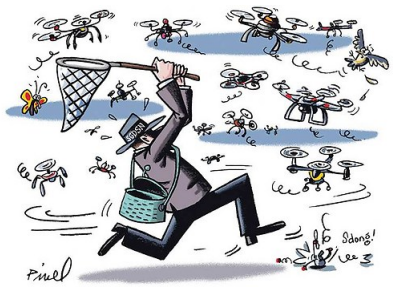
Quelle réponse face aux survols illicites de drones ? | Le Net Expert Informatique

	Quelle réponse face aux survols illicites de drones ?

La multiplication de vols de drones inconnus et leur médiatisation inquiètent une filière française dont la croissance a été favorisée par l'existence d'une réglementation jusque-là assez libérale.

D'objet sympathique, le drone est presque devenu l'ennemi public numéro un depuis quelques semaines, face à la multiplication de vols aussi illicites que mystérieux. Une mini-psychose qui touche une partie de la population d'abord, certains imaginant déjà ces mini-appareils sans pilote se transformer en nouvelles armes aux mains de terroristes. Chez les policiers et les gendarmes ensuite, qui n'ont jusqu'à présent arrêté aucun responsable des soixante vols recensés. La médiatisation du phénomène inquiète enfin une filière en pleine croissance qui avait jusqu'alors bénéficié de la compréhension d'une administration plutôt bienveillante.

Depuis avril 2012, en effet, une réglementation assez libérale encadre l'utilisation des drones. Fruit d'une concertation entre la Direction générale de l'aviation civile et les professionnels, celle-ci comprend quatre scénarios d'utilisation. Tous imposent une altitude inférieure à 150 mètres mais autorisent, dans certains cas, le vol en dehors du champ de vision du pilote. Jusqu'à 1 kilomètre et même « hors vue » sur plusieurs dizaines de kilomètres dans certains cas. Dotée d'un cadre légal solide, la filière a connu un véritable boom avec une cinquantaine de constructeurs de drones et, surtout, 1.300 sociétés de services enregistrées auprès de la DGAC. Celle-ci imposant la constitution d'un dossier, inspiré de celui de l'aviation, détaillant le type de drone utilisé, la qualification des pilotes, les procédures mises en place… La Fédération professionnelle des drones civils (FPDC) revendique 300 membres et en espère 500 d'ici à la fin de l'année. Et estime à 3.000 le nombre d'emplois créés par la filière. C'est justement cette dynamique que les professionnels craignent de voir freinée par des pouvoirs publics susceptibles de réagir aux événements actuels en durcissant la réglementation. « Une hypothèse toutefois peu fondée puisque l'administration fait bien la différence entre une filière qui travaille dans le cadre réglementaire et les auteurs de ces actes irresponsables », relativise Emmanuel de Maistre, fondateur de la Fédération professionnelle des drones civils.

L'autre risque étant que l'opinion publique bascule et pousse les pouvoirs publics à plus de sévérité. Même si, en parallèle, le grand public semble avoir déjà adopté le drone. A lui seul, Parrot, l'un des principaux acteurs du marché du drone de loisirs, a déjà vendu près de 1 million d'appareils en quatre ans.

Les professionnels montent au créneau, en rappelant que ces dernières années des milliers de vols se sont déroulés sans incident. Il reste qu'un drone n'est pas un objet anodin et qu'il engendre des risques : blessure en cas de choc ou de chute, perturbation du trafic aérien, distraction des automobilistes… Une soixantaine d'enquêtes judiciaires ont d'ailleurs été menées depuis trois ans, dont six se sont soldées par une confiscation du matériel et deux par des peines de prison avec sursis. L'une pour un drone qui s'était écrasé sur la piste de l'aéroport de Montpellier et l'autre à l'occasion de l'échouage d'un paquebot sur une plage de Bayonne. Le propriétaire avait voulu filmer le navire, entravant du même coup les opérations de sauvetage. Et si en France la police n'a jamais enregistré d'accident, on l'a parfois frôlé. A l'image de ce qui s'est passé en Catalogne en 2013, lorsqu'un drone de plusieurs kilos qui filmait des festivités est tombé de 30 mètres de haut à quelques centimètres d'une petite fille.

