Tendances et prévisions en cybercriminalité pour 2015 | Le Net Expert Informatique

Tendances et prévisions en cybercriminalité pour 2015

Augmentation des attaques ciblées En 2015, les attaques ciblées deviennent encore plus sophistiquées. Souvent appelées APT (Advanced Persistant Threats), elles sont différentes des cyberattaques traditionnelles. Conçues pour attaquer des victimes spécifiques et pour être silencieuses, les attaques ciblées peuvent être cachées et non détectées dans des réseaux insuffisamment sécurisés.
"Le vecteur des attaques ciblées profite généralement des attaques d'ingénierie sociale", explique Pablo Ramos, chef du laboratoire de recherche ESET en Amérique Latine. "C'est alors que la manipulation psychologique est utilisée pour pousser les victimes potentielles à commettre certaines actions ou à divulguer des informations confidentielles. Les attaques peuvent également prendre l'apparence d'exploits jour-zéro, où elles profitent de vulnérabilités nouvellement découvertes dans un système d'exploitation ou une application particulière."
Au cours de 2014, le blog WeLiveSecurity d'ESET a publié un certain nombre d'analyses approfondies concernant les attaques ciblées, telles que BlackEnergy campaign et Operation Windigo .

Les systèmes de paiement en ligne attirent plus de malware
Alors que toujours plus de personnes adoptent les systèmes de paiement en ligne pour des biens et des services, ces systèmes deviennent encore plus attrayants pour les concepteurs de malware intéressés par les gains financiers.
2014 a vu la plus grande attaque connue à ce jour en matière de paiement digital, quand un pirate a récolté plus de 600.000 dollars US en Bitcoins et Dogecoins en utilisant un réseau de machines infectées.
ESET a signalé les attaques effectuées en mai contre Dogevault site , où les utilisateurs du très populaire portefeuille électronique ont signalé des retraits non autorisés de leurs comptes avant que le site ne soit obligé d'être déconnecté suite à la destruction des données du site par les attaquants. On estime que 56.000 dollars US ont été volés aux utilisateurs du portefeuille en ligne.
Nous avons aussi vu des attaques de force brute telles que Win32/BrutPOS , qui ont essayé d'accéder aux comptes protégés par un mot de passe en les bombardant de mots de passe populaires afin d'avoir un accès à distance – un rappel général en faveur de l'utilisation de mots de passe forts et uniques.

L'internet des choses – nouveaux jouets pour pirates
Alors que de nouveaux appareils se connectent à internet et stockent plus de données, ils deviennent un vecteur d'attaque attrayant pour les cybercriminels. Au cours de 2014, nous avons trouvé plus de preuves de la hausse de cette tendance. Lors de la conférence Defcon, on a vu les attaques sur les voitures en utilisant le dispositif ECU, ou sur la voiture Tesla qui a été piratée afin d'en ouvrir les portes alors qu'elle roulait.
Des attaques et des concepts ont aussi été montrés dans le secteur de la télévision sur différents systèmes, systèmes biométriques sur smartphones, routeurs – pour ne pas mentionner Google glasses.
C'est un domaine émergent pour la cybercriminalité et il restera un secteur de concentration pour l'industrie de la sécurité. Alors que cela pourrait prendre des années avant de devenir une menace grave, il faut agir dès à présent afin de mieux prévenir ce type d'attaques.
Plus d'information
Le rapport complet est disponible sur WeLiveSecurity.com.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : https://mail.google.com/mail/u/0/?hl=fr&shva=1#inbox/14be54fe5faeb40f?compose=14be53ae312f08d7

« Aux mains d’une personne malveillante, l’utilisation d’un drone peut constituer un risque réel » | Le Net Expert Informatique

« Aux mains d’une personne malveillante, l’utilisation d’un drone peut constituer un risque réel »

Y a-t-il différentes bandes de fréquence utilisées en fonction du type ou de la taille du drone ?

Sur les drones civils, à ma connaissance, il n’y a qu’une seule bande de fréquence. Ce n’est pas le cas pour les drones militaires. Mais ceux qui ont survolé Paris à plusieurs reprises rentrent tous dans la catégorie des drones civils.

Y aurait-il par conséquent un risque d’interférences avec d’autres secteurs d’activité (aviation, GPS ou autres) ?
Il y a toujours des risques d’interférences possibles, comme le brouillage des antennes de télévisions. Il y a aussi un risque de perdre le contrôle du drone en cas de champ magnétique ou de fréquence assez forte.

