la-prochaine-decennie-a324409.html

Marketplaces et statut d'agent d'établissement de paiement. En quoi le choix du pays détermine votre liberté d'entreprendre ?

Afin de se mettre en conformité, les places de marché françaises s'orientent vers le statut d'agent d'établissement de paiement. On pourrait croire l'histoire close mais la France manifeste déjà la volonté de soumettre ses e-commerçants à des restrictions locales supplémentaires. Pour retrouver sa liberté d'entreprendre et son autonomie dans l'organisation de ses affaires, la solution passe peut-être par le passeportage depuis un établissement de paiement agréé dans un autre Etat européen.

Les services de paiement sous haute surveillance

L'Autorité de contrôle prudentiel et de résolution a présenté en fin d'année 2014 les règles prudentielles spécifiquement applicables aux établissements de paiement aux fins d'obtention et de conservation de l'agrément en France.

Entre autres points d'attention, l'Autorité Française mentionne le dispositif de gouvernance et de contrôle interne, le niveau de capital minimum et de fonds propres, la protection de la clientèle. Les établissements de paiement (EP) doivent disposer d'une comptabilité retraçant les mouvements liés à chaque opération de paiement. Des obligations somme toute légitimes et qui permettent au régulateur d'exercer ses contrôles dans les meilleures conditions.

La liberté d'entreprendre au sens de l'ACPR

Pourtant, cela ne semble pas suffire à l'ACPR pour délivrer l'agrément dont ont besoin les marketplaces pour se mettre en conformité.

Quand Myriam Roussille se demandait jusqu'où irait l'impérialisme de l'ACPR, se doutait-elle du caractère prophétique de sa note ? A priori, pas jusque-là et pourtant dans les faits, la France semble exiger des agents de ses établissements de paiement des mesures particulières. C'est notamment le cas en matière de gestion du compte de cantonnement et d'exécution des opérations de virement qui devraient être opérées non plus par l'agent lui-même, mais par l'établissement de paiement, sous peine de refuser de délivrer l'agrément.

Pourtant, au sens du code monétaire et financier, le prestataire de services de paiement mandant (l'EP) demeure pleinement responsable vis-à-vis des tiers, des actes de tout agent qu'il a mandaté et s'assure que ses agents se conforment en permanence aux dispositions législatives et réglementaires qui leur sont applicables. De là à passer d'un contrôle a priori à la gestion directe par un EP, il y a un fossé que l'Autorité française n'hésite pas à sauter. Combien de places de marché sont prêtes à abandonner à un établissement de paiement mandant leur liberté de gestion de leurs opérations.

Le passeport européen et sa contractualisation

La question se pose donc rapidement de savoir si un Etat membre de l'UE peut exiger ces mêmes limitations aux agents mandatés par un établissement de paiement dont le siège se situe dans un autre Etat membre.

La directive 2007/64/CE concernant les services de paiement dans le marché intérieur tend à renforcer la concurrence dans un secteur jusqu'ici monopolisé et à en conforter les effets. Pour cela, elle a introduit la notion de passeportage, autorisant un établissement de paiement agréé et régulé par l'autorité ad hoc du pays d'origine, à exercer sur le territoire d'autres Etats membres, par l'application du principe de reconnaissance mutuelle des agréments.

Une place de marché française peut ainsi bénéficier de cette procédure de passeportage en recourant à un établissement de paiement agréé en Europe. Après déclaration par l'EP à son autorité de contrôle de l'Etat d'origine, la place de marché est agréée en tant qu'agent de l'établissement (sous réserve d'un certain nombre de conditions relatives notamment à la lutte contre le blanchiment d'argent et le terrorisme) et peut fournir à son tour des services de paiement en Europe.

L'EP restant pleinement responsable des actes de ses agents, la relation entre lui et ses agents est formalisée par contrat. La procédure de KYC est assumée par les analystes financiers de l'EP dans la majeure partie des cas. Le contrat détaille en outre les procédures de supervision organisationnelles, comptables, informatiques et risques. Les dispositions européennes n'exigent pas des établissements de paiement qu'ils

prennent la main sur la gestion du capital, des fonds propres et du compte de cantonnement de leurs agents.

Le principe de coopération établit entre les Etats membres de l'UE permet-il à l'Etat d'accueil d'exiger au-delà des règles européennes ?

Prééminence de l'Etat d'origine dans la gouvernance financière de l'agent

En vertu de l'article 17 de la directive 2007/64/CE, l'autorité de l'Etat d'origine est seule compétente pour inscrire les agents d'établissement de paiement. Elle est également seule compétente pour surveiller et contrôler l'activité de l'EP et de ses agents.

L'article L612-2-III du code monétaire et financier dispose en outre que les autorités compétentes de l'Etat d'origine sont seules chargées notamment de l'examen de la situation financière, conditions d'exploitation, solvabilité et de la capacité à tenir à tout moment les engagements à l'égard des assurés, adhérents, bénéficiaires et entreprises réassurées.

Faut-il poursuivre ? Rajoutons qu'en France notamment, l'ACPR s'était engagée à ne pas discriminer les EP passeportés par des obligations ou des contrôles supplémentaires et l'on aboutit à vider de sa substance la volonté hégémonique de l'autorité administrative française.

Si les règles relatives à la lutte contre le blanchiment d'argent et le terrorisme sont d'une autre teneur et relèvent en grande partie d'une double compétence entre Etat d'origine et Etat d'accueil, l'ensemble des aspects relatifs à la situation financière, la solvabilité, les conditions d'exploitation et la capacité à tenir ses engagements sont de la compétence de l'autorité de l'Etat d'origine.

Par l'effet du principe de coopération, un Etat d'accueil peut être amené à contrôler le respect de ces obligations, voire à en sanctionner les manquements. En revanche, il ne dispose pas du pouvoir de modifier la relation contractuelle qui existe entre l'EP et son agent, dès lors que les procédures de contrôles en place ont été validées et respectent les conditions fixées par l'Etat d'origine.

La France confirme ainsi l'interprétation particulière qu'elle fait d'une directive Européenne, au seul détriment des entreprises françaises.

Les places de marché françaises ont donc intérêt à étudier le statut d'agent d'établissement de paiement dans l'Etat membre qui leur laissera le degré d'autonomie suffisant pour la conduite de leurs affaires.

Le Royaume-Uni et ses 323 établissements de paiement agréés contre une quarantaine en France, pour un total de 568 EP sur l'ensemble de l'espace économique européen, conforte sa position de terre d'accueil des services financiers.

A propos de NordPay Financial

NordPay Financial devient Établissement de Paiement en 2011, suite à la fusion des entités CentralPay et Paysite-cash, présentes sur le marché depuis 10 ans. Le groupe est aujourd'hui un acteur majeur du paiement en ligne en Europe, régulé par l'autorité des services financiers britannique (FCA) et autorisé par la Banque de France. A travers ses marques historiques Paysite-cash et CentralPay, NordPay Financial offre aux e-commerçants une gamme de services complète dédiée à l'optimisation des encaissements et à la régulation des places de marché. Sa solution de paiement en ligne par carte bancaire rassemble sur une interface unique, la gestion des encaissements multidevises, la détection des fraudes, ou encore SmartLink, le nouveau service de paiement par email/sms.

Présent dans de nombreux pays d'Europe (France, Royaume-Uni, Espagne, etc.), NordPay Financial traite les opérations e-commerce de plus de 10.000 marchands de l'Espace Economique Européen (EEE)

Liens : http://www.finyear.com/Marketplaces-et-statut-d-agent-d-etablissement-de-paiement-En-quoi-le-choix-du-pays-determine-votre-liberte-d_a33295.html

Swift : Le réseau banquier international fait face à une grosse attaque de hackers

Selon une lettre que Swift s'apprête à envoyer vendredi à ses utilisateurs, les méthodes de ces hackers présentent des similitudes avec l'attaque qui avait permis en février à des malfaiteurs de dérober 81 millions de dollars sur un compte de la Banque centrale du Bangladesh auprès de la Réserve fédérale à New York.

Le FBI soupçonne que les malfaiteurs de février avaient bénéficié de complicités internes, avait affirmé mardi le Wall Street Journal.

Le même jour, des hauts représentants de la Réserve fédérale de New York, de la Banque du Bangladesh et du système de paiement international Swift, se sont rencontrés à Bâle, en Suisse, pour discuter de cette fraude cybernétique.

L'attaque menée contre Swift -Society for Worldwide Interbank Financial Telecommunication- montre une véritable tentative pour obtenir un accès à ce système indispensable pour le fonctionnement du monde financier international, selon le texte que s'apprête à publier Swift, cité par le New York Times et le Wall Street Journal.

Cette fois-ci, l'attaque visait une banque commerciale dont elle ne donne pas le nom, et dont les malfaiteurs ont réussi à s'approprier les codes pour envoyer des messages au nom de la banque.

En février, des messages semblant provenir de la Banque du Bangladesh avaient ordonné le transfert vers différents comptes aux Philippines de 81 millions de dollars.

Les méthodes utilisées par les hackers dans ces deux cas « montrent clairement une connaissance approfondie et sophistiquée des opérations de ce type dans les banques visées », selon la lettre de Swift, toujours citée par les journaux. Mai 13, 2016.

Source: RTLInternational

Liens : http://www.koldanews.com/2016/05/13/swift-le-reseau-banquier-international-fait-face-a-une-grosse-attaque-de-hackers-a539130.html

Paiements internationaux : Swift prépare sa mue 2.0

La messagerie bancaire sécurisée s'engage à effectuer les transferts d'argent internationaux en un jour d'ici un an. 21 banques expérimentent de nouveaux processus d'échanges entre elles.

Le système de messagerie bancaire sécurisée Swift prend le taureau par les cornes. La coopérative de banques et d'institutions financières, dont l'infrastructure est utilisée par près de 11.000 membres dans quelque 200 pays pour garantir l'échange de données financières réalisé lors d'un paiement ou d'un achat de titres, a décidé de « *réinventer les paiements internationaux sur la base de nouveaux standards* ». Elle a lancé pour ce faire en décembre dernier un plan baptisé « Global payment innovation initiative » auquel se sont ralliées 45 banques fin janvier.

