وزارة المالية
MINISTERE DES FINANCES
CTRF
CELLULE DE TRAITEMENT DU RENSEIGNEMENT FINANCIER
خلية معالجة الإستعلام المالي
خ م إ م

LETTRE D'INFORMATION DES ACTUALITES INTERNATIONALES
DANS LE DOMAINE DE LA LUTTE CONTRE LE BLANCHIMENT D'ARGENT
ET LE FINANCEMENT DU TERRORISME

Lettre n°88

Bruxelles veut assécher le financement du terrorisme en surveillant bitcoins et cartes prépayées

La Commission européenne a présenté hier un « *plan d'action destiné à renforcer la lutte contre le financement du terrorisme* ». Plusieurs volets sont au programme, mais Bruxelles s'attarde particulièrement sur l'utilisation de moyens de paiement anonymes. Crypto-monnaies, cartes de paiement prépayées et espèces sont ainsi visées.

Alors qu'en France, l'état d'urgence est toujours d'actualité, près de trois mois après les attentats de Paris, la Commission européenne cherche des moyens de lutter contre le terrorisme. L'objectif pour les autorités européennes est de couper le robinet du financement des organisations terroristes, grâce à une série de mesures dont la mise en application s'étalerait sur 2016 et 2017.

Surveiller les plateformes d'échange de crypto-monnaies

Pour parvenir à cet objectif, Bruxelles voudrait agir simultanément sur plusieurs leviers. Outre le renforcement de la vigilance concernant « *les flux financiers en provenance de pays tiers à risque* » la Commission aimerait garder un œil sur « *les risques de financement du terrorisme, liés aux monnaies virtuelles* ».

Les crypto-monnaies permettent en effet d'effectuer des transactions financières de manière quasi instantanée d'un bout du monde à l'autre, dans un anonymat relatif. Si la Commission ne peut agir directement sur ces flux, elle peut cependant aller frapper à la porte des plateformes de change proposant de troquer ses bitcoins contre des euros, des dollars ou toute autre monnaie classique.

Bruxelles propose ainsi dans son « *plan d'action destiné à renforcer la lutte contre le financement du terrorisme* » d'inclure les plateformes de change de crypto-monnaies dans le champ d'application de la directive anti-blanchiment « *de manière à ce que ces plateformes doivent appliquer des mesures de vigilance à l'égard de la clientèle lors de l'échange de monnaies virtuelles contre des monnaies réelles* ». L'objectif affiché des autorités est de « *mettre fin à l'anonymat associé à ce type d'échange* » d'ici « *la fin du deuxième trimestre* ».

En France, les plateformes d'échange doivent déjà se déclarer auprès de l'ACPR. Le Rapport Tracfin sur les crypto-monnaies publié en juillet 2014 suggérait déjà quant à lui la nécessité d'identifier les clients de ces plateformes, à partir du moment où ils effectuent des échanges entre euros et monnaies virtuelles.

Pas de bannissement des crypto-monnaies

Si Bruxelles souhaite réguler les échanges entre crypto-monnaies et monnaies fiduciaires, il n'est pas prévu de bannir leur utilisation. Si les plateformes d'échange seront soumises à de nouvelles obligations, via la quatrième directive anti-blanchiment, les fournisseurs de portefeuilles numériques pour les monnaies virtuelles (type Electrum, MultiBit) ne devraient quant à eux pas avoir à changer leurs habitudes.

Cependant, la Commission note que les monnaies virtuelles « *sont souvent considérées comme un outil intéressant pour les transferts internationaux d'argent* » et qu'elles « *représentent un marché innovant mais petit* ». Elle rappelle également que la Banque centrale européenne (BCE) avait jugé qu'elles ne représentaient pas une menace du point de vue de la stabilité financière de la zone euro. Aucune raison donc d'interdire leur utilisation, pour le moment.

Les cartes de paiement prépayées dans le colimateur de l'Europe

Bruxelles veut aussi « *s'attaquer aux risques liés aux instruments prépayés anonymes* », type TransCash ou PCS, qui permettent à n'importe qui de profiter d'une solution de paiement avec un plafond de 2 500 euros par carte, sans vérification d'identité au moment de l'ouverture du service. Ce type de carte ont notamment été utilisées pour la préparation des attentats de Paris, note la Commission Européenne dans une FAQ.

Les mesures autour de ces cartes n'ont pas encore été précisées, mais l'Europe voudrait abaisser le plafond à partir duquel il devient nécessaire de vérifier l'identité du futur détenteur de la carte avant de lui fournir le service. La Commission précise « *qu'il sera veillé à la proportionnalité de ces mesures, eu égard en particulier à l'utilisation de ces cartes par des citoyens vulnérables sur le plan financier* ». Là encore, il est question d'une application d'ici mi-2016.

Les solutions de type Compte Nickel ne devraient quant à elles pas subir de contrecoup particulier, puisqu'elles nécessitent déjà une vérification de l'identité du client avant même l'ouverture du service.

Les espèces posent également problème

Il y a un dernier mode de paiement anonyme qui pose problème à Bruxelles et des centaines de millions de citoyens l'utilisent quotidiennement : les espèces. Intraçables elles sont pourtant omniprésentes dans la vie courante et il est encore impensable de les faire disparaître. L'Europe voudrait néanmoins émettre une « *proposition législative relative aux mouvements illicites d'argent liquide* », dans laquelle la Commission « *étendra le champ d'application du règlement existant afin d'y inclure l'argent liquide envoyé par fret ou par la poste et de permettre aux autorités d'agir à l'égard de montants plus faibles d'argent liquide en cas de soupçons d'activité illicite* ».

On rappellera que le plafond pour les achats en espèces est passé de 3 000 à 1 000 euros en France le 1er septembre dernier, et que depuis le 1er janvier, les français doivent présenter une pièce d'identité pour toute opération de change d'une valeur de plus de 1 000 euros. Depuis le 1er janvier, les banques doivent également signaler à Tracfin tout dépôt ou retrait d'espèces d'un montant supérieur à 10 000 euros par mois.

Le cas épineux du billet de 500 euros

La Commission, la Banque centrale européenne et Europol vont également travailler de concert pour évaluer la nécessité d'un retrait de la circulation des billets de 500 euros. Ceux-ci représentent un tiers de la valeur de l'ensemble des billets en circulation, alors même qu'ils ne sont que très peu utilisés lors de paiements.