Est-il possible pour un service sécuritaire étatique de contrôler un drone et de le dévier de sa trajectoire, en plein vol, au cas où il constituerait un danger?
Pour l’instant, non. On pourrait leur interdire via un GPS de rentrer dans certaines zones, une sorte de « no fly zone ». Si la démarche pouvait être contournée par de bons ingénieurs en électronique ou en informatique, elle aurait au moins le mérite de limiter les risques. Aujourd’hui, on a plutôt à faire à des gens qui sont là pour provoquer, mais aux mains d’une personne malveillante, cela peut constituer un risque réel. Cela dit, les hélicoptères électriques qui peuvent supporter une charge plus lourde que les drones sont sur le marché depuis déjà 30 ans et n’ont jusqu’à présent jamais servi à commettre un attentat.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source :
http://www.lorientlejour.com/article/914452/-aux-mains-dune-personne-malveillante-lutilisation-dun-drone-peut-constituer-un-risque-reel-.html

Protection des données personnelles : le pas en arrière de l’Europe | Le Net Expert Informatique

Protection des données personnelles : le pas en arrière de l’Europe

L'avenir de la protection des données en Europe se décide au Conseil. Et cet avenir ne s'annonce pas radieux au vu des modifications proposées. Quatre associations de protection ont eu accès aux derniers brouillons et dénoncent un recul des droits.

Depuis 2012, la nouvelle réglementation relative à la protection des données personnelles est en discussion en Europe. Mais le texte a déjà pris au moins une année de retard, en raison notamment des blocages au sein du Conseil.
Et rien ne garantit que ce contretemps sera mis à contribution pour accroître la protection des individus. C'est le constat que dressent quatre associations de protection de la vie privée (Privacy International, EDRi, Access et Panoptykon Foundation) qui ont eu accès aux derniers brouillons du projet débattu au sein du Conseil de l'Europe.

Une réforme sapée par le Conseil
« Malheureusement, au sein du Conseil de l'UE, les gouvernements des Etats membres travaillent à saper ce processus de réforme. Durant plus de trois ans, le Conseil n'a pas seulement échoué à afficher un soutien à cette réforme et aux négociations, mais propose désormais des modifications du texte qui pourraient abaisser le niveau de protection actuel des données en Europe » dénoncent-elle dans un rapport.
Pour les organisations, la protection des données personnelles repose en grande partie sur le principe du consentement. Or, en se basant sur les propositions du Conseil, et en particulier de l'Allemagne, elles observent un profond recul par rapport à la proposition initiale en estimant que le paramétrage du navigateur vaudrait consentement de l'internaute en matière de suivi et de profilage.
L'Allemagne est accusée outre de défendre la possibilité pour les entreprises de procéder à une collecte et à un traitement de données sans recueil préalable du consentement dès lors que l'exploitation répond à un « intérêt légitime ».
« Ces données pourraient être transmises à des tiers sur la base de cette exception d'intérêt légitime et ces tiers pourraient utiliser cette exception pour commencer à traiter des données pour des finalités sans aucun lien ou incompatibles avec l'objectif initial » commente le rapport.
Sur la question de l'information, un recul des droits est également dénoncé. Le Conseil de l'UE propose ainsi de supprimer l'article 11 du texte. Or celui-ci définit concrètement les obligations relatives à l'information des individus, et notamment des enfants, sur la façon dont leurs données personnelles sont utilisées.

Les sanctions pourraient baisser
Les gouvernements préconisent également d'ajouter une exception permettant d'établir des profils des citoyens au nom de l'intérêt public, comme par exemple pour des raisons de sécurité nationale et de défense. Et la liste n'est pas exhaustive, laissant aux Etats la possibilité d'ajouter des exceptions.
Sur le front des sanctions et des actions en justice, les organisations de protection s'inquiètent là aussi d'une régression. Selon elles, les modifications introduites par le Conseil retirent la possibilité de mener des actions collectives. Des membres feraient également pression en faveur de sanctions plus légères, inférieures aux 5% de CA annuel prévus initialement.
Le guichet unique enfin. Censé apporté une simplification administrative, il serait au contraire en passe de se complexifier. Dans le cas de plaintes transnationales, au moins deux autorités de protection devraient être impliquées. Le Bureau européen de la protection des données interviendrait lui en cas de conflit dans la résolution d'un litige entre deux autorités ou plus.
Les désaccords autour du guichet unique ne sont pas nouveaux. Loin d'être une source de simplification, celui-ci constituerait avant tout un cadeau fait aux géants du Web, lui reprochent plusieurs autorités de protection. La présidente de la Cnil s'est d'ailleurs déclarée contre le principe de ce guichet tel qu'imaginé au départ.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source :
http://www.zdnet.fr/actualites/protection-des-donnees-personnelles-le-pas-en-arriere-de-l-europe-39815834.htm