Sur ces 45 établissements qui couvrent 67 % des échanges transfrontaliers traités par Swift, 21 lancent un pilote qui doit d'ici l'automne faire la preuve que le réseau de banques correspondantes de la messagerie, vieux de près de 45 ans , reste pertinent et compétitif face à de nouveaux entrants.

Les chiffres clefs

45 institutions financières se sont engagées à adopter de nouvelles règles d'échanges à partir de 2017.

67% des paiements internationaux traités par Swift devraient alors être réalisés en un jour.

En pratique, les établissements participants s'engagent à ce qu'un transfert d'argent par une grande entreprise cliente, fait au sein du réseau international des banques pilotes, soit crédité en un seul jour ouvré. C'est en effet là que le bât blesse : une opération qui transite via Swift prend aujourd'hui au minimum trois jours et le délai peut aller jusqu'à neuf jours selon la complexité du transfert. Ce, sans que le client ne soit informé sur l'état d'avancement de l'opération ni assuré du délai exact pour que l'argent transféré le soit réellement, ni qu'il soit sûr du coût précis de l'opération. Ces incertitudes sont devenues incompréhensibles voire intolérables dans un monde où l'instantanéité est devenue la norme. Elles font d'ailleurs le succès de nouveaux acteurs comme Transferwise ou Paypal.

Plan stratégique

« La messagerie Swift n'est pas du tout en cause, ce sont les pratiques des banques du réseau en matière de transfert qui doivent être réinventées », souligne Thierry Chilosi, responsable Market initiatives chez Swift. Autrement dit le fonctionnement du réseau de banques correspondantes chargées d'acheminer le transfert doit être sérieusement dépoussiéré et c'est ce à quoi se sont engagés les 21 établissements du pilote via un corpus de nouveaux accords de services multilatéraux proposés par Swift. Cet ensemble de règles devra être validé à la conférence annuelle Sibos organisée par la messagerie internationale à Genève fin septembre, avant d'être étendu aux 45 banques volontaires en 2017.

En parallèle Swift va lancer en mai une réflexion afin de définir une stratégie à cinq ans sur la manière dont la messagerie peut intégrer de nouvelles technologies afin d'améliorer la qualité et le coût de son service. Cela étant, Swift ne craint pas d'être balayé par des innovations comme la Blockchain qui permet de valider des transactions sans passer par un tiers de confiance. « *La technologie ne suffit pas, elle permet d'adresser la question du transfert lui-même mais pas tout ce qui tourne autour et notamment les sujets liés à la lutte contre le blanchiment* », prévient Stanley Wachs, directeur international de l'innovation dans les paiements chez Swift. 14/03/16

Liens : http://www.lesechos.fr/finance-marches/banque-assurances/021765608971-paiements-internationaux-swift-prepare-sa-mue-20-1206874.php

Conséquence de l'interruption du réseau SWIFT en Iran

Répondant aux injonctions européennes dans le cadre des sanctions internationales relatives à la conduite de la recherche d'armement nucléaire, la société SWIFT bloque depuis mi-mars les transactions en provenance ou en direction de la plupart des institutions financières iraniennes. Tony Wicks, expert en Blanchiment d'Argent chez NICE Actimize, répond à trois questions de Finyear pour donner à apprécier le cadre et expliquer pourquoi le blanchiment d'argent va se développer :

Tony Wicks

Pourquoi est-ce que l'action de SWIFT favorise le développement du blanchiment d'argent ?

L'action de SWIFT entraine depuis le samedi 16 mars l'impossibilité pour 25 institutions financières iraniennes d'envoyer et de recevoir des transactions, des titres et des échanges commerciaux au travers de son réseau SWIFT. Chaque année, ce sont près de dix milliards d'échanges qui transitent via SWIFT et une petite fraction d'entre eux, de l'ordre de 0,03%, provient ou est adressée à des banques en Iran. Cette fraction peut sembler minime, mais dans l'environnement actuel des sanctions, elle a une importance significative.

Le blocage du réseau SWIFT est possible parce que la société est basée en Belgique et par conséquent dans l'obligation de suivre le régime de sanctions déterminées par l'Europe. Cela a une incidence non seulement sur les sociétés européennes mais également sur les transactions avec les principaux acheteurs de pétrole brut en Inde, en Corée du Sud, en Afrique du Sud et en Chine. La position européenne a donc des effets extra-territoriaux évidents. Son impact est supérieur en termes d'effets que les récentes sanctions et restrictions européennes sur l'importation de pétrole. Si la Chine veut continuer à en acheter, elle sera confrontée à une grande difficulté pour payer !

Sans canal légal de transferts de fonds, les gestionnaires de fonds iraniens vont devoir se reporter vers un système bancaire alternatif, illégal, dit Shadow banking (dérivé du Hawala Banking) et emprunter de nouvelles méthodes commerciales.

Quels sont les meilleurs moyens pour blanchir de l'argent ?

Dans ce contexte, l'argent va circuler par le biais de méthodes commerciales informelles, via des chaînes complexes d'intermédiaires. Pour mémoire, à la suite des attaques terroristes de 2001, SWIFT a été invité à fournir des informations sur certaines transactions au gouvernement américain dans le cadre du Programme Terrorist Finance Tracking. Ironiquement, le blocage des transactions aujourd'hui va rendre plus difficile la connaissance approfondie de la prolifération des activités et le canal emprunté qui étaient auparavant observables. Les transactions qui vont passer en Shadow Banking disparaîtront purement et simplement des radars.

Si des mouvements d'argent s'évanouissent dans le Shadow Banking ; ils doivent tout de même réapparaître dans le système financier à un moment ou à un autre via des centres d'affaires ou des institutions. Il convient dans ce cas d'être très attentif aux changements de volumes d'activités, en particulier chez les états limitrophes de l'Iran

Les banques et les régulateurs rechercheront les variations inhabituelles dans les nouvelles transactions sur les réseaux financiers. Il est assez vraisemblable en outre que les exportations de pétrole iranien se règlent avec des moyens de paiement physiques et via du blanchiment d'argent basé sur des échanges indirects. Cela sera beaucoup plus difficile à repérer.

Quel sera l'impact sur les banques européennes ?

De nombreuses institutions accueillent avec soulagement la clarté que ce changement implique et seront plus rassurées en sachant que les transactions sur le réseau SWIFT ne pourront plus provenir ou être reçues par des institutions iraniennes. La modification réduit également la probabilité de voir des transactions redirigées, masquées, ou de constater des champs du message de paiement effacés. Dans l'absolu, cela ne change pas l'obligation des institutions d'appliquer des contrôles et des sanctions – d'autant que les entités iraniennes sur les listes n'agissent pas seulement à l'intérieur de l'Iran. Certaines d'entre elles sont à présent contraintes de chercher de nouveaux canaux pour déplacer les fonds à l'intérieur ou à l'extérieur de l'Iran, pour qu'il n'y ait aucun relâchement dans les contrôles et sanctions actuels. Il sera en réalité plus difficile d'identifier les entités sous le coup de sanctions quand

elles effectueront des paiements à partir des pays limitrophes. Elles continueront de dissimuler leur véritable identité et emprunteront les voies du Shadow Banking (comme le Hawala banking) plutôt que les canaux financiers traditionnels.
Liens : http://www.finyear.com/Consequence-de-l-interruption-du-reseau-SWIFT-en-Iran-Tony-Wicks-NICE-Actimize_a22590.html

SWIFT | Professionnels de la finance : garder en tête la blockchain

Les directives sur les services de paiement et la lutte anti-blanchiment relèvent les défis de la réglementation des tiers prestataires de services de paiement
Une nouvelle recherche universitaire du SWIFT Institute analyse les dernières réglementations sur les paiements, qui identifie des lacunes et des conséquences, et présente des recommandations afin d'aider à clarifier les nouvelles politiques.
SWIFT Institute annonce la disponibilité d'une nouvelle recherche qui analyse la régulation des tiers prestataires de services de paiement et des monnaies virtuelles.
Intitulé "The evolution of third party payment providers and cryptocurrencies under the European Union's PSD2 and AMLD4", ce document évalue de manière critique la législation en vigueur et les initiatives législatives en cours pour les tiers prestataires de services de paiement. Il met également en évidence le potentiel de réglementation des crypto-monnaies en termes de lutte contre le blanchiment d'argent et le financement du terrorisme.
L'étude met l'accent sur les développements réglementaires au sein de l'UE, notamment les directives PSD2 (Payment Service Directive) sur les services de paiements et AMLD4 (Fourth Anti-Money Laundering Directive) sur la lutte contre le blanchiment d'argent. Elle comprend également un point de vue étendu sur les marchés nord-américains et asiatiques.
« Au cours de la dernière décennie, l'influence des nouvelles technologies et des méthodes de communication a considérablement changé le paysage financier » indique Peter Ware, Directeur du SWIFT Institute. « Partout dans le monde, de nouveaux cadres juridiques ont été adoptés afin de réglementer les acteurs autres que les établissements de crédits. Cependant, ces cadres juridiques manquent encore de clarté concernant deux nouveaux types d'acteurs : les tiers prestataires de services de paiement et les monnaies virtuelles ».
Selon l'étude, les tiers prestataires de services de paiement permettent aux consommateurs de réaliser des paiements en ligne sans avoir besoin de recourir à une carte de crédit, en établissant « un lien entre le payeur et le commerçant en ligne via le module bancaire en ligne du payeur ». Le consommateur n'a pas besoin d'ouvrir un compte directement chez eux. A la place, ces tiers rassemblent des informations sur les comptes existants des consommateurs et présentent ces informations de manière intégrée. Ils fournissent une passerelle à partir de laquelle les clients se connectent à leurs comptes bancaires en utilisant leurs références et identifiants uniques. En agissant de la sorte, ces tiers arrivent à acquérir un nombre important d'informations sensibles.
Les monnaies virtuelles sont majoritairement utilisées dans les systèmes de paiement qui ne reposent pas sur les acteurs traditionnels tels que les banques et les fournisseurs de services de paiement. L'exemple le plus notable est celui des devises cryptées – comme le bitcoin – qui sont décentralisées et ont recours à des pseudonymes pour leurs transactions.