« *Ces billets sont très demandés au sein des groupes criminels qui s'en servent pour transporter leur argent, en raison de leur grande valeur et de leur faible volume* ». Il est en effet plus facile de transporter clandestinement un seul billet de 500 euros qu'une liasse de 50 billets de 10 euros. Il reste encore à voir si cette mesure sera vraiment efficace, les billets de 100 et 200 euros n'étant pas beaucoup plus difficiles à camoufler.

https://www.nextinpact.com/news/98359-bruxelles-veut-assecher-financement-terrorisme-en-surveillant-bitcoins-et-cartes-prepayees.htm

S’attaquer aux sources de financement, la recommandation de l’ONU

Sous la direction de l’Office des Nations unies de lutte contre la drogue et le crime (Onudc), une rencontre sur le financement de l'extrémisme violent dans le Sahel et la Corne de l’Afrique se tient à Dakar depuis hier, mardi 7 février. L’objectif de ce conclave est de réfléchir sur les voies et moyens pour empêcher le financement des bandes terroristes. Des représentants de pays de l’Afrique de l’Est, du Centre et de l’Ouest prennent part à ce séminaire qui dure trois jours

Un séminaire de trois jours, organisé par l’Office des Nations unies de lutte contre la drogue et le crime (Onudc), est ouvert hier, mardi 7 février. Cette rencontre régionale qui réunit des participants venus des pays de l’Afrique de l’Ouest, du Centre et de l’Est, vise un partage d’expérience afin d’aboutir à un blocus des sources de financements des groupes terroristes. Pour le représentant régional du l’Onudc, Pierre Lapaque, un meilleur contrôle des flux financiers est nécessaire dans la lutte contre l’extrémisme violent et le terrorisme. Selon lui, assécher les sources de financement des groupes terroristes qui tirent plus souvent leurs revenus du détournement, le trafic de drogue et le kidnapping, est d’une impérieuse nécessité.

Pour cela, Pierre Lapaque exhorte les cellules de renseignement financiers et les services d’enquête à faire de sorte que les groupes térroristes et leurs bailleurs soient démantelés. Par ailleurs, Pierre Lapaque a aussi loué l’importance, pour les pays africains, de développer une stratégie commune car, dit-il, les groupes terroristes sont interconnectés. La rencontre de Dakar a pour but donc de faire des recommandations pour une lutte effective contre le terrorisme et l’extrémisme violent en particulier.

A signaler que l’Assemblée générale des Nations Unies a adopté en 2016, un Plan d’action pour la prévention de l’extrémisme violent. Le plan est un appel à une action concertée de la communauté internationale. Il fait plus de soixante dix (70) recommandations aux États membres et au système des Nations unies pour empêcher l’extrémisme violent de se propager davantage. Aussi ce plan préconise-t-il une approche globale comprenant non seulement des mesures essentielles de lutte contre le terrorisme, mais aussi des axes préventifs qui s’attaquent directement aux causes sous-jacentes qui conduisent des individus à se radicaliser et à rejoindre ces groupes extrémistes violents.

L’extrémisme violent est tout ce qui peut avoir des liens avec le terrorisme. Il peut être une pensée violente fondée sur la religion ou une philosophie. Il peut être causé par la frustration, le bas niveau d’éducation, le sentiment d’injustice, le chômage et le désespoir.

http://www.sudonline.sn/s-attaquer-aux-sources-de-financement--la-recommandation-de-l-onu_a_33437.html

Cybercriminalité et blanchiment de capitaux sur internet

Le blanchiment d’argent connaît de nouveaux développements depuis l’avènement d’internet. Le présent article fait le point sur cette cybercriminalité en col blanc.

Dans ce cadre, Internet constitue une source d’inquiétudes, dès lors que l’argent criminel y circule très rapidement, emportant différents risques, comme les risques technologiques, l’anonymat, les limitations à l’accord de licences et au contrôle, les risques géographiques et juridiques, et le risque de transactions (financières) compliquées.

Les criminels disposent ainsi, avec Internet, d’un immense « terrain de jeu » pour y développer leurs activités en profitant d’un avantage incontournable d’invisibilité et

d'anonymat. Il y a d'infinies possibilités pour gagner de l'argent sans être confronté à ses victimes. Prenons l'exemple des « attaques informatiques » ou des « cyberattaques ». Il est possible de pénétrer des systèmes numériques publics et privés sans dévoiler son identité ou le lieu de la transaction. Le « phishing » constitue une méthode par laquelle on s'empare du code PIN d'une carte de paiement ou d'une carte de crédit, ou même le code d'accès particulier pour accéder à son compte bancaire ou encore le « pharming ». Pensons également à la « cyber-rançon », où une rançon est demandée, afin d'éviter qu'un système numérique ne soit mis hors service. Enfin, il convient de relever les nombreuses informations détournées par des personnes malveillantes et les cas d'usurpations d'identité qui se multiplient notamment sur les réseaux sociaux. L'espace de la Toile est devenu une infosphère où se multiplient et où cohabitent des données personnelles ou publiques, dont l'origine et la véracité ne sont pas certifiées. Et le nombre d'exemples à citer est innombrable.

En ce qui concerne la cybercriminalité, il y a une économie souterraine qui pourvoit aux besoins d'outils, de marchandises et de services pour commettre le cybercrime, et même pour vendre et acheter des biens et des informations volées. Cela s'appelle le « Dark Net ». Il s'agit d'un environnement économique véritable avec des producteurs, des commerçants de marchandises et de services, des fraudeurs et des clients.

Il y a aussi les jeux et les paris en ligne qui ont connu une explosion exponentielle sur la Toile. Un des problèmes en cette matière consiste à contrôler où se trouve le serveur informatique des jeux (question de compétence de contrôle et juridique). Et ce, sans parler de la « monnaie virtuelle » ? La « monnaie virtuelle », telle qu ele bitcoin, se distingue de la « monnaie électronique », du fait qu'elle est créée par un groupe de personnes (physiques ou morales), et non par un État, ou une union monétaire. Cette monnaie est destinée à comptabiliser, sur un support virtuel, les échanges multilatéraux de biens ou de services au sein du groupe concerné. Il s'agit d'un système non régulé, caractérisé par un facteur d'opacité.

En fait il y a deux éléments essentiels qui différencient les deux systèmes. En premier lieu, la monnaie virtuelle peut être utilisée dans le « cyberspace ». Les transactions ne peuvent pas êtres rattachées à une zone géographique déterminée. Les flux ne sont pas détectables : ces « monnaies » sont conçues pour exister en dehors du contrôle d'un organe de régulation. Le système peut être fermé (sans convertibilité avec la monnaie officielle) ou ouvert (avec possibilité de convertir les fonds virtuels en monnaie officielle). En second lieu, la monnaie virtuelle permet aussi des transactions totalement anonymes qui peuvent avoir lieu soit directement entre particuliers, soit par l'intermédiaire de prestataires de services. Tous les acteurs opèrent en dehors du secteur traditionnel des services de paiement. Aucun plafond d'utilisation ou plancher d'identification des utilisateurs ne leur est applicable.

L'ensemble de ces nouvelles possibilités qu'offre Internet ont eu, pour corollaire, la création de multiples possibilités d'y blanchir de l'argent. Parmi les méthodes les plus utilisées, il convient de relever l'emploi des « Payable Through Accounts ». Il s'agit ici de comptes bancaires, dont le titulaire a ordonné que, quand un certain solde a été dépassé sur le compte, ce montant soit directement viré sur un ou plusieurs autres comptes (intérieurs ou internationaux). Une autre variante est le « criss-crossing scriptural », par lequel l'argent est transféré mutuellement entre différents comptes en banque à divers noms à l'intérieur et/ou à l'étranger et cela en combinaison avec des transferts d'argent par des firmes de transferts d'argent.

Actuellement les transferts (internationaux) peuvent être exécutés de différentes manières : par les comptes bancaires traditionnels, l'e-monnaie, les services de paiement Internet ou les services de transferts d'argent traditionnels.