Les drones vont de toute façon voir le paysage changer. Impuissant depuis les premiers survols de sites sensibles, notamment des centrales nucléaires, l'Etat ne compte plus se laisser faire. Le Secrétariat général de la défense et de la sécurité nationale (SGDSN) a été mandaté par le Premier ministre pour évaluer la menace et organiser la riposte « à moyen et long terme ». Les pistes sont d'abord réglementaires : immatriculation, enregistrement des drones, obligation de s'assurer.

Dans le domaine du drone de loisirs, pourquoi ne pas rendre obligatoire la note très bien faite de la DGAC recensant les 10 commandements pour l'usage d'un drone en France ? Les pistes sont aussi techniques avec la possibilité de les doter de puce d'identification ou de transpondeur, pour les rendre détectables. Même si ces dispositifs peuvent être contournés. « La grande mode étant désormais de fabriquer son drone en kit à partir de pièces achetées sur Internet », constate un spécialiste de la lutte contre les drones illicites. Dès lors, le SGDSN a aussi pour mission d'évaluer des dispositifs techniques, pour neutraliser les drones ou protéger les sites sensibles. Des technologies existent : brouillage du signal GPS, radars actifs ou passifs, voire laser ou canons à eau. « Aucune solution ne semble disponible immédiatement même si des industriels assurent en avoir », indique le SGDSN. Pour vérifier leurs dires, une série d'expérimentations sont déjà en cours avec l'appui technique du centre français de recherche aérospatiale (l'Onera). Le SGDSN a voulu aller plus loin en allouant 1 million d'euros à la recherche. Quelque 23 entreprises ont ainsi répondu à un appel à projets « Protection de zones sensibles vis-à-vis des drones aériens » lancé par l'Agence nationale de la recherche. Les candidats devraient être choisis ces jours-ci et se voir financer pour des projets sur dix-huit mois au maximum.

La réglementation va également évoluer à l'échelon européen. La Commission européenne s'en préoccupe et vient de réunir tous les acteurs la semaine dernière en Lettonie. L'objectif étant de réfléchir à une uniformisation des pratiques, très différentes d'un pays à l'autre. Avant cela la DGAC devrait encore faire évoluer la réglementation française. Avec pour l'instant des pouvoirs publics qui semblent prudents. « On ne veut pas faire abstraction de la filière et nuire à son développement », entend-on aussi bien au SGDSN qu'à la Gendarmerie des transports aériens (GTA).

Les points à retenir

Face à la multiplication des vols illégaux de drones, le Premier ministre a chargé le Secrétariat général de la défense et de la sécurité nationale d'évaluer la menace et d'organiser la riposte.

Les pistes sont d'abord réglementaires : immatriculation, enregistrement des drones, obligation de s'assurer.

Mais les réponses sont aussi techniques avec la possibilité de les doter de puce d'identification ou de transpondeur, pour les rendre détectables.

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

Source : http://www.lesechos.fr/idees-debats/editos-analyses/0204206144122-quelle-reponse-face-aux-vols-illicites-de-drones-1100859.php
Par Frank Niedercorn Journaliste au sein du service Prospective des « Echos »

Vote électronique : Confidentialité et sécurité des données a confirmé le Conseil d'Etat | Le Net

Expert Informatique

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer

Vote électronique : Confidentialité et sécurité des données a confirmé le Conseil d'Etat

Le Conseil d'Etat a été amené, dans un arrêt du 11 mars 2015 n° 368748, à se prononcer sur la confidentialité et la sécurité des données à l'occasion de l'organisation d'un vote électronique pour les élections professionnelles de délégués du personnel.

En l'espèce, la CNIL, saisie d'une plainte d'un syndicat, prononce un avertissement à l'encontre d'une société n'ayant pas pris toutes précautions utiles pour préserver la sécurité et la confidentialité des données à caractère personnel lors de l'élection des délégués du personnel organisée par voie électronique avec recours aux services d'un prestataire extérieur. La société et le prestataire forment un recours en annulation de cette délibération devant le Conseil d'Etat.

Le Conseil d'Etat rejette la requête et retient qu'il résulte des dispositions du Code du travail, « dont l'objectif est de garantir la sincérité des opérations électorales par voie électronique, que l'utilisation d'un système de vote électronique pour l'élection des délégués du personnel est subordonnée à la réalisation d'une expertise indépendante lors de la conception initiale du système utilisé, à chaque fois qu'il est procédé à une modification de la conception de ce système ainsi que préalablement à chaque scrutin recourant au vote électronique ».