L'étude conclut que même si les directives PSD2, AMLD4 et autres réglementations sont un pas dans la bonne direction, certains aspects restent à éclaircir et nécessitent davantage d'attention. Par conséquent, le rapport propose des recommandations aux organismes de réglementation et aux professionnels de la finance.

Recommandations pour les organismes de réglementation :

1. Eclaircir les ambigüités qui subsistent
2. Harmoniser le cadre législatif de l'Union européenne
3. Coordonner les initiatives réglementaires internationales
4. Eviter une approche locale concernant les monnaies virtuelles
5. Adopter une perspective rationnelle sur les monnaies virtuelles

Recommandations pour les professionnels de la finance :

6. Regarder au-delà des forces disruptives
7. Nécessité de conformité
8. Ne pas systématiquement rejeter les monnaies virtuelles
9. Garder en tête la Blockchain

Les recherches ont été entreprises par Nathan Van De Velde, Niels Van De Zande et Peggy Valcke de l'Université belge KU Leuven et ont récemment été présentées lors de la conférence annuelle SIBOS de SWIFT à Singapour.

NOTES

La Directive relative aux services de paiements (PSD2), adoptée par le Parlement européen en octobre 2015 est une législation de l'Union européenne qui améliore la protection des consommateurs, favorise l'innovation et augmente la sécurité des services de paiement.

Le quatrième Directive anti-blanchiment (AMLD4), qui a finalement été adoptée en mai 2015, fait partie d'un ensemble de mesures visant à empêcher l'utilisation du système financier à des fins de blanchiment de capitaux ou de financement du terrorisme.

A propos du SWIFT Institute

Lancé en avril 2012, le SWIFT Institute encourage la recherche indépendante afin d'étendre la compréhension des pratiques actuelles et des futurs besoins au sein du secteur financier. Dirigé par SWIFT, et travaillant en étroite collaboration avec des professeurs de grandes universités internationales, le SWIFT Institute rassemble l'industrie financière et les universitaires afin de partager des connaissances et d'engager des réflexions sur des importants à l'échelle mondiale. Les recherches couvrent différents aspects des transactions bancaires et incluent les domaines suivants : paiements, systèmes de compensation et de règlement, cash management, trade finance, trust et titres

www.swiftinstitute.org.

À propos de SWIFT

SWIFT est une société coopérative qui permet aux membres de son réseau d'échanger des informations financières standardisées et automatiques de manière sûre et fiable, et, dès lors, de réduire les coûts, de limiter les risques opérationnels et de supprimer des processus opérationnels inefficaces. Plus de 10 800 organismes bancaires, établissements financiers, institutions et entreprises dans plus de 200 pays bénéficient des produits et services et de l'expertise de SWIFT et de sa plateforme de communication sécurisée unique au monde. SWIFT assure l'échange sécurisé de données propriétaires en garantissant confidentialité et intégrité. SWIFT facilite également le rapprochement des acteurs de la communauté financière pour élaborer ensemble des pratiques de marché, définir des standards et envisager des solutions

aux questions d'intérêt commun. En utilisant SWIFT, les clients peuvent bénéficier d'un large panel de solutions métiers et optimiser la gestion des flux financiers.
Liens : http://www.finyear.com/SWIFT--Professionnels-de-la-finance-garder-en-tete-la-blockchain_a34775.html

Le projet de loi de finances 2016 menace les logiciels libres de comptabilité

Le projet de loi de finances 2016 qui est en passe d'être voté par l'Assemblé nationale contient un article qui pourrait venir remettre en cause certains logiciels libres. L'article 38 prévoit que tout logiciel chargé d'enregistrer des règlements de clients doit être, non seulement sécurisé, mais aussi inaltérable :
Lorsqu'elle enregistre les règlements de ses clients au moyen d'un logiciel de comptabilité ou de gestion ou d'un système de caisse, utiliser un logiciel ou un système satisfaisant à des conditions d'inaltérabilité, de sécurisation, de conservation et d'archivage des données en vue du contrôle de l'administration fiscale.
L'objectif de l'administration fiscale est très clair : il s'agit de s'assurer qu'on ne peut pas tricher en enregistrant de mauvaises sommes, ou bien en oubliant dans sa caisse ou dans son logiciel de comptabilité. C'est l'un des aspects de la lutte contre la fraude fiscale, mais cet article signifie aussi que l'on ne peut plus utiliser de logiciel libre dans le domaine.
En effet, l'outil informatique qui sert à enregistrer une commande doit être inaltérable. Or, par définition, les logiciels open-source sont altérables, puisque l'on a accès au code source. En théorie, n'importe quel fraudeur pourrait modifier le code et faire en sorte que les sommes enregistrées ne correspondent pas à la réalité. La France n'est pas le premier pays à le faire : en Belgique par exemple, les commerçants sont obligés d'utiliser des caisses munies de boîtes noires qui enregistrent toutes les activités.
L'idée serait de faire en sorte que les logiciels disposent de telles boîtes noires. L'administration française doit pouvoir s'assurer que le logiciel soit digne de confiance… et les logiciels libres sont explicitement dans le viseur. Plus qu'une interdiction, la solution pourrait passer par l'ajout de code fermé pour former une boîte noire autour des logiciels libres. Ce qui serait contraire à l'esprit de l'open-source, mais aussi à la licence de bon nombre de ces logiciels libres.
Ce problème assez technique n'a pas retenu l'attention des parlementaires, qui comptent bien voter la loi et la faire appliquer en 2018, voire dès 2017. Les éditeurs de logiciels de comptabilité fermés ont d'ores et déjà fait savoir qu'ils étaient prêts… il faut dire que c'est bien dans leur intérêt ! Rappelons que ne pas diffuser la source d'un logiciel ne suffit pas à garantir son inaltérabilité : il existe de nombreux moyens pour modifier n'importe quelle application, comme le montre le piratage de certains logiciels.
Au-delà des logiciels de comptabilité, ce projet de loi concerne aussi les outils d'encaissement sur internet. Et dans ce domaine, comme souvent, les plus gros acteurs sont open-source : PrestaShop, Magento ou encore WooCommerce (module WordPress), par exemple, sont tous libres. Seront-ils tous interdits en France ?
Liens : http://www.macg.co/logiciels/2015/12/le-projet-de-loi-de-finances-2016-menace-les-logiciels-libres-de-comptabilite-92237

Bientôt la fin du chèque ?

Dans le cadre de loi Sapin 2, l'Assemblée Nationale a voté le 10 juin, un article qui réduit de moitié la durée de validité d'un chèque. Elle passera donc d'un an à 6 mois.
A compter du 1er juillet 2017, la durée de validité d'un chèque passera à 6 mois en France au lieu de 12 auparavant. Par cette mesure, le gouvernement entend encourager des modes de paiements rapides et sécurisés (cartes, prélèvements ou virements). Le chèque est de moins en moins accepté dans les commerces physiques.
Le circuit d'encaissement d'un chèque est parfois un peu compliqué, avec des risques de pertes, des vérifications interminables en caisse et surtout des risques d'impayés. Il reste pourtant un moyen de paiement plébiscité par les Français pour régler des dépenses courantes comme la cantine, les cotisations aux activités sportives ou de loisirs.
Selon les statistiques de la Banque centrale européenne, en France, 13 % des paiements ont été effectués par chèque en 2014. Les Français en utilisent 37 par an en moyenne, contre 11 en Angleterre et moins d'un en Allemagne. Ce moyen de paiement risque pourtant à terme de disparaître totalement.
N'est-il pas souhaitable de développer des moyens de paiement électroniques afin d'établir en permanence une traçabilité ? Cela permettrait aussi de lutter plus efficacement contre le blanchiment d'argent et le développement de l'économie souterraine. Le recours à l'argent liquide est aussi de plus en plus limité. Depuis le 1er septembre 2015, le plafond de paiement en espèces dans les commerces est passé de 3000 à 1000€. Le paiement sans contact pour les règlements de moins de 20€ se généralise par ailleurs. 14 juin 2016
Liens : http://www.ceriseclub.com/actualites/2016/06/14/23346/bientot-la-fin-du-cheque.html

Des hackers perdent un milliard de dollars en raison d'une faute d'orthographe

En février, la Banque centrale du Bangladesh s'est vu dérober quelque 80 millions de dollars. Elle aurait pu perdre davantage sans la faute de frappe de ses braqueurs.
Une petite faute d'orthographe dans un ordre de virement bancaire a permis d'éviter un braquage de près d'un milliard de dollars (900 millions d'euros) impliquant la Banque centrale du Bangladesh, révèle le quotidien britannique *The Guardian*. Les voleurs ont néanmoins réussi à s'enfuir avec quelque 80 millions de dollars (72 millions d'euros) indique le quotidien britannique.
Fausse "foundation". Le mois dernier, un groupe de pirates aurait réussi à violer le système de la Banque du Bangladesh avant de lancer trois douzaines de demandes de transfert vers des entités factices aux Philippines et au Sri Lanka, notamment vers une pseudo "Shalika Foundation". Si les braqueurs ont réussi à subtiliser près de 80 millions, un dernier virement à hauteur de 20 millions (18 millions d'euros) a néanmoins échoué car ceux-ci ont écrit "fandation" au lieu de "foundation", éveillant les soupçons d'un organisme de routage. Celui-ci a rapidement mis le doigt sur la supercherie et fait stopper les transferts.
Une attaque non élucidée. La Banque du Bangladesh a déclaré avoir récupéré une partie du butin, et travaillerait avec les autorités de lutte contre le blanchiment

d'argent aux Philippines pour recouvrir le reste des sommes dérobées par les hackers. Mais, à ce jour, la manière dont ces derniers ont pu s'introduire dans le système reste toujours un mystère, précise le *Guardian*. 11 mars 2016,

Liens : http://www.europe1.fr/international/des-hackers-aurait-pu-voler-1-milliard-de-dollars-sils-navaient-pas-fait-une-faute-dorthographe-2690758

Une société promet des virements internationaux sans frais bancaires

Un cauchemar pour les banques? Une société estonienne lancée par des concepteurs de Skype et Paypal réinvente les transferts d'argent en mettant en relation des personnes ayant des besoins de change complémentaires. Frontaliers, ne pas s'abstenir Vous en avez assez de payer des frais bancaires sur vos virements internationaux? TransferWise, un nouvel outil internet lancé par deux Estoniens passionnés de hightech, permet d'effectuer ce type d'opérations sans passer par les banques.