Nouveau coup de filet dans le milieu de la cybercriminalité au Mali | Le Net Expert Informatique

Nouveau coup de filet dans le milieu de la cybercriminalité au Mali

Trois nouvelles interpellations ont eu lieu, ce jeudi, au Mali dans une affaire de lutte contre la cybercriminalité. Une bande dirigée depuis les Etats-Unis trafique les lignes de téléphonie mobile, et empoche une partie importante des sommes qui reviennent normalement aux opérateurs. Rien que pour le Mali, selon la section cybercriminalité de la police nationale, le manque à gagner serait évalué à plusieurs centaines de millions de francs CFA.

Le chef du réseau est basé aux Etats-Unis et l'on ne connaît que son prénom : Monsieur Constant. Il a la double nationalité, camerounaise et américaine. C'est un as de l'informatique et Internet n'a pas de secret pour lui.
Constant repère dans des pays d'Afrique de l'Ouest de jeunes travailleurs dans des cybercafés. Ils reçoivent de ce nouveau partenaire basé aux Etats-Unis des appareils sophistiqués. Des outils qui servent à masquer, via Internet, les appels internationaux.
Par exemple, de Bamako un client appelle en dehors du pays, à Paris, via un numéro appartenant à une société malienne de téléphonie mobile. Mais dans le cœur du compteur détraqué, l'appel est considéré comme une communication locale. Or le client qui téléphone va, lui, payer une communication internationale.
Selon la section de lutte contre la cybercriminalité de la police malienne qui travaille avec très peu de moyens, un opérateur privé local aurait déjà perdu, par ce procédé, quelques centaines de millions de francs CFA. Au moins huit personnes ont déjà été arrêtées ou interpellées au Mali. Et dans deux autres pays voisins, des complices sont actuellement recherchés.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.rfi.fr/afrique/20150306-mali-reseau-cybercriminels-passe-etre-demantele/

Casper, le logiciel espion qui surveillait la Syrie | Le Net Expert Informatique

	Casper, le logiciel espion qui surveillait la Syrie

Un chercheur en informatique a découvert un nouveau programme espion, qu'il attribue aux mêmes développeurs que le programme Babar, pour lequel la France est soupçonnée.

Les développeurs des programmes espion Babar et Evil Bunny, que le Canada soupçonne être les services de renseignement français, ont créé un troisième programme espion qui ciblait la Syrie.
Pour rappel, Le programme espion Babar a un « grand frère » : Evil Bunny
C'est la conclusion à laquelle aboutit Joan Calvet, un expert de l'entreprise de sécurité informatique ESET dans un rapport qui doit être publié jeudi 5 mars. Il a pu mettre la main sur un exemplaire de ce nouveau programme, dont le nom que lui ont donné ses créateurs reprend à nouveau celui d'un célèbre dessin animé. Cette fois-ci, les développeurs ont baptisé leur création Casper.

Une dizaine de personnes visées en Syrie
Ce logiciel a été retrouvé sur les ordinateurs d'une dizaine de personnes, toutes situées en Syrie. Il n'est pas exclu que ce programme ait été mis en œuvre ailleurs. Il a aussi été utilisé très récemment – contrairement à Babar – et faisait partie d'une opération bien précise : il a été actif en Syrie seulement quelques jours, entre le 9 et le 16 avril 2014.
La trace de ce programme a été retrouvée sur un site officiel du gouvernement syrien, celui d'une commission créée en 2011 sous l'égide du ministère de la réconciliation nationale afin que les Syriens victimes de destructions lors de la guerre civile puissent porter réclamation.

Un programme de reconnaissance
A l'inverse de Babar, Casper ne capture pas d'informations directement : c'est un programme de reconnaissance. Lorsqu'il pénètre dans un ordinateur, il en établit un descriptif précis – langue utilisée, programmes installés, logiciels antivirus configurés – avant de le faire parvenir à ses commanditaires. Ensuite, ces derniers décident si la cible est réellement digne d'intérêt.
Le deuxième stade est vraisemblablement celui de l'envoi d'un autre programme espion capable, lui, d'intercepter des informations. Casper prévoit d'ailleurs ce cas de figure : il peut lui être ajouté des modules complémentaires. Cette technique est de plus en plus courante dans les attaques étatiques sophistiquées.