Indépendamment du mode de payement, toutes ces manières de transférer de l'argent ont leurs propres vulnérabilités en matière de risques de blanchiment de capitaux. Généralement

ces transferts internationaux se déroulent dans la deuxième phase du blanchiment : l'empilement.
Des transferts bancaires, des hommes de paille et des mules bancaires sont des méthodes souvent utilisées pour blanchir des avantages patrimoniaux illégaux obtenus par le « phishing ». Afin de cacher son identité, le criminel peut également contacter plusieurs personnes en leur offrant de l'argent pour utiliser leur compte personnel afin d'y effectuer des transactions. Dans de nombreux cas, les hommes de paille ouvrent un nouveau compte personnel à ces fins et quand la transaction en question a été effectuée, ils déclarent que les fonds leur appartiennent. Les fonds sont ensuite transférés à d'autres comptes intérieurs et/ou étrangers ou retirés en liquides. Souvent les liquides sont ensuite envoyés par des services de transferts d'argent à l'étranger. Et ainsi la chaîne du papier est interrompue et le criminel a su effacer ses traces et le lien avec le délit sous-jacent est brouillé.
Le recours à des « shell companies », des sociétés qui n'ont pas d'activités (commerciales), aucun actif ou obligations financières, sont des structures intéressantes pour les « cyberblanchisseurs ». En effet, ces sociétés disposent de différents comptes bancaires étrangers, souvent situés dans des pays offshore. Ces compagnies sont utilisées comme preuve de paiement pour les banques et permettent ainsi d'effacer la trace de l'argent.
Bien que les nouvelles plateformes de paiement en ligne et les monnaies digitales gagnent de plus en plus en influence dans notre vie quotidienne et environnement social, les cybercriminels et les cyberblanchisseurs dépendent toujours de notre système financier et bancaire traditionnel. Les virements (internationaux) sont toujours rapides et efficaces et généralement utilisés au premier stade du blanchiment de même que la cybercriminalité existe en volant de l'argent des comptes en banques des victimes par des techniques frauduleuses.
En outre, le blanchiment d'argent classique dans les casinos est accompagné du blanchiment dans les jeux et paris en ligne, notamment sur les chevaux, le football, etc.
Les plateformes de jeux et de paris en ligne, qui sont vulnérables pour le blanchiment de capitaux et d'autres crimes financiers par la nature de leurs opérations, peuvent servir comme facilitateurs de blanchiment. Les institutions de jeux sont des commerces très actifs en matière de transactions en liquides qui fournissent une série très large de produits et de services financiers, et qui sont semblables à ceux fournis par des compagnies financières et de services de transactions financières. En plus, les compagnies de jeux servent à des clients variés et souvent temporaires dont ils ne savent que très peu. Les logiciels fournis par les organisateurs de jeux et de paris en ligne rendent possible de transférer et d'accumuler de grandes sommes d'argent, et déposer et retirer de l'argent gagné par des virements bancaires ou différents systèmes de paiement électroniques.
Profitant de failles juridiques et de faiblesses des moyens de lutte, le crime organisé diversifie ses activités. Pour cela, il recourt à des moyens sophistiqués notamment aux réseaux numériques pour commettre ses méfaits et masquer ses actes illicites, et ce à l'échelle mondiale. Le crime organisé s'affranchit en effet des contraintes géographiques et juridiques pour saisir des opportunités, notamment avec des opérations de blanchiment. Des efforts sont donc attendus concernant les moyens de lutte, en particulier pour améliorer le recueil, la conservation et l'exploitation de la preuve fondée sur des données numériques.
La lutte contre la cyberdélinquance est un défi non seulement pour l'Europe et chacun de ses Etats-membres, mais pour le monde entier. Face aux possibilités infinies offertes par le numérique et aux risques que cela engendre, un dispositif législatif performant et dynamique est indispensable, qui ne cesse pas de s'améliorer et de s'adapter. Aussi le contrôle et la lutte contre la cybercriminalité doivent être continuellement dynamiques et innovantes. Mais dans ce domaine, rien n'est figé et des pistes demeurent à explorer
https://creobis.eu/aml/

Le volet cyber des nouveaux textes sécuritaires

Le début d'année 2016 est marqué par une nouvelle vague de textes sécuritaires.
Après la loi de programmation militaire en 2013, la loi contre le terrorisme en 2014, la loi sur le renseignement, la loi sur la surveillance des communications électroniques internationales, la loi sur l'état d'urgence en 2015, voilà donc le projet de loi prolongeant l'état d'urgence, sans oublier celui « renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale », la proposition de loi tendant à renforcer l'efficacité de la lutte antiterroriste, fraichement adoptée au Sénat et le très prochain projet de loi portant modification de la loi de 1955 sur l'état d'urgence.

L'état d'urgence prolongé

Commençons par le projet de loi prolongeant l'état d'urgence, déposé hier au Sénat, adopté le même jour en Commission des lois. Il ne comporte qu'un article. Il vise donc à proroger l'état d'urgence de 3 mois à compter du 26 février, mais également à autoriser sur toute la période, des perquisitions (notamment informatique) et le blocage d'accès aux sites provoquant à la commission d'actes de terrorismes ou en faisant l'apologie.
Selon le ministère de l'Intérieur, « dans le contexte de menace élevée et dans l'attente d'un renforcement durable et proportionné des moyens à la disposition des institutions », cette prorogation visera « à permettre à l'autorité administrative de continuer à assurer la sécurité du territoire par un contrôle et des mesures appropriées à l'encontre des personnes à l'égard desquelles il existe des raisons sérieuses de penser qu'elles constituent une menace pour la sécurité et l'ordre publics ».
Pour lui, pas de doute : le danger terroriste est toujours imminent, même si, au regard des derniers chiffres publiés par ses soins, seules 5 procédures de terrorisme ont été initiées suite aux 3 289 perquisitions administratives décidées depuis les attentats du Bataclan. Soit une moyenne de 657,8 perquisitions pour 1 procédure (dont on ne connaît pas encore le sort final). L'Intérieur, qui n'a eu de cesse de pratiquer la politique du chiffre, indique désormais que « l'efficacité des mesures prises dans le cadre de l'état d'urgence ne saurait toutefois se résumer à un bilan chiffré ni aux seules suites judiciaires qui y sont réservées, en ce que le recours à ces mesures pose les bases d'une lutte plus efficace contre le terrorisme et la radicalité ».

L'avant-projet de loi modifiant à nouveau la loi de 1955 sur l'état d'urgence

Ce texte est en principe programmé pour l'après-modification de la Constitution souhaitée par François Hollande. Comme la loi du 13 novembre 2015, votée après les attentats du Bataclan, il vient modifier la loi de 1955 sur l'état d'urgence. Si la première a autorisé les perquisitions informatiques, ce futur dispositif veut autoriser les saisies de ces mêmes données et matériels, toujours dans un cadre administratif sans intervention du juge.
Tel qu'analysé, ces perquisitions et saisies pourront viser toute personne « à l'égard de laquelle il existe des raisons sérieuses de penser que son comportement constitue une menace pour la sécurité et l'ordre publics ». La saisie sera en elle-même autorisée si l'autorité administrative a « des raisons sérieuses de penser qu'elle est nécessaire à la prévention des menaces pour la sécurité ou l'ordre publics » et si elle démontre que « l'exploitation d'un système informatique ou d'un équipement terminal présent sur les lieux où se déroule la perquisition » n'a pu être réalisée dans les temps de la perquisition. Ce qui sera toujours le cas face à un stockage de plusieurs gigas de données…
Les agents auront 15 jours pour fouiller tablettes, PC, disques durs externes, clefs USB, Smartphones. Le texte ne dit rien du sort des éléments saisis ou copiés à cette occasion, pas plus des retranscriptions ou les délais de conservation, qui sont donc illimités.