«Adieu les banques, vous avez fait votre temps!», raille le site internet fondé par Taavet Hinrikus et Kristo Kaarmann, 31 et 32 ans, spécialistes des systèmes d'appels internet gratuits Skype et de paiement en ligne Paypal.

TransferWise, lancé en janvier 2011 et dont l'utilisation est facturée 1 livre sterling (1,2 euro) pour tout transfert d'argent jusqu'à 230 euros (0,5% au delà), a déjà généré 60 millions d'euros de chiffre d'affaires et la croissance est de 20% par mois, assurent-ils.

Les virements internationaux suscitent des frais bancaires compris généralement entre 3% et 6%, avec des taux de change arrondis en faveur des opérateurs.

TransferWise a des clients dans toute l'Europe et plus particulièrement en Grande-Bretagne, en France et en Espagne, selon ses dirigeants.

Hinrikus était le directeur de la stratégie de Skype jusqu'en 2008. Kaarmann était consultant pour les cabinets d'audit Deloitte et PricewaterhouseCoopers avant de lancer TransferWise.

L'idée leur est venue alors que Hinrikus vivait à Londres et réglait ses dépenses en livres mais était payé en euros par Skype, société basée dans son Estonie natale. Kaarmann de son côté était payé en livres à Londres mais il remboursait sa maison en euros à Tallinn.

«Nous avons constaté que nous avions des besoins de change complémentaires et nous avons commencé à changer de l'argent entre nous au taux médian du marché -- le taux que vous trouvez dans les journaux, pas le taux majoré que vous propose votre banque», dit Hinrikus à l'AFP.

«On s'est rapidement rendu compte qu'on économisait une fortune en évitant les virements internationaux et on s'est dit que ce serait peut-être une bonne idée commerciale. C'est ainsi que TransferWise est né», ajoute-t-il.

Une idée toute simple

Le système consiste à relier des gens ayant des besoins de change complémentaires.

Ainsi, un client en Grande-Bretagne qui veut envoyer de l'argent chez lui en Estonie peut mettre des livres sur un compte TransferWise, explique Hinrikus. La société recherche alors un client en Estonie qui a besoin de faire la même opération en sens inverse et l'invite à déposer ses euros sur TransferWise, ajoute-t-il.

Au lieu d'envoyer l'argent d'un pays à l'autre, TransferWise verse à chaque client le montant demandé converti en livre ou en euro au taux de change médian du marché à un coût très réduit.

Mais le système ne pourrait-il pas être détourné pour blanchir de l'argent?
Donata Huggins, porte-parole de TransferWise, assure que ce service a reçu l'approbation de la Financial Services Authority (FSA), l'organisme chargé de la réglementation de l'industrie des services financiers au Royaume-Uni.
Ce qui signifie qu'il est soumis aux mêmes règles commerciales que les banques au Royaume-Uni. «Les fonds de nos clients sont placés sur des comptes séparés des comptes bancaires d'affaires», précise-t-elle.
TransferWise emploie 25 salariés et a reçu environ 1 million d'euros d'investissments provenant de différentes sources, comme le fondateur de Paypal, Max Levchin et l'homme d'affaires français Xavier Niel, co-actionnaire du quotidien Le Monde et patron de Free.
Liens : http://www.letemps.ch/no-section/2013/02/16/une-societe-promet-virements-internationaux-frais-bancaires

En finir avec les banques dans 10 ans ?

Aujourd'hui, grâce à la révolution numérique, chacune des fonctions qu'une banque remplit actuellement peut être faite plus vite, de façon plus efficace et sans intermédiaire central en utilisant les technologies numériques.
Le transfert d'argent n'a de nos jours plus besoin d'un établissement bancaire centralisé**.** Des applications comme Abra ou, pour les échanges monétaires en devises, Transferwise permettent de répondre à des problématiques complexes de façon élégante, simple et décentralisée, en concurrence. Et les banques ne pourront pas fournir un service équivalent sans changer profondément de métier.
Les habituels services de gestion de compte sont, eux aussi, appelés à évoluer bien au-delà des « home-bankings » proposés par les banques historiques. Mint en est un exemple assez flagrant qui propose de rassembler en un point unique tous les comptes et toutes les opérations bancaires pour les présenter de façon efficace sur différents supports. Dans la même veine, chacune des start-ups présentées dans cet article de Capital illustre une façon de se passer de la banque traditionnelle ou d'en contourner les services.
Mais plus important encore, les cryptomonnaies, Bitcoin en tête, représentent la révolution fondamentale qui donnent toutes les briques de base nécessaires à la remise en question complète du concept même de banque. Bitcoin, déjà évoqué de nombreuses fois dans ces colonnes, se passe de tout point centralisateur tel que le serait une banque. En outre, là où tout échange monétaire nécessite actuellement un tiers de confiance (joué par le système bancaire dans l'écrasante majorité des cas), Bitcoin propose un système fonctionnant sans tiers de confiance : les transactions sont infalsifiables, non répudiables, et définitives.
On peut arguer de la grande volatilité des cours de Bitcoin pour ne voir dans cette innovation technologique qu'un gadget amusant et voué à l'échec, mais la réalité est que cette cryptomonnaie est une excellente preuve de concept par l'exemple : oui, une cryptomonnaie peut fonctionner sans tiers de confiance ni système bancaire, oui, des transactions commerciales peuvent être menées en l'utilisant, et oui, le marché peut arriver, seul, à déterminer la valeur et la pérennité de cette monnaie sans l'intervention d'un *Deus Ex Machina* ou d'une banque centrale politisée. On comprend que ces caractéristiques rendent particulièrement moites les mains de banquiers, de politiciens ou même de syndicalistes.

Et très concrètement, Bitcoin aura permis l'émergence d'un bouillonnement de projets dans le domaine, visant à répondre à différentes problématiques monétaires et bancaires. Outre des variantes plus ou moins sérieuses de cryptomonnaies, on trouve différentes initiatives de regroupement de briques technologiques (cryptomonnaie, système de paiements, plate-forme de trading, …) comme par exemple SuperNet, plate-forme d'échange en pair-à-pair (sans centralisation, donc).
Comme on le voit, on assiste au développement de plus en plus rapide d'organisations autonomes fortement distribuées, qui se passent très bien de toute permission d'un État pour effectuer les transactions, et qu'empêcher, réguler ou encadrer s'avérera impossible (ou trop coûteux), par la nature même de ces innovations. En outre, les voitures à chevaux n'ont pas évolué avec des chevaux plus rapides. Les abaques ne sont pas devenus électriques. Les banques telles qu'on les connaît n'évolueront pas en réseaux décentralisés, elles seront remplacées**.**
Et si les révolutions précédentes (depuis les appareils photos numériques jusqu'aux biotechnologies en passant par l'impression 3D) sont un indicateur du rythme auquel on doit s'attendre, il est probable qu'il ne faudra pas vingt ans pour un tel changement. Or, d'après un récent rapport de … Goldman Sachs (une banque, eh oui), dans les sondés de la Génération Y (qui ont la trentaine actuellement), 33% admettent s'attendre à pouvoir se passer complètement d'une banque dans les cinq à dix ans à venir, et 50% estiment que l'une ou l'autre start-up aura, d'ici là, pris le relais de ces dernières…
Lorsqu'on voit ce que les hommes d'État ont fait du système bancaire actuel, lorsqu'on voit à quel point ils ont corrodé l'idée même de monnaie et de comportements économiques sains, on comprend que déposséder l'État du système bancaire et renvoyer celle-ci vers les citoyens est **un objectif à la fois noble et nécessaire**.
Et, maintenant que la technologie le permet, c'est même atteignable.
Liens : http://www.contrepoints.org/2015/05/08/207050-en-finir-avec-les-banques-dans-10-ans

Les banques organisent la riposte face aux fintech, dans les transferts d'argent

C'est maintenant qu'il faut agir. » Tel est, en substance, le message que les banques membres de Swift (Society for worldwide interbank financial telecommunication) avaient adressé à ce réseau mondial d'échange de données financières, en 2015, lors du salon Sibos organisé par ce dernier. L'objet de cette urgence ? La modernisation des infrastructures de paiements internationaux de Swift. Il faut dire que la création de cette coopérative belge - qui compte quelque 10.000 adhérents dans 200 pays environ, dont 7.000 banques - remonte aux années 1970. Certes, Swift - qui permet aux banques d'échanger des informations financières automatisées et standardisées, donc à moindre coût - représente toujours *« une grande partie des paiements internationaux interbancaires, entre pays nécessitant une conversion de devises, qu'il s'agisse de paiements au bénéfice d'entreprises ou de particuliers »*, a souligné Thierry Chilosi, l'un des responsables de Swift pour la zone Europe, Moyen-Orient, Afrique, lors d'une conférence de presse, le 11 mars.
Mais cette position devient plus difficile à tenir, depuis quelques années. D'abord parce que les nouvelles technologies ont considérablement modifié les attentes des utilisateurs finaux de Swift. Désormais habitués à voir nombre de leurs demandes

satisfaites quasi-instantanément, d'un simple glissement du pouce sur l'écran de leur smartphone, ils ne comprennent plus qu'envoyer de l'argent à l'étranger prenne deux à cinq jours, quand ce n'est pas dix jours pour certains pays. Une durée qui n'est qu'agaçante pour la clientèle des particuliers, mais qui devient carrément problématique dans le domaine du commerce international. En 2016, il n'est en effet pas simple pour un fournisseur d'admettre que son paiement par le donneur d'ordre mette plus de temps à franchir les mers que les navires chargés d'acheminer sa cargaison.