Un programme fantomatique et complexe, une « partie d'échecs » avec les logiciels antivirus.
Ce programme espion au nom de fantôme porte bien son nom, tant il est difficile à détecter. Lorsqu'il atterrit sur un ordinateur, Casper s'adonne à une « partie d'échecs » avec les logiciels antivirus : il analyse très finement lesquels sont présents sur la machine et adapte son mode d'infection. Dans certains cas, il peut tout bonnement s'autodétruire lorsqu'il estime que les risques sont trop grands. « On voit rarement ce niveau de précision dans l'évitement des antivirus chez les programmes espion », note Joan Calvet, signe là encore d'une grande sophistication.
« Casper est tellement furtif et sous le radar des entreprises de sécurité, qu'on ne retrouve sa trace qu'épisodiquement pour le moment. J'espère qu'en publiant ces informations, d'autres chercheurs vont pouvoir amener leur pièce au puzzle ! », explique aussi M. Calvet.
Signe supplémentaire de sa complexité et de la motivation des attaquants, il utilise une faille dite « 0-Day », c'est-à-dire une vulnérabilité inconnue. Ce type de vulnérabilité, inédite donc invisible pour les antivirus, intéresse de près les chercheurs en sécurité informatique. Utiliser une telle faille, c'est prendre le risque de l'exposer en plein jour et de la voir rapidement corrigée.

Les mêmes auteurs que Babar
Pour Joan Calvet, il n'y a guère de doute. Casper est l'œuvre des développeurs qui ont créé Babar et Evil Bunny. Outre des portions du code rigoureusement identiques entre ces programmes, il leur a trouvé de nombreux points communs, notamment dans leur manière de se cacher ou de détecter les antivirus.
« Toutes les fonctionnalités communes nous font dire avec un haut degré de certitude que Bunny, Babar et Casper ont été développés par la même organisation », écrit Joan Calvet.

Un Etat à la manœuvre ?
Casper, comme Babar, n'est pas un programme d'espionnage massif, comme certains dispositifs révélés par les documents d'Edward Snowden. Il s'agit d'outils de haut niveau destinés à obtenir des informations précises sur des cibles déterminées. Selon M. Calvet, « le ciblage précis d'individus en Syrie montre un intérêt géopolitique probable » :
« Non seulement Casper est bien développé, mais en plus ses auteurs semblent bien comprendre comment nous – les chercheurs en sécurité – travaillons, et ils ont fait en sorte de rendre notre tâche difficile. En regardant rapidement le programme, on peut avoir l'impression d'avoir sous les yeux un logiciel malveillant banal, sans se douter de toute la machinerie de reconnaissance contenue dans Casper. Je dirais donc que Casper a été développé par une équipe de professionnels, soucieuse de faire un logiciel malveillant discret. Ce "professionnalisme" peut tout à fait correspondre à une entité étatique. »

France : quelle implication ?
En 2014, Le Monde révélait sur la base de documents fournis par Edward Snowden que les services de renseignement canadiens soupçonnaient la France d'avoir développé un programme espion nommé Babar.
Rappel : Quand les Canadiens partent en chasse de « Babar »
Il y a quelques semaines, deux chercheurs en informatique révélaient davantage d'informations sur Babar et dévoilaient du même coup l'existence d'Evil Bunny, le « grand frère », moins évolué, de Babar, développé par la même organisation.
Pas de trace nouvelle d'une implication hexagonale dans Casper. La France, qui à ce stade n'est que soupçonnée par les services de renseignement canadiens d'être derrière Babar, et donc derrière Casper, s'est dotée, comme les autres grandes puissances militaires mondiales, de capacités offensives sur Internet, confiées à l'armée et aux services extérieurs, la DGSE. Les autorités refusent de s'exprimer sur ce sujet extrêmement sensible, couvert par le plus haut niveau du secret-défense. Récemment, une vidéo réalisée par l'armée française rompait légèrement avec ce mutisme en vantant ses capacités d'« attaque » et « destruction » dans ce « combat numérique ».

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lemonde.fr/pixels/article/2015/03/05/casper-le-logiciel-espion-cousin-de-babar-qui-surveillait-la-syrie_4586723_4408996.html
Par Martin Untersinger

Facebook sera jugé en France pour avoir abusivement suspendu un compte | Le Net Expert Informatique

Facebook sera jugé en France pour avoir abusivement suspendu un compte

L'affaire « Gustave Courbet » connait son premier dénouement devant le tribunal de grande instance de Paris. La justice estime qu'elle est compétente pour recevoir une plainte contre Facebook – bien que le service soit américain -, le problème ayant été rencontré sur notre territoire.