La proposition de loi des sénateurs Républicains et UDI

Au Sénat, encore, a été adoptée la proposition de loi signée Philippe Bas (LR), président de la commission des lois, François Zocchetto et Michel Mercier (UDI-UC). Tendant à renforcer l'efficacité de la lutte antiterroriste, elle n'a que peu de chances d'être adoptée par l'Assemblée nationale. Elle ne constitue pas moins un bouillon de culture, les élus de l'opposition ne voulant pas se laisser coiffer par les socialistes dans ce concours Lépine des textes sécuritaires. D'ailleurs, ces derniers n'ont pas hésité à plonger leur doigt dans ce pot de confiture pour sucrer davantage leurs propres textes, comme on le verra plus bas.

Mais que trouve-t-on dans cette « PPL » ?

Faciliter l'accès aux données informatiques lors des perquisitions

Depuis la loi contre le terrorisme de novembre 2014, lors d'une perquisition, les officiers de police judiciaire peuvent se voir autoriser à accéder aux données stockées ou accessibles depuis le système informatique qui y est implanté. Ils peuvent à cet effet requérir toute personne susceptible « d'avoir connaissance des mesures appliquées pour protéger les données auxquelles il est permis d'accéder dans le cadre de la perquisition » ou « de leur remettre les informations permettant d'accéder aux données ». La PPL porte à 45 000 euros le fait de s'abstenir de répondre dans les meilleurs délais à leurs demandes, contre 3 750 euros aujourd'hui.

Un article 4 permet quant à lui de faciliter grandement les interceptions judiciaires. Il fait sauter l'autorisation du premier ministre normalement exigée pour développer, utiliser, diffuser des outils techniques développés pour casser le secret des correspondances. Le juge pourra faire ainsi appel à des experts ou au centre technique d'assistance (CTA) afin de concevoir ces mouchards informatiques.

Autoriser la saisie des emails stockés

En principe, les interceptions de sécurité (les « écoutes » téléphoniques, mais également des échanges électroniques) ne peuvent porter que sur le flux des correspondances. La PPL veut autoriser désormais les officiers et agents de police judiciaire « à accéder, en tous lieux, aux correspondances numériques émises ou reçues » depuis une adresse ciblée. Outre les échanges dynamiques, l'interception ciblera donc le stock des correspondances.

Autoriser les IMSI catcher judiciaires

Dans le cadre d'une enquête de flagrance concernant la criminalité organisée, l'article 5 autorise le parquet à installer des fausses antennes relais (ou IMSI catchers) afin de recueillir les données techniques de connexion pour identifier un terminal, un numéro d'abonnement et géolocaliser les appareils.

Mieux : comme dans l'univers du renseignement, ces IMSI catchers pourront également être déployés pour faire de l'interception de correspondances. Simplement, le formalisme procédural sera alors plus lourd, puisque la violation de la vie privée est plus profonde, du moins pour les personnes concernées.

Micros et caméras espions

Toujours sur autorisation du juge judiciaire, à la demande du procureur, les OPJ et les agents pourront installer en douce des micros et caméras espions dans des lieux, véhicules privés ou publics. À cette fin, procureur, juge d'instruction ou OPJ pourra « requérir tout agent qualifié d'un service, d'une unité ou d'un organisme placé sous l'autorité ou la tutelle du ministre de l'Intérieur ». Ces personnes seront autorisées à s'introduire dans ces espaces, même de nuit.

Ce dispositif ne concerne cependant « que » les enquêtes de flagrance et les enquêtes préliminaires en matière de lutte contre la criminalité organisée. La PPL démultiplie néanmoins l'intervention du procureur dans ces opérations, par exemple pour dresser le procès-verbal de chaque étape.

Délit de consultation des sites terroristes

Le texte de l'opposition compte introduire dans notre droit le délit de consultation habituelle de sites terroristes, ou plus exactement « mettant à disposition des messages, images ou représentations soit provoquant directement à la commission d'actes de terrorisme, soit faisant l'apologie de ces actes ».

Il est certes prévu une exception pour les journalistes, la recherche scientifique ou lorsqu'il s'agit de glaner des preuves en justice, mais pour les autres curieux, le seul fait de lire un peu trop souvent ces contenus odieux sera condamné de deux ans d'emprisonnement et 30 000 euros d'amende. Rien n'est dit sur les modalités pratiques de cette répression, spécialement comment seront jaugés les flux de visiteurs pour déceler ce critère de l'habitude.

L'entrave au blocage des sites

Le seul fait d'entraver les mesures de blocage, par exemple en reproduisant les données du site en cause, sera puni de cinq ans d'emprisonnement et de 75 000 euros d'amende. Cette sanction tombera également lorsqu'un individu reproduira dans un tweet ces mêmes données, s'il est toutefois démontré qu'elle avait pour volonté d'entraver le blocage.

Le nouveau projet de loi renforçant la lutte contre le terrorisme

Ce projet de loi déposé également cette semaine au Sénat par le Gouvernement, veut renforcer la lutte contre le crime organisé, le terrorisme et leur financement, tout en « améliorant l'efficacité et les garanties de la procédure pénale ». Puisqu'on est ici face à un projet de loi, son avenir est nettement plus assuré qu'une simple proposition parlementaire venant de l'opposition sénatoriale. Le texte contient de nombreuses mesures touchant au secteur des nouvelles technologies.

Les IMSI Catcher judiciaires, là encore

L'article 2 du projet de loi reprend l'idée de la proposition de loi de Philippe Bas, à savoir autoriser le recours à l'ISMI catcher pour la criminalité et la délinquance organisées, afin de glaner les données de connexion passant sous ses radars.

Comme dans la PPL, cet usage sera possible pour une durée d'un mois, renouvelable autant de fois que nécessaire. Le projet de loi du gouvernement apporte cependant une nuance : il veut aussi permettre au seul procureur de la République d'autoriser seul ces grandes oreilles électroniques « en cas d'urgence ». Dans une telle hypothèse, son autorisation devra simplement être confirmée par le juge des libertés et de la détention dans le délai de 24 heures « à défaut de quoi il est mis fin à l'opération ».

Sonorisation et captation dans les lieux privés, là encore

Là encore, l'inspiration de l'exécutif est commune à celle des sénateurs de l'opposition. Selon l'étude d'impact, l'article 3 permet « avec l'autorisation du juge des libertés et de la détention, la sonorisation, la fixation d'images et la captation de données en enquête de flagrance ou préliminaire, pour une durée d'un mois renouvelable une fois, soit pour une durée beaucoup plus réduite que celle désormais fixée pour l'instruction, de quatre mois renouvelable jusqu'à deux ans ».