L'émergence de nouveaux acteurs

Si, encore, il n'y avait que le problème du délai des transferts d'argent internationaux. Mais non. Particuliers comme entreprises, les utilisateurs finaux de Swift réclament également un service meilleur marché, davantage de transparence sur les tarifs afin de savoir exactement quelle somme le bénéficiaire recevra, ainsi qu'une plus grande traçabilité des transactions, entre leur déclenchement et le moment où le compte du bénéficiaire est crédité, un peu à la manière de que proposent DHL et UPS dans le transport de colis. Ces nouvelles exigences, Swift doit les prendre en considération d'autant plus rapidement que de nouveaux entrants s'ingénient d'ores et déjà les satisfaire. C'est le cas de PayPal et, beaucoup plus récemment, de fintech [startups spécialisées dans les technologies financières ; Ndlr] comme TransferWise. Ces nouveaux concurrents, dont l'émergence est favorisée par la directive européenne sur les services de paiement (DSP2), notamment, opèrent principalement sur le marché des transferts d'argent internationaux entre particuliers.

Mais Thierry Chilosi, chez Swift, ne se fait aucune illusion : « Ces nouveaux acteurs vont venir sur le segment B2B (business to business), car il représente 80% à 85% des revenus que les banques tirent du marché des paiements internationaux. »

De fait, il n'y a pas de commune mesure entre les quelques milliers d'euros adressés par une personne émigrée à sa famille restée au pays, et les dizaines ou centaines de millions d'euros que s'échangent des multinationales. Un potentiel auquel Western Union, acteur traditionnel des transferts d'argent entre particuliers, s'intéresse également.

La blockchain, complémentaire de Swift

Face à cette menace, Swift a lancé en décembre 2015 un projet d'innovation visant à améliorer les éléments pointés du doigt par ses utilisateurs, projet qui a été adopté par 45 banques dans le monde, parmi lesquelles figurent trois établissements français, à savoir BNP Paribas, la Société générale et Natixis (groupe BPCE). L'un des objectifs étant par exemple de ramener à une journée le délai de réception des fonds. Un pilote, porté par 21 banques, dont une Française (BNP Paribas), vient d'être mis en place. Il portera dans un premier temps sur le marché B2B des paiements internationaux, avant d'être sans doute étendu au transfert d'argent entre particuliers. Swift dévoilera les résultats de cette expérimentation à l'automne prochain, au cours de l'édition 2016 de son salon Sibos, qui se tiendra à Genève.

Des résultats qui, comme la coopérative l'espère, pourraient convaincre bien d'autres banques de rallier ce projet de modernisation des paiements internationaux. Et ce, d'autant plus qu'il *« ne nécessitera pas d'investissements technologiques de la part des banques, mais (seulement) une amélioration de leurs processus internes, de leur back-office »*, assure Stanley Wachs, directeur international de l'innovation des paiements chez Swift. Parallèlement, cette dernière lancera à partir du mois de juin des ateliers de réflexion sur la façon dont les technologies de rupture telles que la blockchain pourraient aider à réinventer les paiements interbancaires internationaux, dans les cinq prochaines années. La blockchain, cette technologie ouverte et libre, qui

permet la circulation de monnaies cryptées comme le Bitcoin, est *complémentaire de Swift »*, estime Stanley Wachs. Complémentaire et non pas concurrente, *« la blockchain n'apportant pas du tout le même niveau de sécurité que Swift, puisqu'elle ne possède pas, par exemple, les capacités de lutte contre le blanchiment dont les banques disposent »*, insiste Stanley Wachs. 14/03/2016

Liens : http://www.latribune.fr/entreprises-finance/banques-finance/industrie-financiere/les-banques-organisent-la-riposte-face-aux-fintech-dans-les-transferts-d-argent-556444.html

#FinTech
L'avenir du secteur du transfert d'argent

De nouveaux acteurs bousculent le secteur du transfert d'argent et oblige le leader historique Western Union à élargir son offre. Devenu un réflexe pour le grand public lorsque l'envoi d'argent à l'étranger était évoqué, Western Union voit aujourd'hui sa domination remise en cause par des startups FinTech. Ce mastodonte, qui réalise un chiffre d'affaires de 5,7 milliards de dollars (en 2012), contrôle avec MoneyGram 50% du marché des transferts d'argent du continent africain avec des commissions les plus élevées du secteur (12% environ).

Leader historique du marché, Western Union a augmenté depuis 2009 ses partenariats et a élargi son offre multicanale, notamment via la possibilité de transférer de l'argent en ligne et vers des comptes mobiles.

Ce qui a influencé Western Union à se repositionner

Depuis 2009, il n'est plus nécessaire de disposer d'une licence bancaire dans l'exercice de cette activité. Cela a donc favorisé dans un premier temps, l'entrée de nouveaux acteurs comme TransfertWise et WorldRemit bousculant le secteur jusqu'alors emblématique, grâce à la technologie et avec une promesse simple : le rendre plus efficace, rapide et moins coûteux.

WorldRemit a finalisé une levée de 100M$ aux Etats-Unis il y a quelques mois. Pour en savoir plus à propos de ce marché et des évolutions à venir, la rédaction de Maddyness est allée à la rencontre de son fondateur.

Quels sont les chiffres clés de WorldRemit à ce jour ?

Aujourd'hui, WorldRemit réalise un quart de millions de transactions par mois. En 2013, nous avons enregistré un CA de 9.3 millions de dollars. Suite à une très forte croissance, nous avons eu le plaisir d'annoncer un CA de 25 millions de dollars en 2014.

Vous avez levé récemment 100 millions de dollars : à quoi l'argent va-t-il servir ?

L'investissement que l'on a reçu de Technology Crossover Ventures (TCV) va nous aider à devenir d'une part le leader mondial des transferts d'argent en ligne et d'autre part un challenger dans le secteur des versements d'argent, au beau milieu de Western Union et de MoneyGram.

Nous voulons multiplier nos partenariats avec les banques et les opérateurs mobiles dans le monde. Nous souhaitons couvrir davantage de pays et développer d'autres façons de transférer de l'argent. Par ailleurs, notre base de données s'agrandit de plus en plus. Nous mettons un point d'honneur à renforcer nos équipes de relations clients dans tous nos bureaux internationaux.

Quelle est votre vision du marché du transfert d'argent à long terme?

Avec l'évolution grandissante du transfert d'argent, c'est encore plus surprenant qu'uniquement une petite parcelle de transferts a été envoyée par internet.

Selon la banque mondiale en 2014, l'ensemble des transactions réalisé par des personnes depuis leur domicile représente l'équivalent de la moitié d'un trillion de dollars dans le monde entier.
Seulement 5% des transactions ont été réalisées sur internet. C'est donc pour nous une énorme opportunité de business. Notre vision à long terme serait de prendre le marché online et devenir le leader international des versements d'argents entre particuliers.

Quelle est votre « Secret Sauce » ?

Dès le départ, nous avons vu dans WorldRemit une réelle opportunité. Je pense que notre secret est que l'on a toujours considéré WorldRemit comme une « one-world solution » de transferts d'argent plutôt comme une entreprise globale divisée en différents départements.
Nous nous sommes aperçus que le transfert d'argent en Afrique était peu ou mal considéré par la concurrence et qu'il y a avait pour nous une grande opportunité de ce côté-là.
Mais nous ne sommes pas arrêtés là. Nous avons prouvé que nous pouvions nous internationaliser notamment avec le bureau que nous avons ouvert aux Etats-Unis l'année dernière.

Où voyez-vous votre secteur d'activité dans 5 ans?

Le futur du secteur du transfert d'argent est inéluctablement en ligne, par conséquent sur nos mobiles. WorldRemit aura un tour d'avance dans 5 ans car nous permettons déjà de transférer de l'argent de mobile à mobile. La moitié de nos transactions se réalisent d'ores et déjà via nos applications IOS ou Android et via le net sur notre version mobile. Par ailleurs, nous continuerons de développer des services de paiement sur mobiles et rendre le transfert d'argent plus pratique pour les clients.

Selon vous, quelle sera la tendance sur les moyens de transactions et les systèmes de paiements dans le futur et quel en sera l'impact pour WorldRemit ?

Avant, envoyer de l'argent était peu pratique, obligeant de déposer l'argent chez des agences et d'attendre longtemps. En plus, le service clients était quasi inexistant. Mais tout ne doit pas être comme ça.
Chez WorldRemit, nous réalisons des transferts d'argent en ligne. Cela signifie que nous offrons un service plus rapide, avec un grand nombre de transactions qui arrivent instantanément sur les comptes bancaires et les comptes sur mobiles.
Etre en ligne signifie également que l'on a une meilleure couverture des préventions des fraudes que des agents traditionnels de transfert d'argent. Il est également plus facile de faire des contrôles en ligne qu'avec des espèces.

Vous êtes en train d'innover la façon dont on transfère de l'argent qui est déjà très compétitif et est un secteur saturé, quelle est votre point de vue sur la tendance autour de la politique de prix?

Depuis des années, des entreprises implantées dans le secteur telles que Western Union ou MoneyGram ont imposé des commissions excessives et ont passé des accords avec les agents.L'année dernière, L'Africa Progress Panel – dirigé par Kofi Annan – a dénoncé ces pratiques en Afrique.
Depuis avec l'appui du G8 et du G20, ils ont l'intention de réduire les coûts des transactions. Notre mission chez WorldRemit est d'insister sur le transfert d'argent duopole et d'offrir des prix intéressants à nos clients.