Si le plaignant estime que le réseau social a fait montre de censure abusive en fermant son compte, la défense explique de son côté que les plaintes doivent être adressées devant des juridictions américaines. Selon l'AFP, le tribunal vient de trancher puisqu'il considère que l'affaire pourra être jugée en France.

Pour rappel, l'affaire a débuté en 2011. A cette époque, le compte Facebook d'un internaute avait été suspendu au motif que l'une de ses publications revêtait un caractère pornographique. L'image mise en ligne n'était en fait qu'une reproduction du célèbre tableau du peintre Gustave Courbet (L'origine du monde), représentant le sexe d'une femme.
Si le réseau social interdit toute représentation pornographique sur son outil, il avait eu la main lourde sur ce qui revêt du domaine de l'Art. L'internaute avait donc entamé une attaque en justice à l'encontre du réseau social et réclamait initialement la somme de 20 000 euros de dommages et intérêts.

L'affaire #Unbonjuif ou #Unbonmusulman chez Twitter
La question de savoir à quelle loi sont soumis ces services américains, lors de faits commis en France s'est déjà posée par le passé. En 2013, des messages racistes et antisémites avaient été publiés sur Twitter, par des abonnés résidant en France. Le service de micro-blogging avait par la suite été poursuivi par des associations. Ces dernières réclamaient, à l'occasion d'une procédure en référé devant le tribunal de grande Instance de Paris que le nom de certains utilisateurs leur soit communiqué, afin que d'autres actions en justice puissent être initiées. A l'époque, Twitter avait adopté la même position que Facebook. Le service de micro-blogging précisait qu'il restait soumis à la loi américaine et appelait à ce qu'une décision de la justice américaine, ou d'une commission rogatoire internationale, soit prononcée en la faveur de cette divulgation.
Malgré un appel, Twitter avait été sommé de fournir l'identité des personnes en cause. La justice avait également demandé au service de micro-blogging de mettre en place un moyen afin qu'une personne puisse signaler des contenus illicites plus facilement.

Expert Informatique et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.
Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source :
http://pro.clubic.com/blog-forum-reseaux-sociaux/facebook/actualite-757473-facebook-proces.html?&svc_mode=M&svc_campaign=NL_ClubicPro_New_06/03/2015&partner=-&svc_position=889007891&svc_misc=-&crmID=639453874_889007891&estat_url=http%3A%2F%2Fpro.clubic.com%2Fblog-forum-reseaux-sociaux%2Ffacebook%2Factualite-757473-facebook-proces.html

Réglementation des drones et droit des robots | Le Net Expert Informatique

source : http://live.orange.com/drones-parrot-amazon-zephyr/

Réglementation des drones et #droit des robots

Le survol des drones au dessus des centrales nucléaires [1] ainsi que d'autres sites sensibles et parisiens [2] représente une menace face à laquelle les réponses, notamment réglementaires, semblent encore insuffisantes.

En effet, la détection par radar militaire mais également l'interception de ces engins volants se révèlent difficiles de par la furtivité des drones et l'incapacité actuelle des autorités à les tracer et à les écarter.

Au niveau réglementaire, l'utilisation des drones ou plus exactement d' « aéronefs qui circulent sans monde à bord » civils, à distinguer des drones militaires, est encadrée par deux arrêtés d'avril 2012 [3], un arrêté relatif aux conditions de navigabilité et de télépilotage et un autre relatif aux exigences liées à l'espace aérien.