Dès lors, « à supposer même que le système de vote électronique en litige n'ai fait l'objet d'aucune modification de sa conception depuis sa précédente utilisation par l'entreprise, […] une expertise indépendante était requise préalablement à sa mise en place pour les élections professionnelles organisées par la société requérante ».

Par ailleurs, « il résulte de [l'article R. 2324-5 du Code du travail sur la confidentialité des données transmises] que la transmission aux électeurs des identifiants et mots de passe leur permettant de participer au vote doit faire l'objet de mesures de sécurité spécifiques permettant de s'assurer que les électeurs en sont les seuls destinataires ». Ainsi, « c'est à bon droit que la CNIL a estimé que la transmission par simple courriel de ces données aux électeurs méconnaissait les obligations » découlant de ce même article.

En outre, le Conseil d'Etat rappelle, conformément à un arrêté ministériel du 25 avril 2007, que « le respect de ces dispositions implique nécessairement que le chiffrement des bulletins de vote soit ininterrompu », et ce dès l'émission du vote sur le poste de l'électeur jusqu'à sa transmission au fichier dénommé « contenu de l'urne électronique ».

Enfin, si l'employeur a recours à un prestataire extérieur pour l'organisation du vote électronique, il reste malgré tout responsable de ce traitement de données. Le Conseil d'Etat précise ainsi que « la circonstance que des opérations de traitement de données soient confiées à des sous-traitants ne décharge pas le responsable de traitement de la responsabilité qui lui incombe de préserver la sécurité des données ». Cela ne méconnaît pas « le principe constitutionnel de responsabilité personnelle, dès lors que ces sous-traitants ont agi sur instruction du responsable de traitement ».

Le Conseil d'Etat a ainsi estimé que la sanction de la CNIL visant à rendre public l'avertissement était proportionnée au regard de la nature et de la gravité des manquements constatés, et sa publication appropriée « à la recherche de l'exemplarité ».

[block id="24761" title="Pied de page HAUT"]

A Lire aussi :
Nouveautés dans l'organisation des votes électroniques pour les élections professionnelles
3 points à retenir pour vos élections par Vote électronique
Le décret du 6 décembre 2016 qui modifie les modalités de vote électronique
Modalités de recours au vote électronique pour les Entreprises
L'Expert Informatique obligatoire pour valider les systèmes de vote électronique
Dispositif de vote électronique : que faire ?
La CNIL sanctionne un employeur pour défaut de sécurité du vote électronique pendant une élection professionnelle
Notre sélection d'articles sur le vote électronique

Source : http://www.snaless.org/vote-electronique-confidentialite-et-securite-des-donnees_juri_2855.php

---

1 milliard d’adresses mails volées, 2 pirates inculpés | Le Net Expert Informatique

1 milliard d’adresses mails volées, 2 pirates inculpés

Les deux pirates vietnamiens qui ont piraté 8 fournisseurs de services de messagerie américains et volé 1 milliard d’adresses et des informations confidentielles entre 2009 et 2012 ont été inculpés. Un troisième homme qui a permis de tirer 2 millions de dollars de cette affaire est aussi dans le collimateur de la justice.

Il s’agissait bien du casse du siècle. Deux pirates, de nationalité vietnamienne, ont été inculpés, le premier -plaidant coupable – pour le piratage de 8 fournisseurs de services de messagerie et le second pour le vol d’informations confidentielles. D’après le département de la Justice américaine (DOJ), il s’agit de la plus importante brèche de données dans l’histoire des États-Unis. Les attaques se sont déroulées entre février 2009 et juin 2012.
Après avoir volé ce trésor de guerre d’adresses mails, les pirates ont envoyé des spams à des dizaines de millions d’utilisateurs, et parvenus à générer 2 millions de dollars de profits, toujours selon le DOJ.
Quoc Nguyen, 28 ans, a piraté les serveurs de fournisseurs de messagerie et volé des données marketing contenant plus d’un milliard d’adresses mails et, avec son compère Giang Hoang (25 ans), utilisé ces données pour envoyer des spams. Ce dernier a été arrêté en 2012 avant d’être extradé aux États-Unis l’année dernière. Le verdict pour son procès est prévu le 21 avril. Quant à Quoc Nguyen, il est toujours en fuite. En parallèle, un grand jury fédéral a par ailleurs inculpé ce week-end un ressortissant canadien, Da Silva, co-propriétaire de 21 Celsius, une société qui fait tourner le site e-commerce Marketbay.com. Ce dernier s’est rendu complice de Nguyen en lui permettant de générer les 2 millions de dollars de revenus à partir des vols de données réalisées, entre mai 2009 et octobre 2011.