Bien entendu, selon le projet de loi, « aucune séquence relative à la vie privée étrangère aux infractions visées dans les décisions autorisant la mesure ne [pourra] être conservée dans le dossier de la procédure ». Ces faits privés seront donc connus des agents, mais devront être gommés du dossier...

Le même article autorise tout autant l'interception des mails déjà archivés, « stockés dans un système informatique » qu'il soit local ou distant.

Coups d'achat notamment sur Internet

À l'article 8, le projet de loi facilite la technique dite du coup d'achat à l'instar de ce qui existe déjà pour le trafic de stupéfiants. Un enquêteur va pouvoir acheter des armes, dans le cadre d'un possible trafic portant sur ces biens, pourquoi pas sur Internet. Ces opérations lui permettront de constater une infraction et tenter d'identifier les auteurs et les complices.

Extension des compétences des tribunaux français pour les infractions sur Internet

L'article 11 prend pour racine le rapport du procureur général Marc Robert sur la cybercriminalité. Il étend la compétence pénale des juridictions française dès lors qu'une infraction est commise à l'encontre d'un Français ou d'une entreprise ayant son siège dans le pays.

Tout crime ou délit réalisé sur Internet sera réputé réalisé en France s'il vise une personne physique résidant en France ou une personne morale qui y a son siège. Cela ne vaudra que pour les infractions punies d'une peine de prison, et donc pour la contrefaçon.

Contre le piratage informatique commis en bande organisée

Le projet de loi autorise au même article 11, le recours aux moyens de procédure exceptionnels à l'encontre du piratage informatique commis en bande organisée : surveillance portée à tout le territoire national, infiltration, enquête sous pseudonyme, (mais pas de garde à vue pendant 96 heures).

Fouille des bagages... et des fichiers sur les PC qui s'y trouvent ?

Par ailleurs, l'article 17 étend les pouvoirs des forces de l'ordre. Lors d'un contrôle d'identité ou d'une « visite » de voiture, ils pourront également procéder à l'inspection visuelle, mais aussi à la fouille de bagages.

Une question s'impose : est-ce que la fouille des bagages pourra être étendue aux fichiers stockés par exemple dans un ordinateur portable, trouvé dans le coffre d'un véhicule ou le sac d'un piéton ?

Questionné, Me Éric Morain, pénaliste, nous explique qu' « en matière douanière le portable est considéré comme une marchandise et peut à ce titre être fouillé par les douanes. L'assimiler à un bagage pour vérifier qu'il n'est pas dangereux en soi par un contrôle visuel extérieur, oui. Autoriser sa fouille me paraîtrait toutefois exagéré dans le cadre d'un simple contrôle d'identité ».

Même analyse de Nicolas Hervieu, juriste en droit public et droit européen des droits de l'Homme : « En l'état actuel de cet article 17, interpréter la notion de "bagage" de façon extensive pour permettre l'accès aux données stockées dans un ordinateur serait plus que risqué d'un point de vue juridique. En effet, le droit français actuel prévoit globalement des régimes distincts pour la fouille ou saisie de biens matériels, d'une part, et la consultation de données numériques, d'autre part (voir par exemple l'article 11 I de la loi du 3 avril 1955 relative à l'état d'urgence). Or, sur le fondement de l'article 8 de la Convention européenne, la Cour européenne exige que toute ingérence dans la vie privée - telle une consultation de données - soit prévue par une législation claire, précise et prévisible. Par conséquent, une "fouille numérique" fondée sur un texte prévu prioritairement pour les fouilles de bagages "physiques" serait très fragile juridiquement ».

Des comportements et des fichiers

Autre grande nouveauté, avec l'article 18 du PJL, les forces de l'ordre qui vérifient une identité, pourront retenir durant 4 heures, une personne sur place ou dans les locaux de la police. Il suffira qu'il « existe des raisons sérieuses de penser que son comportement est lié à des activités à caractère terroriste » ou bien « qu'elle est en relation directe et non fortuite avec une personne ayant un tel comportement ». Une disposition applicable aux mineurs.

Pendant ces 4 heures de retenue, sans avocat, un OPJ aura le droit de consulter les fichiers « qui intéressent la sûreté de l'État, la défense ou la sécurité publique » ou « qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté ». Soit l'ensemble des fichiers sécuritaires. On devine sans mal les suites douloureuses, si son nom venait à transparaitre d'une manière ou d'une autre dans ces fiches secrètes…

Interception de communication (écoutes)

Suite à un arrêt de la CEDH, l'exécutif veut mettre à jour le droit des interceptions judiciaires. L'article 25 « renforce les garanties applicables au cours de l'instruction en matière d'interceptions de communication, en exigeant des décisions motivées » de la part du juge. Surtout cet article limite dans le temps ces écoutes : la durée maximale pour une ligne déterminée sera d'un an, voire deux ans pour la délinquance et la criminalité organisées. Pour les professions sensibles (avocat, parlementaire ou magistrat), des garanties procédurales supplémentaires sont apportées.

Des caméras piétons au veston

Expérimentées depuis l'automne 2012, ces caméras ont pour vocation de prévenir les incidents lors de l'intervention des forces de l'ordre : équipés de ces dispositifs électroniques, policiers et gendarmes pourront ainsi capter images et sons passant sous l'objectif (notre actualité). Ce n'est pas seulement un système anti débordement : elles serviront également à constater une infraction et aider à la collecte de preuve.

Selon le projet de loi, leur usage sera toutefois optionnel. L'enregistrement sera « déclenché lorsqu'un incident se produit ou, eu égard aux circonstances de l'intervention ou du comportement des personnes concernées, est susceptible de se produire ». C'est évidemment le porteur qui décidera d'appuyer ou non sur le bouton « Record ».

Ces caméras seront visibles : elles devront être « portées de façon apparente » et « un signal visuel spécifique » indiquera si l'enregistrement est en cours. « Le déclenchement de l'enregistrement fait l'objet d'une information des personnes enregistrées, sauf si les circonstances l'interdisent » temporise le texte.

Ces enregistrements, inaccessibles aux personnels auxquels les caméras sont fournies, seront ensuite conservés pendant 6 mois, sauf bien sûr s'ils sont utilisés dans le cadre d'une procédure judiciaire, administrative ou disciplinaire.

La PNIJ va devenir obligatoire

Signalons l'article 33 du projet de loi qui, tel que résumé par l'étude d'impact annexée au projet de loi, veut rendre « obligatoire le recours à la plate-forme nationale des interceptions judiciaires [PNIJ], dans un souci d'efficacité, de meilleur contrôle des frais de justice et d'une plus grande confidentialité et sécurisation des opérations ».

À cette fin, le Code de procédure pénale et le Code des douanes seront mis à jour pour contraindre magistrats, services d'enquête et agents spécialement habilités à recourir à cette plateforme.

Rappelons que son but est de centraliser les demandes adressées aux opérateurs de communication électroniques (OCE) pour glaner les métadonnées et le contenu des communications électronique d'une personne déterminée (téléphone fixe, mobile, internet, etc.).

Placée sous la responsabilité du garde des Sceaux, et sous le contrôle d'une personnalité qualifiée (Mireille Imbert Quaretta, l'ex de la Hadopi), la PNIJ est censée fluidifier les échanges avec les OCE. Son déploiement, commencé le 9 février 2015, devrait être achevé le 11 avril 2016.