Le principe est le suivant :
sauf autorisation particulière, les drones doivent survoler un espace bien précis délimité en volume et en temps, en dehors de toute zone peuplée. De plus, en fonction de deux catégories de critères (finalité d'utilisation et poids du drone), des règles particulières s'appliquent. Ainsi, les drones civils professionnels utilisés par exemple par les agriculteurs ou les photographes doivent notamment se faire connaître auprès des autorités.
Concernant l'utilisation de drone de loisirs qui est en vente libre, il faut également respecter des règles spécifiques qui sont rappelées dans une notice rédigée par la Direction Générale de l'Aviation Civile (DGAC) en décembre 2014 [4] et qui interdisent notamment le vol de nuit, le survol des sites sensibles ainsi que de l'espace public en agglomération.
Au final, la violation des conditions d'utilisation des drones est passible d'un an d'emprisonnement et de 75000 euros d'amende en vertu de l'article L.6232-4 du code des transports.
Autre point d'importance à souligner, même si la prise de vue aérienne est réglementée par l'article D. 133-10 du code de l'aviation civile, il n'en demeure pas moins que la captation et l'enregistrement d'images relatives aux personnes relèvent également de la loi « Informatique et Libertés »[5].
En effet, il est important de souligner également le risque de collecte de données à caractère personnel par les drones. Un facile parallèle peut être établi entre le survol des drones et le passage dans nos rues des « Google cars ». La CNIL avait constaté lors de contrôles effectués fin 2009 et début 2010 que la société Google, via le déploiement de véhicules enregistrant des vues panoramiques des lieux parcourus, récoltait, en plus de photographies, des données transitant par les réseaux sans fil Wi-Fi de particuliers, et ce à l'insu des personnes concernées. Cette collecte déloyale de très nombreux points d'accès Wi-Fi constitue un réel manquement à la loi « Informatique et Libertés ».
Concernant les drones, il faudra donc s'attacher à vérifier qu'ils ne récupèrent pas également des données à caractère personnelle de façon illégale. En effet, les drones sont des machines qui peuvent embarquer une quantité importante de capteurs divers et variés tels un appareil photo, une caméra ou un dispositif de géolocalisation permettant de collecter et diffuser des données à caractère personnel avec pour conséquence l'atteinte manifeste à la vie privée des individus.
Consciente de ces enjeux depuis 2012, la CNIL, en liaison avec le Groupe des 29 CNIL européennes (G29) réfléchit activement à l'amélioration de la réglementation à ce sujet.

Au final, la réglementation relative aux drones qui, d'une part, a le mérite d'exister et, d'autre part, est relativement souple et adaptable en prévoyant plusieurs scénarii spécifiques, apparaît même novatrice au niveau international. Les Etats Unis par l'intermédiaire de la Federal Aviation Association (FAA) n'ont dévoilé que le 15 février 2015 et pour la première fois des recommandations pour encadrer l'utilisation des drones civils commerciaux sur le sol américain [6].
Toutefois, la DGAC a prévu quand même de réviser prochainement la réglementation des drones afin de mieux prendre en compte la massification de l'utilisation de drones civils. Cette révision devra si possible prendre en compte une future réglementation européenne à ce sujet.

Plus largement, ce focus juridique sur les drones peut élargir son horizon en s'intéressant à la problématique du droit des robots qui, au regard de la vitesse de création des inventions technologiques, constitue indéniablement un des enjeux majeurs juridiques mais également éthiques des années à venir.
Certes pour les objets connectés, les enjeux juridiques ont déjà été identifiés mais il semble qu'il faille pousser le cadre juridique plus loin pour les futures générations de robot doté d'une certaine forme d'intelligence artificielle.
La vente du robot, comme tout bien, entraine pour le vendeur une obligation de garantie et engage sa responsabilité délictuelle du fait d'un défaut de sécurité de l'un de ses produits ou services entraînant un dommage à une personne. Cependant, il est probable que l'autonomie des robots grandissante, il faille réfléchir à la responsabilité propre du robot. De prime abord, la responsabilité juridique repose sur la notion de discernement, actuellement les machines restent sous la responsabilité de son gardien soit de l'usager ou encore de son fabricant par le biais de la responsabilité des produits défectueux.
Il est possible que, dans un futur plus ou moins proche, le législateur décide de mettre en place une personnalité juridique spécifique du robot. Cette dernière, se distinguant du régime juridique lié aux animaux et des biens, devra être encadrée afin de prévoir la sécurité des utilisateurs mais également la sécurité du robot lui-même. Pour commencer, il pourrait même s'agir de la reprise des trois règles de la robotique édictée par Isaac Asimov [7]!

[1] Dix-sept centrales nucléaires sur les dix-neuf que compte le parc français ont été survolées par des drones depuis début octobre. Six l'ont été simultanément dans la nuit du 31 octobre.
[2] http://www.liberation.fr/societe/2015/02/24/paris-survole-par-des-ovnis_1209273
[3]Les arrêtés du 11 avril 2012 relatifs d'une part à l'utilisation de l'espace aérien par les aéronefs qui circulent sans personne à bord et d'autre part à la conception des aéronefs civils qui circulent sans aucune personne à bord, aux conditions de leur emploi et sur les capacités requises des personnes qui les utilisent constituent le socle réglementaire d'utilisation des drones civils.
[4] Règles d'usage d'un drone de loisir : http://www.developpement-durable.gouv.fr/IMG/pdf/Drone-_Notice_securite-2.pdf
[5] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée.
[6] « Drones civils – les Etats-Unis avancent sur leur législation : les différences avec le modèle français » par Emmanuel de Maistre, président de Redbird : http://www.infodsi.com/articles/154099/drones-civils-etats-unis-avancent-legislation-differences-modele-francais-emmanuel-maistre-president-redbird.html?key=a0a42d0bc78aa63d
[7] http://nte.mines-albi.fr/SystemiqueSudoku/co/v_regle_vie_Azimov.html