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://www.lemondeinformatique.fr/actualites/lire-1-milliard-d-adresses-mails-volees-2-pirates-inculpes-60472.html?utm_source=mail&utm_medium=email&utm_campaign=Newsletter

---

Les experts de la sécurité se penchent sur la Watch d’Apple | Le Net Expert Informatique

Les experts de la sécurité se penchent sur la Watch d’Apple

La firme de Cupertino a donc lancé officiellement sa montre connectée, la Watch, le 9 mars 2015 hier soir. Tout a été dit sur ce gadget déclinable en plusieurs versions dont une luxueuse au prix stratosphérique de 11 000 euros. Mais cette annonce a aiguisé la curiosité des experts en sécurité qui se sont penchés sur les faiblesses de la tocante numérique.

Nos confrères de The Register ont interrogé plusieurs spécialistes de la sécurité sur ce sujet. Ainsi, Ken Westin, chercheur chez Tripwire a indiqué que « le fait que le dispositif soit à la fois WiFi et Bluetooth va faciliter le développement des fonctionnalités supplémentaires à la montre et de s'interopérer avec d'autres équipements. Mais cela va également augmenter la surface d'attaque de l'appareil ». Pour lui, il ne fait aucun doute que « les chercheurs et les hackers ont été émoustillés pour trouver de nouvelles vulnérabilités et s'appuyer sur des attaques existantes qui profitent des faiblesses du WiFi et du Bluetooth ».

Problème de confidentialité des données
Un autre aspect de sécurité selon l'expert réside dans la confidentialité des données. « Avec ces connectivités, il sera intéressant de voir comment les données peuvent être utilisées pour suivre les personnes dans espaces physiques. Cela peut avoir un impact pour un cyberattaquant, tout comme pour des campagnes publicitaires trop ciblés ». L'arrivée d'applications tierces n'est pas faite pour rassurer le spécialiste qui y voit un risque supplémentaire pour la sécurité et la vie privée.

La fraude au paiement
En disposant d'une capacité NFC, l'Apple Watch peut servir pour le paiement mobile. Les risques de fraudes existent donc. Une récente étude de Drop Labs montre que le niveau de fraude sur les paiements avec Apple Pay est de 6% contre 1% en moyenne pour les transactions par carte bancaire. Pour la défense d'Apple, le problème vient surtout d'un niveau d'authentification faible de la part des banques. Une affaire récente a démontré ce risque. Certains spécialistes s'interrogent sur la fiabilité de la technologie NFC avec la capacité de la contourner.

Une révision des politiques de BYOD ?
Phil Barnett, directeur général EMEA de Good Technology, préfère souligner les menaces que les montres connectées et plus généralement les « wearables technology » impliquent dans le monde du travail. Elles s'inscrivent dans les politiques de BYOD (Bring Your Own Device) qui selon lui doivent être révisées. « Le BYOD a déjà connu les smartphones et des tablettes, les accessoires connectés arrivent comme les prochains véhicules de la donnée. Ils représentent une immense opportunité pour la productivité, mais ils nécessitent avant leur arrivée en entreprise de les sécuriser. »
Cela passe pour lui par plusieurs axes : « Chiffrement des données transitant sur le Bluetooth et la conteneurisation des données de l'entreprise. Par ailleurs, un contrôle plus granulaire des politiques de sécurité devrait permettre de trouver un équilibre entre risques et productivité. » A condition qu'il n'y ait pas de défaut dans la cuirasse, comme le montre la faille Freak qui affaiblissait le chiffrement des navigateurs Apple et Android. La firme de Cupertino vient d'ailleurs de publier iOS 8.2 qui règle ce problème.