L'exécutif promet au passage également d' « adapter les textes relatifs aux scellés et au déchiffrement des données afin de tenir compte des fonctionnalités de la plateforme et d'alléger la charge des services de la justice ». Il faudra attendre pour connaître les détails précis puisque ces modifications se feront par voie d'ordonnance, afin de contourner la procédure parlementaire classique…

Des fichiers policiers nettoyés

La Cour européenne des droits de l'Homme avait tapé sur les doigts de la France dans l'arrêt Brunet c/ France du 18 septembre 2014, dégommant les carences du fichage policier, en l'espèce du STIC, le système de traitement des infractions constatées. Elle pilonnait en

particulier la conservation de faits classés sans suite, occasionnant du coup une atteinte à la vie privée du principal concerné.
Après cette baffe sur l'autel des droits de l'Homme, le droit français sera donc mis à jour, toujours par voie d'ordonnance. Le gouvernement envisage « de détailler les critères pris en compte par l'autorité judiciaire pour décider de l'effacement ou du maintien des données dans le fichier ». Ce choix pourrait dépendre « des finalités du fichier appréciées au regard de la nature et des circonstances de commission de l'infraction et de la personnalité de l'intéressé ».
Ce n'est pas tout, puisqu'« il est par ailleurs envisagé de prévoir la possibilité pour le procureur de la République de procéder à l'effacement des données du fichier quel que soit le motif de classement sans suite et non plus comme actuellement uniquement lorsque celui-ci est motivé par l'absence de charges. »
Dans son analyse d'impact, l'exécutif estime que « la création de nouvelles possibilités d'effacement du fichier [sera] de nature à entraîner une augmentation du nombre de requêtes en effacement des données transmises aux procureurs de la République ». Bref, il s'attend à une belle vague de demandes d'effacement, soit le plus joli témoignage de la performance actuelle de ces fichiers.
https://www.nextinpact.com/news/98387-le-volet-cyber-nouveaux-textes-securitaires.htm

Cyberfraude: la menace (presque) fantôme

Comment se défendre quand on ne voit pas le danger? C'est l'une des difficultés soulevées par les participants de la conférence "Cyberfraudes: bonnes pratiques et moyens d'action" qui s'est tenue à l'occasion du Congrès des Daf, le 7 juillet dernier. Retour sur cet événement.
140 jours. C'est le délai moyen entre la survenance d'une cyberattaque et le moment où l'entreprise victime découvre qu'elle a été piratée. Soit près de 5 mois durant lesquels les fraudeurs ont tout le loisir d'exploiter les données, de les revendre, de monter des arnaques sur mesure pour s'attaquer à cette société... Ce chiffre de 140 jours, avancé par Helena Pons-Charlet, head of legal chez Microsoft, à l'occasion du dernier Congrès des Daf et directeurs financiers(1) qui s'est tenu le 7 juillet 2016 à Paris, jette une lumière crue sur l'un des dangers sous-estimés de la cybercriminalité: son invisibilité. Or, si une entreprise sera parfaitement consciente de subir une attaque lorsqu'un cryptovirus infecte son système, une grande partie de l'iceberg de la cybercriminalité reste immergée, alors que la menace est quotidienne. Les données, graal du hacker En 2015, selon les données de Microsoft, la fraude a provoqué 400 Md€ de perte de CA au niveau mondial. Et la menace ne fait que s'étendre: 71% des entreprises déclarent avoir été victimes d'une tentative de fraude, selon l'éditeur de logiciels. Et il ne s'agit là que de celles qui ont identifié l'attaque... Mais que cherchent les hackers? Bien souvent, une chose dont les dirigeants n'ont pas encore bien mesuré l'entière valeur : les données de l'entreprise. "Les données, c'est la nouvelle monnaie du XXIe siècle", affirme Helena Pons-Charlet. En effet, "une cyberattaque est bien souvent le point d'entrée d'un mécanisme de fraude", avertit Sébastien Hager, souscripteur assurance France chez Euler Hermes. Elle permet de recueillir des informations confidentielles qui constitueront la base d'une tentative de détournement crédible, du type fraude au président. Et l'essor du BYOD (bring your own device) ne fait qu'accroître le danger: non seulement il entraîne des failles de sécurité en laissant des appareils privés, pas toujours bien protégés, accéder au système d'information de la société, mais en cas d'attaque, il offre également au fraudeur un accès à un panel de données encore plus large, professionnelles et personnelles. La cybercriminalité se professionnalise Les petites entreprises sont des cibles de choix pour les hackers. "Ma structure est bien trop petite pour intéresser les fraudeurs", se disent beaucoup de chefs d'entreprise. Grave erreur! "Il est plus difficile aujourd'hui de s'attaquer aux grandes

entreprises via leur SI", souligne François Nogaret, associé chez Mazars. Ces dernières disposent de moyens suffisants pour protéger efficacement leur SI. C'est pourquoi les petites entreprises, qui n'ont pas forcément mis en place autant de procédures de sécurité que les grands comptes, deviennent des cibles de choix pour les hackers. Parallèlement, les activités de cybercriminalité se sont démocratisées. Deux raisons à cela: la disponibilité de l'information (par exemple grâce aux réseaux sociaux, très pratiques pour tout savoir sur la famille, les relations amicales et dates de vacances des collaborateurs) et l'industrialisation des outils de fraude. "Aujourd'hui, un hacker va vendre son produit à des fraudeurs qui ne sont pas forcément qualifiés", révèle François Beauvois, commissaire de police, chef de la division anticipation et analyse à la sous-direction de la lutte contre la cybercriminalité. Tutoriels de formation en ligne, service après-vente... Les hackers sont devenus des businessmen, fournissant aux fraudeurs toute une gamme d'outils prêts à l'emploi. "Nous assistons au développement d'une sous-traitance du crime, en mode "crime as a service"!", déclare François Beauvois. On est loin de l'image d'Épinal de l'étudiant surdoué qui joue les hackers: "Les entreprises sont face à des mafias", résume David Luponis, senior manager chez Mazars.

Comment se déroule une tentative de fraude?

Olivier Peiffer, CEO de Polimiroir Group, ETI industrielle spécialisée dans les prestations mécaniques et de sous-traitance étendues, a apporté un retour d'expérience sur les tentatives de fraude subies par son entreprise.