Quels sont vos business modèles sur le long terme?

WorldRemit a en commun avec de nombreux services innovants, l'utilisation existante de la technologie mise à sa disposition dans le monde. Dans notre cas, on a cherché des milliers de systèmes financiers et nous les avons articulé ensemble de façon à ce qu'ils forment une seule et même plateforme.

Quel est votre positionnement face à des nouveaux acteurs comme Transferwise?
On est souvent cité à leur côté, mais nous ciblons 2 types de clients totalement différents. Transferwise est sur l'environnement du FX* (Forex ou marché des changes) et nous sur le transfert d'argent international. Il y a peu de similitudes.
*FX: Le forex est le marché des changes ou devises. *"Le marché sur lequel des devises du monde entier sont échangées l'une contre l'autre, à des taux de change qui varient sans cesse. Sur ce marché mondial, toutes les monnaies sont vendues et achetées en temps réel". Définition infinance.fr*
Quel est votre argument commercial?
En tant que business en ligne, on a été très actif dans l'acquisition de nouveaux clients en ligne partout dans le monde. De notre expérience, nous comptons aussi sur nos clients pour faire le relais : Plus de 70% de nos clients reviennent utiliser nos services et nombreux d'entre eux recommandent WorldRemit à leur entourage familiale et amicale basée sur l'expérience satisfaisante qu'ils ont eu avec nos services. Nous avons également investi davantage de temps et d'énergie sur le transfert via mobile (d'un smartphone vers un compte Mobile Money) que d'autres sociétés.
Avez-vous une stratégie spécifique de segmentation pour les pays comme l'Inde, la Chine ou les Philippines?
WorldRemit est un service global et différent de nos concurrents. On permet de transférer de l'argent et d'apporter de la valeur ajoutée dans des endroits mal desservis. Nous développons continuellement notre empreinte dans le secteur du versement d'argent.
Quelle est votre cible dans les pays émergents (ouvriers, personne n'ayant pas de comptes bancaires…) ?
Les gens envoient de l'argent de chez eux pour plusieurs raisons?: aussi bien pour payer leurs factures que leur voyage, leur loyer ou payer des frais hospitaliers ou pour des écoles et leurs études. Dans de nombreux cas nous n'avons pas de «?cibles?» spécifiques. Si vous avez besoin d'envoyer de l'argent à vos amis ou à votre famille, l'équipe de WorldRemit est disponible pour vous accompagner dans vos démarches. Le fait que nous réalisons des transactions dans des pays émergents est l'une de nos plus grandes satisfactions dans notre business.
Il y a plus de 2.5 milliards de personnes dans le monde qui n'ont pas accès à des services financiers dont 1 milliard qui possède un téléphone portable. C'est un champ de possibilités très important pour nous.
Comment évaluez-vous le blanchiment d'argent en termes de risque pour votre métier sur le long terme?
WorldRemit a été créé sur une grosse plateforme pour veiller aux aspects de conformité et de déontologie.
En tant qu'ancien conseiller auprès des Nations Unies, je sais que les problèmes liés au blanchiment d'argent et la régulation liée au financement du terrorisme peuvent être très contraignantes pour les sociétés de transfert d'argent. Nous avons une équipe d'experts dédiée afin de répondre aux exigences des systèmes de régulations financières dans tous les pays dans lesquels nous opérons.
Comment gérez-vous le problème du blanchiment d'argent en particulier aux Etats-Unis, en France et au Royaume-Uni ?
Notre groupe de directeurs qui veillent à ses problématiques est basé à Denver afin de superviser les entretiens avec le système de régulation et de toutes les problématiques dans tous les Etats-Unis. Avec les directeurs internationaux et les managers de «?conformité?» nous avons toute l'expertise nécessaire afin de répondre à n'importe quelle demande du régulateur. Nous avons été approuvés par le régulateur financier

du Royaume-Uni (FCA) et sommes soumis aux mêmes restrictions que n'importe quel opérateur financier.

Quelle stratégie avez-vous mis en place autour du conflit d'intérêt sur vos clients/utilisateurs?

WorldRemit est soumis aux lois de "connaître son client – Know Your Client" (KYC) afin de prévenir d'attaques frauduleuses de notre plateforme. Nous vérifions l'identité de nos clients et enregistrons toutes nos transactions. En tant que "digital service", nous avons construit un algorithme puissant et complexe qui permet de détecter les fraudes. Nous sommes mieux informés pour les régulations et conflit d'intérêt que n'importe quelle entreprise de transfert d'argent.

Vous êtes un grand admirateur de Steve Jobs? Qu'avez-vous appris de lui qui vous aide dans votre business?

Steve Jobs était un entrepreneur extraordinaire. Il avait cette capacité à savoir ce que les gens comme vous et moi voulaient avant que l'on ne le sache nous-même. Il pouvait savoir ce qu'il se passait de l'autre côté de la montagne et surprendre les autres avec une extrême attention aux détails. Sa vision s'alliait aux tendances du comportement humain et de la technologie comme personne, ce qui lui a permis d'avoir une stature unique pour conduire son entreprise vers le succès.

Liens : https://www.maddyness.com/innovation/2015/04/10/worldremit-ismail-ahmed/

Richard Branson investit 25 millions de dollars dans la start-up de transfert de fonds TransferWise

Il y a quelques mois, la start-up TransferWise gagnait en visibilité en annonçant le transfert d'un milliard de livres sterling sur sa plate-forme.

Avec Sir, Richard Branson vient d'investir avec quelques autres 25 millions de dollars (soit 18 459 750 € d'après le taux équitable de TransferWise au moment de l'écriture de cet article) elle franchit un deuxième jalon en relations publiques.

Une partie de cet argent serait d'ailleurs destinée à une campagne de publicité, à laquelle Branson pourrait participer. D'après le CEO, la start-up pourrait déjà être rentable, mais préfère investir dans sa croissance. Au total, la start-up aura reçu 31 millions d'euros de fonds depuis sa création.

Créée, il y a trois ans par deux estoniens, cette entreprise permet de transférer des fonds à l'étranger en prenant une commission de 0,5 % (1 € au minimum pour des transferts de 200 € ou moins).

L'offre

Ce qui est nettement moins cher que la même opération réalisée auprès d'une banque. Car même quand une banque affirme qu'elle ne fait pas payer de frais, elle prend une commission non négligeable sur les taux de change, commission qui peut avoisiner les 5 %. Pour la start-up, il n'y a qu'un taux juste, et c'est le taux interbancaire.

Le client peut donc réaliser jusqu'à 90 % d'économies. Elle donne l'exemple d'un transfert de 1000 £ qui rapporterait 1 231 € avec son service contre 1 176 € avec une banque typique, soit 55 € d'économies.

La firme communique d'ailleurs sur ces frais cachés avec agressivité en Angleterre, ce qui lui a valu quelques problèmes avec les autorités de régulation de la publicité. Elle regrette que cette autorité ne comprenne pas toujours le fonctionnement des transferts.

Quoi qu'il en soit, la start-up garantit le taux effectif le meilleur pour le client, et s'engage à s'aligner si le client trouve un taux plus avantageux.
À l'heure actuelle, la majorité de ses 10 000 clients sont basés au Danemark, en Pologne, au Royaume-Uni, en Suède et en Suisse.

Le secret des taux bas

Comment la start-up peut-elle proposer des taux aussi bas ? En fait, elle n'échange pas d'argent.
Quand un client français veut envoyer 1 000 € à sa tante aux États-Unis, il vire l'argent sur le compte de la filiale française de TransferWise. Le système de la start-up recherche alors un client américain qui veut faire une transaction en sens inverse, peut-être pour son grand-père français, et qui dépose des dollars dans sa filiale américaine. Elle opère alors un transfert de la filiale américaine pour créditer le compte de la tante, au taux interbancaire, et un transfert de la filiale française pour créditer le compte du grand-père, au taux interbancaire inverse.
En d'autre termes, l'argent ne franchit pas les frontières.
C'est ce que le cofondateur et président Taavet Hinrikus aime comparer à Skype, lui qui en était l'un des premiers employés.

Les limites

La limite du système est que les transferts doivent être relativement symétriques entre deux zones. Dans le cas d'un pays, qui accueillerait beaucoup plus d'immigrés qu'elle n'a d'émigrés, on peut penser que les transferts seront essentiellement unilatéraux, ces derniers envoyant de l'argent à leur famille au pays natal.
Notons d'une part que ce système pourrait aider au blanchiment d'argent, dans la mesure où les régulations sur les transferts nationaux sont souvent moins contraignantes que les transferts internationaux. Et, d'autre part, qu'il n'est pas interdit de penser que certaines banques utilisent un système similaire, au moins en partie.

Liens : http://www.lediligent.com/2014/06/10/richard-branson-investit-25-millions-de-dollars-dans-la-start-up-de-transfert-de-fonds-transferwise/

Paiement en ligne
Etat des lieux en Belgique

Quels moyens de paiement sont les plus appropriés pour un site de commerce électronique? Quels sont leurs avantages et inconvénients ?

De nombreux sites de commerce électronique nécessitent la mise en place de solutions de paiements électroniques, surtout en BtoC (vente vers le consommateur final), le vendeur souhaitant recevoir la confirmation du paiement avant de livrer le produit ou fournir le service demandé.
Au balbutiement du commerce électronique, de nombreux sites se contentaient de recueillir les numéros de cartes de crédit des clients via un simple formulaire en ligne, procédé particulièrement peu fiable pour le client, dont la carte de crédit pouvait être débitée par une personne malintentionnée qui avait repéré le numéro lors du transfert, mais aussi pour le commerçant: celui-ci n'avait pas de certitude que le détenteur effectif de la carte était bien celui qui passe commande. De plus, les données bancaires étant stockées sur son serveur raccordé à internet, le cybercommerçant risquait d'être victime d'un acte de piratage. D'où l'apparition d'une certaine méfiance autour des paiements sur Internet

Ces méthodes sont maintenant heureusement révolues, avec le développement d'autres moyens de paiement que la carte de crédit, la généralisation de systèmes de contrôle permettant d'éviter l'usurpation de cartes de crédit, et surtout avec l'apparition de sociétés spécialisées dans la gestion des transactions de paiement électronique assurant un rôle de tiers de confiance, les « Payment Service Providers » (PSP).