---

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://securitedessystemesjuridiques.blogspot.fr/2015/03/reglementation-des-drones-et-droit-des.html

---

Windows concerné aussi par la

Faille SSL Freak | Le Net Expert Informatique

Windows concerné aussi par la Faille SSL Freak

Sécurité : Microsoft a révélé que Windows était également touché par la faille de sécurité nommée Freak qui permet de pratiquer une attaque type « man in the middle » sur les connexions sécurisées https.

En début semaine, nous apprenions l'existence d'une nouvelle faille de sécurité portant sur les protocoles SSL et TLS. Baptisée Freak (Factoring RSA Export Keys), elle permettrait à un assaillant de lancer une attaque contre une connexion https afin de la forcer à activer une clé de chiffrement moins puissante qui peut ensuite être cassée en quelques heures. Cette faille a été découverte par une équipe de spécialistes européens, parmi les lesquels des français de l'Inria et des experts de Microsoft Research. Or, Microsoft vient d'annoncer que Windows était finalement lui aussi concerné par Freak. Une information qui n'avait pas été communiquée immédiatement au moment de la présentation des conclusions de cette étude.

Un correctif en préparation

Dans un bulletin de sécurité diffusé hier, l'éditeur indique que Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows 8, 8.1, Windows Server 2012 et Windows RT sont affectés. Microsoft indique qu'il a engagé une enquête technique qui pourrait déboucher sur la diffusion d'un correctif.

Selon les dernières estimations des chercheurs qui ont découvert Freak, voici la liste des navigateurs Internet concernés : Internet Explorer, la version Android de Chrome, le navigateur par défaut d'Android, Safari sur iOS et Mac OS X, le navigateur BlackBerry ainsi qu'Opera sur Mac OS X et Linux.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.zdnet.fr/actualites/faille-ssl-freak-windows-est-aussi-concerne-39815920.htm
Par Eureka Presse

Canons à eau, système de brouillage, radars : les pistes de l'Etat pour contrer les drones | Le Net Expert Informatique

Un drone, près de Paris, le 27 février 2015. (DOMINIQUE FAGET / AFP)

Canons à eau, système de brouillage, radars : les pistes de l'Etat pour contrer les drones

Face à l'ampleur du phénomène, les autorités françaises contre-attaquent. Après plusieurs vols de drones au-dessus de Paris, le secrétariat général de la défense et de la sécurité nationale (SGDSN) a présenté ses solutions pour mettre fin à ce phénomène. Ces mesures sont détaillées dans un rapport confidentiel destiné au Premier ministre, dont La Croix a pris connaissance, mercredi 4 mars.
Selon le SGDSN, des « petits avions sans pilote ont été signalés au-dessus de sites sensibles » une soixantaine de fois depuis l'été dernier, rapporte La Croix. Des survols qui « constituent une alerte sur les risques potentiels induits par un emploi inapproprié ou malveillant, reconnaît le SGDSN. Il n'existe aujourd'hui aucune solution immédiatement disponible, tant en France qu'à l'étranger » pour contrer le phénomène.

Neutralisation, détection et adaptation de l'arsenal législatif
Selon La Croix, le SGDSN propose plusieurs mesures pour détecter et neutraliser les drones. D'ici à la fin mars, de nouveaux dispositifs de détection seront expérimentés. « Des radars passifs ou actifs notamment orientés au-dessus des agglomérations et des sites sensibles », précise Le Figaro. Ils devraient couvrir une zone de vol entre 50 et 100 m et combler ainsi un « trou dans la raquette », concédé par la SGDSN.
Pour neutraliser les drones, le « jet de matière » est envisagé, à savoir les canons à eau. Des brouilleurs plus denses du signal entre le drone et la télécommande du pilote sont aussi à l'étude. Tout comme des leurres GPS pour tromper l'engin, l'emploi de lasers ou d'un système qui mettrait en panne les engins à l'approche d'une zone interdite. Au-delà de ces solutions, qui ne sont pas disponibles dans l'immédiat, l'Agence nationale de la recherche étudie 23 projets pour identifier des procédés innovants.
Enfin, la SGDSN envisage de muscler l'arsenal législatif : rendre les drones détectables à l'aide d'une puce obligatoire, obligation d'installation d'une puce permettant la neutralisation de l'engin à distance, immatriculation, formation des pilotes, assurance obligatoire… De nouvelles infractions pourraient aussi être créées, comme la « peine complémentaire de confiscation » ou un ciblage de la responsabilité civile des pilotes, évoque Le Parisien.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.francetvinfo.fr/internet/drones/canons-a-eau-systeme-de-brouillage-radars-les-pistes-de-l-etat-pour-contrer-les-drones_840475.html#xtor=EPR-2-newsletterquotidienne-20150305-lestitres-coldroite/titre4