Polimiroir est une société multisite, composée de plusieurs petites structures d'une cinquantaine de personnes, et qui développe une importante activité à l'export. La société a été victime de tentatives de fraude au président: des personnes très bien informées, connaissant parfaitement la vie de l'entreprise et des collaborateurs (recours au tutoiement ou au vouvoiement dans les échanges, prénoms des enfants des salariés, dates de congés ou d'arrêt maladie des uns et des autres, etc.), ont mené des attaques très ciblées en empruntant l'identité d'Olivier Peiffer. En utilisant le mail et le numéro de téléphone de ce dernier, le fraudeur contactait des assistants et jouait sur la persuasion pour les convaincre d'effectuer des virements. "Les fraudeurs n'agissent pas au hasard, ils étudient toutes les informations en amont pour avoir une approche logique. Ils essayent tout jusqu'à trouver une faille, et jouent sur la rapidité des échanges téléphoniques", témoigne Olivier Peiffer. Ces attaques, qui n'ont heureusement pas abouti, se sont renouvelées tous les jours pendant deux mois. Jusqu'à ce qu'Olivier Peiffer échange directement avec l'imposteur au téléphone, celui-ci comprenant alors qu'il était démasqué. Cette expérience illustre bien le caractère sensible des données de l'entreprise et des collaborateurs. Des informations en apparence anodines, telles que les dates de vacances ou les prénoms des enfants, susceptibles d'être partagées sur les réseaux sociaux, se transforment en failles de sécurité lorsqu'un fraudeur décide de mener une enquête minutieuse en vue de monter une arnaque. De même, accéder via une cyberattaque invisible aux mails des interlocuteurs-clés de l'entreprise permet de tout savoir du style, du ton et de la teneur des échanges entre collaborateurs. Pour mieux les imiter.

http://www.daf-mag.fr/Thematique/achats-1033/Breves/Cyberfraude-menace-presque-fantome-307688.htm#wzyaYQ0A2yMw1bsf.97

La cyberfraude, phénomène en expansion

Vie quotidienne, contexte professionnel, économie… Les nouvelles technologies prennent de plus en plus de place dans notre société. Cette situation favorise le développement de la cyberfraude, qui continue son inquiétante progression au classement des tentatives de fraude. Le commissaire François Beauvois, spécialiste du sujet, dépeint avec précision le panorama de la cyberfraude.

Comment définiriez-vous la cyberfraude ?

On parle de cyberfraude lorsque est commise une infraction dont l'élément informatique est l'outil ou la finalité. Il peut par exemple s'agir de piratage informatique, ou du blocage de l'accès à un site marchand pour ensuite réclamer une rançon. Le panorama des cyberfraudes évolue constamment, à l'image de ses auteurs, habitués à évoluer dans un univers technologique en perpétuelle mutation. Parmi le vaste panel des cyberfraudes actuellement observées, certaines frappent plus particulièrement les entreprises françaises, comme l'extorsion.

Pouvez-vous nous en dire plus sur ce type de cyberfraude ?

L'extorsion est une forme très répandue de fraude du fait de son faible coût, et des fortes marges qu'elle dégage. Elle a été largement popularisée grâce à l'émergence des outils d'anonymisation (mails anonymes, crypto-monnaies), nécessaires à ce genre d'activité. Le déni de service est par exemple une forme d'extorsion. Il consiste à solliciter massivement un serveur afin de le saturer : lorsque le nombre de requêtes dépasse les capacités de réponse du serveur, celui-ci n'est plus en mesure de répondre, et, du point de vue de l'utilisateur, le site Internet consulté ne répond plus. En parallèle de cette attaque, les cybercriminels procèdent à une demande de rançon : ils réclament une forte somme d'argent pour faire cesser l'attaque ou éviter qu'elle ne se reproduise. La victime est alors contactée par l'auteur via un service de mail anonyme utilisant le réseau Tor, donc quasiment intraçable. La rançon est généralement exigée en bitcoins ou toute autre monnaie anonyme.

Techniquement, comment fonctionne la cyber-extorsion ?

La victime reçoit un mail frauduleux dont la forme est en tout point conforme aux standards pratiqués dans le milieu professionnel (pas de fautes d'orthographe, pièce jointe type facture format Office, ton approprié), et l'ouvre. Pour pouvoir activer sa charge malveillante, le pirate a besoin de l'activation des macros, des mini-programmes informatiques, sous Microsoft Office. Alors, plutôt que d'employer des artifices complexes, le pirate se contente de demander poliment à la victime de faire le travail. Et ça fonctionne ! La victime, qui veut satisfaire sa curiosité, active les macros, qui téléchargent le logiciel malveillant. Ce logiciel va rendre inutilisables tous les fichiers de type Office, Adobe Reader, et autres, que ce soit sur le disque dur de la machine, les lectures réseau ou bien les services Cloud (Google Doc, Dropbox). Pendant ce temps, le programme prend aussi le contrôle de l'ordinateur et empêche l'utilisateur d'agir en bloquant le clavier. Un message de demande de rançon s'affiche : la marche à suivre pour payer en crypto-monnaie est détaillée. L'utilisateur est alors enjoint de payer la rançon s'il veut que lui soit communiquée la clé de déchiffrement, seul moyen pour lui de pouvoir récupérer ses fichiers de travail. L'intérêt de cette fraude est qu'elle est relativement simple à mettre en œuvre (système de diffusion, serveurs d'envoi de clé de déchiffrement, wallet bitcoin) et donc très rentable. Les noms de ces logiciels malveillants sont actuellement Petya, Locky, Cerber et maintenant Zepto.

Connaît-on d'autres types de cyberfraude qui peuvent inquiéter les entreprises françaises ?

Une autre forme de fraude plus élaborée est le malware dit bancaire. Son mode de propagation est similaire à celui du rançongiciel présenté ci-dessus : un mail infecté dont les macros insérées dans la pièce jointe vont télécharger une charge active. Toutefois, son fonctionnement est plus subtil et insidieux. L'objectif des malwares bancaires est de voler des données. Toutes les formes de données saisies par l'utilisateur vont pouvoir être capturées : touches tapées sur le clavier, clics sur les sites Internet et claviers virtuels, consultations web transitant par le navigateur, etc. L'objectif pour le fraudeur est de voler le maximum d'informations monétisables : informations bancaires, identifiants/mots de passe de comptes bancaires en ligne. Cela suppose une structure beaucoup plus lourde que dans le cas des rançongiciels. Les données sont envoyées à des exécutants qui se connectent sur les comptes

en ligne pour procéder à des virements frauduleux sur des comptes bancaires de prête-nom, les «mules». Ces personnes sont des complices plus ou moins conscients du dispositif. Le profil va de la personne en situation de détresse financière qui accepte un travail bien rémunéré à l'individu malhonnête parfaitement conscient des implications de ses actes. L'argent est ensuite collecté en liquide par un «superviseur» responsable d'un cheptel de mule. Enfin, l'argent est transféré par virement et blanchi selon divers procédés (achats de smartphones coûteux, voire de manteaux de fourrure). On le voit, un tel dispositif n'est pas à la portée du malfrat du dimanche. Seule une structure criminelle organisée et pérenne peut se permettre d'entretenir un tel système. Toutefois, les gains semblent être à la hauteur de l'investissement. Un exemple type de ce genre de fraude est le malware Dridex.

Observez-vous le développement de nouvelles formes de cyberfraude ?

Les nouvelles formes de cyberfraude résident plus dans leurs modalités : le crime devient un service. Le hacker qui a programmé son malware va le tester sous des formes spécifiques (service payant, sous-traité), puis le vendre au moyen d'un système de licence. L'utilisateur final pourra acheter, en plus du malware, la prestation de diffusion (elle aussi fournie par un autre acteur). Le marché est similaire à celui de l'économie classique dont il s'inspire : sous-traitance et retour sur investissement.

Quels conseils donneriez-vous aux entreprises pour faire face à la cyberfraude ?