Quelles sont les différentes solutions qui se présentent à l'heure actuelle en Belgique ?

a) Paiements immédiats, en ligne

Il existe différentes formules de paiement en ligne: carte de crédit, carte de crédit jetable, paiement à débit immédiat (cartes de débit et transferts électroniques), paiement par e-mail ou via des comptes de tiers, communications surfacturées, paiements mobiles

1. La carte de crédit

C'est le moyen de paiement en ligne numéro 1, grâce à sa simplicité et son universalité, mais que le cybercommerçant doit accepter avec prudence.

Avantages :

- **s**implicité**:** nécessité juste de recueillir un numéro de code, un nom et prénom, une date de validité, et un code de vérification, informations qui se trouvent sous une structure identique sur toutes les cartes du monde;
- universalité: possibilité de réceptionner des paiements quelque soit le pays d'origine de l'acheteur, sans se soucier des éventuelles opérations de change nécessaires;
- paiement différé au niveau du consommateur**:** élément favorisant bien évidemment les achats impulsifs.

Inconvénients:

- public restreint aux personnes majeures, ayant généralement dû justifier de revenus réguliers pour recevoir une carte de crédit**.** Il y a néanmoins environ 3 millions de cartes en circulation en Belgique (dont plus de 90% émises par l'acquéreur Bank Card Company);
- usurpation (de moins en moins) aisée**:** la simplicité du dispositif engendre la possibilité pour toute personne ayant noté les numéros de la carte d'un tiers d'effectuer des opérations sur le compte de celui-ci. Ce risque n'est évidemment pas lié au commerce électronique, de telles opérations pouvant aussi être effectuées par fax ou téléphone;
- coûts des commissions sur les transactions perçus par l'acquéreur et par le PSP**.** Ils sont variables selon le contrat, dans un ordre de grandeur de 0,8 à 2,5%, plus souvent un montant fixe par mois, plus un coût fixe par transaction
- les transactions sont plafonnées à un certain montant total de dépenses par mois**.** Généralement, il s'agit par défaut de 1250 euros. Ainsi, ce mode de paiement est inapproprié pour la vente de produits d'un montant supérieur et ne devrait pas être le seul proposé aux clients si le panier moyen attendu dépasse les 500 euros.

Aussi, surtout si le site s'adresse à un public international, la carte de crédit reste un des principaux moyens de paiement à proposer sur un site Internet.

La carte de crédit jetable

Une formule alternative consiste à utiliser une carte de crédit « jetable ».

Compte tenu du climat de méfiance autour du paiement par carte de crédit apparu au début du commerce électronique, plusieurs banques ont imaginé le concept de carte

de crédit virtuelle de manière à rassurer le client: ainsi, au lieu de taper son propre numéro de carte de crédit, le consommateur encode en ligne un autre numéro qui est:

- soit éphémère (valable pour une seule transaction),
- soit permanent, mais dont le consommateur peut modifier à tout moment le montant maximum utilisable et parfois d'autres limites (par exemple valable dans un seul pays).

Ce compte virtuel est lié à une carte de crédit classique ou bien à un compte bancaire, mais le couplage n'est connu que de la banque et du client.

Ce moyen de paiement était anecdotique en Belgique jusqu'à l'arrivée sur le marché, fin 2011, de la carte prépayé « B-Paid » lancée par la Poste. Cette carte, commercialisée au prix de 12 euros par an, rechargeable en ligne, par virement, ou par dépot dans un bureau de Poste, est utilisable dans toutes les boutiques en ligne proposant « Mastercard Secure ». D'autres banques ont lancé depuis des solutions équivalentes.

D'autres formules ne sont acceptées que sur certains sites d'e-commerce adaptés en fonction. Ce procédé limite dès lors souvent l'usage aux pays où la banque est présente et aux cybercommerçants avec lesquels elle a conclu un accord.

Ce mode de paiement peut être pertinent pour les sites de commerce électronique s'adressant à des profils d'acheteurs novices en commerce électronique et plutôt méfiants, à des consommateurs mineurs, ou lorsque l'acheteur potentiel souhaite conserver l'anonymat. En effet, avec ce procédé, généralement seule la banque émettrice dispose du nom du client.

A noter que ce mode de paiement n'est pas approprié par rapport à la carte de crédit traditionnelle lorsque la réservation ou les achats nécessitent de présenter la carte qui a été utilisée (par exemple pour retirer des tickets).

2. Méthodes de virements électroniques pré-remplis

Ce moyen de paiement national est bien adapté au BtoC, mais aussi au BtoB.

A l'origine, plusieurs banques belges importantes ont développé leur propre système permettant de valider en ligne des virements pré-remplis d'un de leurs comptes à un autre. Ce système se basait parfois sur l'outil de Web-banking « maison » ou sur une plate-forme électronique spécifique. Il pouvait donc être utilisé par tout client de banque qui s'était abonné à ce service, moyennant parfois un contrat supplémentaire. Le client était redirigé vers cet outil en cliquant sur le bouton correspondant à sa banque affiché sur le site d'e-commerce. Il validait ensuite un virement électronique (pré-rempli) qui transférait le montant sur le compte du vendeur.

Chaque banque ayant son propre système (CBC/KBC Online, Belfius NetBanking, ING Home'Pay), le cybercommerçant devait souscrire à un abonnement auprès de chacune d'entre elles et adapter son site de commerce électronique afin de pouvoir accueillir l'ensemble des clients de ces différentes banques (sauf s'il faisait appel à un PSP qui intégrait les différentes solutions des banques dans sa solution). Dès lors, peu de cybercommerçants ont proposé ce mode de paiement, et donc peu de clients ont souhaité disposer de ce service auprès de leur banque. Ce mode de paiement est donc resté peu utilisé, jusqu'à ce que le secteur bancaire belge, inquiet de la prépondérance des paiements par cartes de crédit, tente de reprendre des parts de marché. Il s'est repositionné via, cette fois-ci, une solution commune aux principales banques belges actives en ligne, basée sur la carte de débit classique Bancontact-MisterCash déployée par Atos Worldline (ex-Banksys).

Service « Bouton Bancontact »

Lors de l'étape « paiement », le navigateur Internet de l'acheteur est redirigé vers l'interface de Web-banking de sa banque, auquel il est généralement familiarisé. Il

encode le numéro de la carte de débit, c'est-à-dire un nouveau numéro PAN (Primary Account Number), comportant 17 chiffres et commençant par 6703. Le titulaire valide l'opération de la même manière qu'il effectue d'ordinaire ses transactions bancaires en ligne (selon les banques, via par exemple une calculette « digipass », etc.). Cette redirection permet de s'assurer que l'acheteur est bien le titulaire de la carte.

Le cybercommerçant devra payer une commission par transaction (compris entre 1 et 1,5%), mais aussi des frais d'abonnement et de transaction auprès du prestataire qu'il aura choisi pour implémenter le programme de capture et de suivi des commandes sur son site Internet.

Avantages:

- sécurité des transactions: celles-ci s'effectuent avec le même niveau de sécurité que les opérations bancaires en ligne. Le risque de piratage est très faible;
- non répudiation possible: l'usage à l'interface de Web-banking est personnel, protégé par un mot de passe;
- la carte de débit est fort répandue: plus de 10 millions d'exemplaires en Belgique, les belges en ayant plusieurs. Ainsi le site d'e-commerce peut atteindre une population plus large: les adolescents, les retraités et les sans-emplois.
- pas d'apprentissage nouveau pour les personnes déjà habituées à effectuer des opérations bancaires en ligne. Celles-ci seront donc assez facilement disposées à utiliser ce mode de paiement;
- pas de plafond mensuel: la transaction sera acceptée du moment que le compte bancaire est suffisamment alimenté ou que l'ouverture de crédit à la consommation qui aurait été accordée à ce client est suffisante. Toutefois, des plafonds sont parfois fixés dans le contrat de Web-banking;
- bonne adaptation aux transactions BtoB (entre sociétés), l'usage de la banque en ligne se généralisant dans les entreprises.

Inconvénients:

- non universalité: il s'agit d'un système de portée nationale pour l'instant, mais qui devrait s'élargir dans le cadre du SEPA (Single Euro Payments Area, zone de paiement européenne unique). De plus, tous les clients des banques n'ont pas souscrit à un abonnement de Web-banking, qui fait parfois l'objet d'un supplément;
- contestation difficile: contrairement au paiement par carte de crédit qui applique un remboursement direct en cas de contestation, avec charge pour le vendeur de montrer qu'il y a une fraude, le client devra introduire un dossier pour être remboursé s'il n'a pas reçu le produit et n'a pas été directement remboursé par le vendeur.

Ce mode de paiement rencontre un fort développement en Belgique, atteignant maintenant de l'ordre de 1/5 des paiements électroniques en ligne.

Il est plus particulièrement recommandé lorsque le site s'adresse particulièrement aux jeunes, ou bien à d'autres sociétés (BtoB), lorsque le panier moyen est d'au moins 10 euros.

A noter l'apparition d'une concurrence, dans le chef de Maestro, qui ne fonctionne toutefois actuellement, pas avec les cartes de débit Maestro émises par certaines (petites) banques belges.