Les entreprises qui

appliquent des mesures de protection des données personnelles jouissent d’une meilleure réputation, les clients leur font davantage confiance et elles se démarquent clairement sur le marché

Les entreprises qui appliquent des mesures de protection des données personnelles jouissent d’une meilleure réputation, les clients leur font davantage confiance et elles se démarquent clairement sur le marché

L’absence d’accord au niveau européen conduit les entreprises à différer toute action au profit de celles qui appliquent des règles strictes de sécurité et de confidentialité déjà en place.

Le fait que les efforts d’harmonisation des règles européennes de collecte, d’utilisation et de conservation des données s’enlisent dans des débats politiques, pourrait bien faire perdre une part substantielle de leur avantage concurrentiel à la majeure partie des entreprises de l’UE qui avouent être mal préparées aux changements à venir[i], selon Iron Mountain, le spécialiste des services de conservation et de gestion de l’information.
Dans un document consultatif*, Iron Mountain souligne l’importance pour les entreprises de mettre en œuvre de solides mesures de protection des données, indépendamment de ce que préconisent les propositions réglementaires. En effet, il est démontré que **les entreprises qui appliquent de telles mesures jouissent d’une meilleure réputation, que les clients leur font davantage confiance et qu’elles se démarquent clairement sur le marché**.

Forrester avance que « dans la lutte pour acquérir, servir et fidéliser les clients, la sécurité des données et le respect de la confidentialité sont aujourd’hui des gages qui aident à se différencier de la concurrence ».[ii]

Ce document aide les entreprises à mesurer pleinement les effets de la nouvelle réglementation et à comprendre leur importance. Bon nombre de dispositions font toujours l’objet d’intenses débats parmi les dirigeants de l’UE trois ans après la première proposition de loi : celles relatives aux données du secteur public, le droit d’accès aux données par les organismes chargés de l’application de la loi et la possibilité pour les entreprises internationales de traiter directement avec le régulateur sur leur marché d’origine (le « guichet unique »), . Le retard pris pour parvenir à un accord ne reflète pas uniquement les intérêts divergents des 28 États membres, mais aussi l’évolution rapide des technologies, des nouveaux consommateurs connectés et du Big Data.
« La proposition de loi est extrêmement puissante et elle aura des répercussions dans le monde entier », déclare Edward Hladky, Directeur Général Adjoint d’Iron Mountain France. « Certains concepts seront étudiés de près dans quelques zones géopolitiques : la cohérence des règles et leur mise en œuvre à travers les frontières, le droit à l’oubli et le besoin d’une désidentification efficace des données personnelles utilisées dans les secteurs de la santé et de la recherche. »
« Toutefois, avec autant de propositions en constante évolution, les entreprises peuvent être tentées d’attendre de voir ce que la version finale contiendra réellement. Nous pensons que ce serait une erreur. L’éthique veut que les organisations protègent les données fermement et efficacement et qu’elles les utilisent et les conservent de manière responsable et transparente. Autant cela renforce la confiance des clients, autant les violations de données les rendent méfiants. L’équation est simple : la confiance nourrit la fidélité et la fidélité nourrit les ventes. Les entreprises ont beaucoup à gagner en agissant dès maintenant, avant que la loi les oblige à le faire. »

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.infodsi.com/articles/154353/attente-nouvelle-legislation-europeenne-protection-donnees-pourrait-couter-cher-competitivite-image-marque-entreprises.html
* Le livre blanc, en version anglaise, édité pour la journée européenne de la protection des donnes, « An opportunity to plan and manage the impact of legal change » est disponible sur http://www.ironmountain.co.uk/services/dpd.aspx

[i]52 % des entreprises d’après une étude menée au Royaume-Uni, en Allemagne et en France par Ipswitch Software en octobre 2014. http://www.techweekeurope.co.uk/e-regulation/european-teams-woefully-unprepared-general-data-protection-regulation-155316#ArDP0sA9ymVzYTPT.99
[ii]https://www.forrester.com/Predictions+2015+Data+Security+And+Privacy+Are+Competitive+Differentiators/fulltext/-/E-RES116328