Plusieurs types de mesures permettent de se protéger contre la cyberfraude. Elles peuvent être :

- Structurelles : mettre en place un système de sauvegarde des données hors ligne, installer une sécurité minimum : antivirus, pare-feu et les maintenir à jour. Cela ne demande pas de lourds investissements mais l'implication d'au moins deux personnes est indispensable pour assurer une couverture toute l'année.
- Financières : traiter ce risque comme les autres : provisions, assurance ou autre.
- Ressources humaines : sensibiliser le personnel sur les bons réflexes à avoir : traiter tout mail d'une source inconnue avec prudence. En cas de comportement suspect de la machine ou de doute, débrancher la prise réseau de la machine ou la prise électrique et évoquer le sujet avec une personne compétente

http://www.optionfinance.fr/services/lettres-professionnelles/la-lettre-du-risque-clients-avec-euler-hermes/comment-reagir-face-a-la-fraude/la-cyberfraude-phenomene-en-expansion.html

Une gigantesque cyber fraude découverte

Près d'un milliard de dollars auraient été dérobés dans plus d'une centaine d'établissements bancaires implantés dans 30 pays, révèle un rapport de l'éditeur russe Kaspersky dévoilé par la presse anglo-saxonne.

Le montant précis n'est pas encore connu, il serait compris entre 300 millions et un milliard de dollars. En raison de l'ampleur de la fraude et surtout de la nature des cibles de la cyber attaque, les banques, Kaspersky reste relativement flou et notamment sur l'identité des banques victimes. L'éditeur précise toutefois que les principales victimes sont des banques russes, américaines, allemandes, chinoises, ukrainiennes et canadiennes.

«L'attaque la plus sophistiquée»

Les membres du gang de cybercriminels sont d'origine russe, ukrainienne et chinoise. L'éditeur russe collabore avec Interpol et Europol sur ces investigations. «Ces attaques révèlent une nouvelle fois que les criminels sont prêts à exploiter toutes les failles et les vulnérabilités de tous les systèmes», indique Sanjay Virmani.

Chris Dogget, directeur de la filiale américaine de Kaspersky, affirme que le cybergang Carbanak (du nom du malware déployé) prouve que les attaques sont de plus en plus sophistiquées. «C'est probablement l'attaque la plus sophistiquée que nous ayons jamais vu en termes de tactiques et méthodes que les cyber criminels ont utilisé pour rester cachés».
http://www.lefigaro.fr/flash-eco/2015/02/16/97002-20150216FILWWW00058-une-gigantesque-cyber-fraude-decouverte.php

Le cyber-terrorisme, menace imminente, estiment des experts

Le cyber-terrorisme, utilisation des nouvelles technologies pour provoquer des dégâts majeurs par des groupes comme l'État islamique, est une menace imminente qu'il faut prendre au sérieux, ont estimé mardi à Davos de hauts responsables.

Lors d'une table-ronde consacrée au "Terrorisme à l'âge digital", le prince saoudien Turki bin Faisal Al Saud, ancien chef des services de renseignements de son pays, a ainsi estimé que "la menace inquiétante est le recours au cyber-terrorisme. Les groupes terroristes, grâce à leur bonne maîtrise des technologies modernes, vont l'employer pour faire avancer leur cause".

"Ils cherchent les façons les plus mortelles d'utiliser les technologies modernes, a-t-il ajouté. "Ils ne s'en priveront pas".

Pour le général pakistanais à la retraite Raheel Sharif, qui commandait jusqu'en novembre dernier l'armée pakistanaise, il s'agit là "d'une vraie menace. Avec les progrès technologiques augmentent les risques que quelqu'un pirate un système sophistiqué et s'en serve pour provoquer le maximum de dégâts".

Ce genre de menace "devrait nous empêcher de trouver le sommeil", a-t-il ajouté. "Nous devons trouver de meilleurs moyens de protéger les systèmes informatiques. Il peut y avoir des piratages bien plus dangereux que ceux qui consistent à pénétrer dans les systèmes de partis politique", a-t-il dit, évoquant le piratage, attribué par la CIA à la Russie, du parti démocrate américain pendant la campagne électorale aux États-Unis.

"Ce serait une évolution logique pour des groupes qui deviennent de plus en plus experts en la matière", a pour sa part estimé Rob Wainwright, directeur d'Europol. "Et même s'il leur manque des savoir-faire, ils peuvent aisément les acheter sur le darknet (partie d'internet cryptée et non référencée dans les moteurs de recherche classiques qui offre un plus grand degré d'anonymat à ses utilisateurs, ndlr), où le commerce d'instruments de cyber-criminalité est florissant".

"Cela dit, il n'est pas si facile de s'en prendre aux infrastructures cruciales de la plupart des pays", a-t-il estimé. "Et ce n'est pas quelque chose qui provoque un effet aussi immédiat et spectaculaire que de tirer à l'arme automatique dans une salle de spectacle. Je ne suis pas certain que cela va advenir, mais c'est clairement un scénario auquel nous devons nous préparer".

La patron d'Europol a précisé que le seul site Twitter avait fermé, au cours de la dernière année, un quart de million de comptes en lien avec les jihadistes de l'organisation Etat islamique et que Europol estimait que pas moins de 90 plateformes différentes et médias sociaux étaient actuellement utilisés par l'E

http://www.atlasinfo.fr/Le-cyber-terrorisme-menace-imminente-estiment-des-experts_a78730.html

Le marché des Bitcoins est en plein essor au Maroc

Dans le domaine du virtuel, une monnaie existe : Le Bitcoin. D'autres monnaies virtuelles sont disponibles sur le marché mondial.

Surprise, le Maroc observe un essor rapide de l'utilisation du bitcoin et autres. Plus de 200 000 dollars de Bitcoins s'échangent au quotidien dans le royaume, indique Aziz Elmi, trader professionnel de cryptographie et leader d'une communauté dans le même domaine au sein du pays, relayé par *Coin Telegraph.*

Aziz Elmi est l'un des développeurs principaux d'Atlas Coin, une des rares monnaies africaines (il en existe deux sur le continent). Ce dernier est très optimiste quant au potentiel du Maroc dans le monde des monnaies digitales.

Le Maroc est ainsi perçu comme un des leaders dans l'adoption du Bitcoin, à l'instar du Kenya, du Ghana et du Nigéria. Selon le trader, les Marocains utilisent le Bitcoin pour investir, surtout avec l'essor des «Cloud mining sites» (Des sociétés qui permettent aux utilisateurs d'acheter la capacité d'extraction de matériel dans les centres de données). Les ressortissants du royaume injectent beaucoup d'argent dans ces entreprises-là. «Chaque jour, des milliers de dollars sont échangés au Maroc, spécialement via les réseaux sociaux tels que Facebook, WhatsApp et Twitter. J'ai personnellement créé plusieurs groupes d'échanges qui sont prospères grâce à l'activité générée», déclare Aziz Elmi.

Cependant, l'industrie Bitcoin au Maroc est entourée d'une sorte de secret et de peur. Les échanges se font dans la discrétion selon ce trader professionnel. «Nous sommes très précautionneux sur ce terrain car nous ne savons pas quel sera la réaction du gouvernement une fois que les échanges seront publics», ajoute l'expert en monnaie virtuelle. Et Aziz Elmi de conclure : «Le gouvernement marocain ne s'est jamais penché sur la question. C'est encore nouveau pour les représentants du royaume»

https://www.yabiladi.com/articles/details/51033/marche-bitcoins-plein-essor-maroc.html