3. Systèmes de paiement par e-mail ou via des comptes virtuels de tiers

Il s'agit de systèmes de paiement très faciles à mettre en place et de portée internationale, mais à l'origine surtout conçus par les transactions CtoC. Le marché du

paiement électronique présente de grandes opportunités d'affaires au niveau mondial de sorte que plusieurs sociétés multinationales se sont positionnées dans ce créneau.
Il en est ainsi de la société eBAY qui a racheté la société « PayPal », concepteur d'un système de paiement sous cette dénomination.
Ce système s'inspire du principe des cartes virtuelles: il couple un moyen de paiement classique, comme une carte de crédit, à un identifiant auquel est associé un mot de passe. Une fois inscrit (en communiquant par exemple un numéro de carte de crédit), le client peut effectuer des transferts d'argent auprès de toute autre personne disposant aussi d'un compte « PayPal », en communiquant l'identifiant (dans le cas de Paypal, une adresse e-mail) et le mot de passe. Il est possible de payer, mais aussi de recevoir de l'argent.
Il présente les mêmes avantages et les mêmes inconvénients que le moyen de paiement auquel il est généralement couplé, la carte de crédit. On notera surtout que PayPal est un moyen de transfert financier de portée internationale, simple (il est facile de s'inscrire et de l'utiliser, avec juste un login et un mot de passe), accepté par un très grand nombre de marchands et auquel plus de 200 de millions de personnes ont souscrit.
De plus, il n'y a pas de frais d'installation, d'abonnement mensuel, de frais d'installation de passerelles techniques etc.
Le système n'est pas par contre incomparablement moins sûr que le paiement par virement pré-rempli, validé par un code unique généré par exemple par un Digipass: Il ne s'appuye que sur un couplage « login + mot de passe », que des personnes malintentionnées peuvent tenter de recueillir auprès des utilisateurs par pishing notamment, en se faisant passer pour le service d'assistance de Paypal,..
En effet, dans certaines régions du monde, l'ouverture d'un compte virtuel n'est pas aussi contrôlé que l'attribution d'une carte de crédit, notamment au niveau de l'identité du détenteur. De sorte que ce mode de paiement doit être utilisé avec prudence lorsqu'il s'agit de verser de l'argent à un individu que l'on ne connaît pas ou à une société qui n'a pas pignon sur rue. Pour compenser cette faiblesse importante au niveau de l'authentification des deux parties, PayPal inclut dans les frais de commission perçus (3,4% en Belgique actuellement, plus 0,35 euro et une éventuelle marge de change de 2,5%) une assurance qui couvre les transactions jusqu'à un certain montant (actuellement 500 euros).
Les sociétés spécialisées Ogone et Neos Solution peuvent intégrer PayPal sur un site d'e-commerce. En Europe, PayPal est utilisé dans plus de 30% des cas pour des transferts financiers sans lien avec eBay.
A noter que les micro-paiements (à partir même de 0,01 euros) sont généralement bien assurés par ces systèmes.
Un mot enfin sur le système « Western Union ». Il s'agit d'un système de transferts de fonds, d'une personne à une autre, basé sur un nombre très important d'agences à travers le monde. Il est bien adapté par exemple pour verser de l'argent à des proches résidant à l'étranger, surtout dans des pays où l'accès aux services bancaires n'est pas généralisé. Par contre, il ne convient pas pour le commerce électronique et encore moins pour le paiement en « CtoC », auprès de personnes qui ne sont pas connues du donneur. Un vendeur qui ne permet qu'un paiement via ce système doit inspirer une grande méfiance. Ainsi, en Belgique, une très large majorité des plaintes pour escroqueries et arnaques via Internet proviennent de personnes qui ont versé de l'argent via Western Union à des inconnus.

4. Les codes uniques, prépayés

Ces cartes prépayées peuvent être achetées en magasin (réseau de boutiques affiliées), ainsi qu'en ligne ou par virement bancaire. L'internaute doit gratter les chiffres au dos de la carte (ou télécharger ce code sur un site web). En tapant ce code unique, il est alors possible d'accéder à des services Premium de réseaux sociaux, de consulter des documents en archives, de télécharger des logiciels, de jouer en ligne,…

Exemples de prestataires :

- www.paysafecard.com/be
- www.allopass.com
- www.ticketsurf.com
- www.cash-ticket.com
- www.wexpay.com
- www.Zeevex.com
- www.Neosurf.info

Ces dispositifs ne sont pas liés automatiquement à un compte bancaire et présentent généralement un anonymat bancaire. Ils sont simples d'utilisation, s'adressent plus particulièrement à un public non ou peu bancarisé, et sont très adaptés aux petits montants d'achats (moins de 5 euros) ainsi qu'à la fourniture de biens dématérialisés (ex: jeux en ligne). Par contre, ils présentent l'inconvénient qu'il est nécessaire pour l'acheteur d'acquérir des codes préalablement.

Les monnaies virtuelles

A noter également, le développement de monnaies virtuelles, en circulation uniquement en ligne. ex:

Webmoney, Ukash, Bitcoins,…

Au stade actuel, des monnaies virtuelles doivent être acceptées avec grande prudence par les e-commerçants, les cours de ces monnaies pouvant varier fortement et ces monnaies étant parfois utilisées comme moyen de blanchir de l'argent.

B) Paiements immédiats, via GSM:

Transfert validé par une application mobile

Les principales plateformes d'applications pour smartphone (sous iOS, Android, Windows Phone) proposent maintenant des solutions à installer sur son GSM, qui permettent à l'utilisateur,

- soit de signer électroniquement un virement (en employant en parallèle un Digipass; ex: l'application « scasher » de KBC),
- soit de valider un transfert financier d'un portefeuille virtuel à un autre (ex: Paypal).

En Belgique, les paiements par mobile restent toutefois actuellement marginaux (de l'ordre de 1% des paiements en e-commerce, hors achat d'applications / logiciels). Ils sont surtout employés pour l'achat de tickets / vouchers virtuels.

C) Paiements en différé

Si en BtoC, le client n'étant généralement pas connu du vendeur, la prudence voudrait que le paiement soit exigé avant livraison, le paiement en ligne n'est pas pour autant incontournable.

A côté des « véritables » moyens de paiement électronique en ligne, pour donner confiance au consommateur et réduire le pourcentage élevé d'abandons de commandes au stade du paiement, il est recommandé de proposer sur un site d'e-commerce au moins une formule de paiement « off-line »

1. Paiement contre livraison

Il s'agit d'une solution coûteuse, mais rassurante, tant pour le client que pour le vendeur. Cette formule très classique permet au client de régler le montant de l'achat

auprès du livreur, au moment de la livraison ou lors du retrait dans un point de livraison (exemple: les points de vente affiliés au réseau Kiala ou au réseau Mondial Relay).

Avantages:

- Rassurant pour les 2 parties: le vendeur ne prend pas le risque de livrer de la marchandise sans être sûr d'être payé. L'acheteur ne prend pas le risque de payer de la marchandise qu'il n'est pas certain de recevoir;
- Pas de contestation possible concernant la livraison;
- Simplicité technique: Pas d'installation technique particulière à prévoir sur son site Internet;
- Service pouvant être international (en fonction de la société de livraison sélectionnée)

Inconvénients:

- Nécessité pour l'acheteur d'être présent lors de la livraison. L'acheteur doit disposer à ce moment de liquidités pour régler le livreur, celui-ci n'étant pas systématiquement équipé d'un terminal mobile de paiement bancaire. Certains prestataires logistiques offrent la possibilité de retirer l'article auprès de points d'enlèvement (station essence, librairies, supermarché, etc.) où le paiement s'effectuera classiquement à la caisse;
- Commission importante perçue par le prestataire de livraison pour ce service, surtout au niveau international;
- Risque d'une plus grande proportion de commandes bidons ou refusées lors de la livraison, ce qui peut entraîner pour le cybercommerçant des frais de livraison et de retour de marchandises non couverts;
- Ne convient évidemment pas pour la fourniture de produits dématérialisés (fichiers musicaux, etc.)

Ce mode de paiement est particulièrement adapté pour la vente de produits, d'une certaine valeur (entre 20 et 1 000 euros), qui doivent être livrés aux clients. Aussi, dans ce cas, il est recommandé de proposer cette formule en plus des modes de paiement en ligne, éventuellement moyennant un supplément.

2. Paiement par virement bancaire

Cette solution est la moins chère, mais elle est évidemment risquée pour le vendeur. Le client effectue un virement bancaire ordinaire sur le compte bancaire du vendeur. Il existe deux possibilités.

a) Soit le vendeur exige que le montant lui parvienne pour que la livraison soit effectuée.

Avantages:

- Gratuité du virement bancaire (ou très faible coût au niveau européen) tant pour l'acheteur que pour le vendeur;
- Fiabilité par rapport à d'autres moyens de paiemenst traditionnels, tels que le chèque.

Inconvénients:

- Non immédiateté. Plusieurs jours peuvent s'écouler, voire plus d'une semaine lors de virements internationaux (hors format normalisé « européen »), avant que l'argent ne parvienne sur le compte du vendeur;
- L'acheteur doit faire confiance au vendeur quant à la livraison. De plus, celle-ci sera retardée, le vendeur attendant d'être payé avant de fournir le produit ou service demandé;
- Coût important pour les transactions de/vers des pays hors Union Européenne.

b) Soit le vendeur demande au client de payer après réception, au terme du délai de réflexion (voir ci-dessous).

3. Factures

La facture est la solution incontournable en Business to Business. Celle-ci est traditionnellement établie sous format papier, mais peut maintenant légalement se présenter sous format électronique (voir dossier « facturation électronique »), évolution qui facilite le traitement administratif tant pour le commerçant que pour l'acheteur.

Certes, ce mode de paiement n'est pas le plus recommandé pour un site orienté vers une clientèle nouvelle, compte tenu du risque par le cybercommerçant de non paiement de la marchandise livrée. Si ce risque est significatif, la formule « livraison contre paiement » est plus appropriée.

Liens : http://www.retis.be/comment-vendre-en-ligne/parcours-client/servir/paiement/