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

Source : http://www.silicon.fr/les-experts-de-la-securite-se-penchent-sur-la-watch-dapple-110567.html

Les drones miniatures, une nouvelle arme aux mains des terroristes | Le Net Expert Informatique

Un drone aperçu au-dessus de Paris le 27 février 2015. (AFP)	**Les drones miniatures, une nouvelle arme aux mains des terroristes**

Les engins volants télécommandés se multiplient. Or, il est très facile d'y placer un explosif et d'activer la charge à distance

Des drones non identifiés sont repérés de plus en plus souvent au-dessus de nos têtes. Des dizaines de vols ont ainsi été aperçus ces six derniers mois en France, notamment dans le ciel de Paris et à la verticale de sites stratégiques, comme des centrales nucléaires ou des installations militaires – le dernier en date a été détecté samedi près de la base militaire de Seine-Port, où se trouve un centre de la Marine chargé des communications avec les sous-marins en plongée. Or, ces engins ne manquent pas d'inquiéter militaires et policiers, risque d'attentat oblige.

«Des drones vendus en magasin entre quelques centaines et quelques milliers de francs sont conçus pour transporter des appareils photo de 800 grammes à 4 kilos, indique Alexandre Vautravers, rédacteur en chef de la Revue militaire suisse. Il est facile d'y fixer une grenade à main, qui ne pèse que 500 grammes, et de leur adjoindre un mécanisme de déclenchement par téléphone portable. Un tel dispositif n'est pas très différent du système qui permet de déclencher un obturateur et peut être bricolé sans connaissances pointues. Il est couramment utilisé en Afghanistan et en Irak par des rebelles qui n'ont jamais fréquenté d'école d'ingénieurs.»

Une arme puissante

Ce constat est d'autant plus alarmant qu'une grenade à main constitue une arme puissante. Lâchée sur une foule, elle peut faire plusieurs dizaines de morts. Introduite dans un espace confiné, elle acquiert un pouvoir de dévastation décuplé. Il suffit, dans ce cas, d'une fenêtre ouverte et d'un pilote pas trop maladroit.

«Des drones non armés équipés d'une caméra peuvent également servir à des actions terroristes, continue Alexandre Vautravers. Ils sont susceptibles de réunir des informations précises sur des installations sensibles. Des photos aériennes de qualité permettent par exemple de déterminer l'épaisseur de leurs murs et donc la résistance de leurs bâtiments.»

Ces appareils facilitent aussi les attaques au lance-roquettes ou au mortier, comme en avait utilisé en son temps l'Armée républicaine irlandaise (IRA). Ils peuvent communiquer en temps réel l'emplacement précis de cibles à des tireurs placés à des centaines de mètres, voire à plusieurs kilomètres. Et après une première salve manquée, ils sont même susceptibles d'aider à corriger le tir.

Il ne s'agit pas là de science-fiction. Un attentat au drone miniature peut survenir à n'importe quel moment. Et, dans les milieux de la sécurité, personne ne doute que cette possibilité est envisagée très sérieusement par les organisations criminelles. Il s'agit donc aujourd'hui de mettre d'urgence au point une série de défenses.

Différents boucliers

Le premier type de parade est «cinétique». Ce qui signifie qu'il oppose à l'engin volant un autre corps en mouvement. En termes plus concrets, il consiste à repérer le drone à l'aide d'un radar ou d'un dispositif optique, puis de le frapper avec un projectile. «Un tireur d'élite est un bon moyen d'y parvenir, assure Alexandre Vautravers. Il a de grandes chances d'atteindre sa cible à une distance de 1000 mètres, ne coûte pas cher et ne représente guère de danger pour des tiers. Il est aussi possible d'utiliser des systèmes automatisés liés à des canons ou des missiles mais leurs munitions, plus lourdes, risquent de produire d'importants dégâts collatéraux.»

Un deuxième type de parade est «électromagnétique». Il consiste à brouiller les signaux échangés entre le drone et son pilote de manière à rendre l'appareil incontrôlable et donc incapable de commettre l'attentat prévu. Il suppose cependant de définir précisément les zones et les fréquences concernées, afin de limiter les dommages involontaires.

Un troisième type de parade est d'ordre légal. «Un certain nombre de pays, dont les Etats-Unis, y travaillent déjà, confie Alexandre Vautravers. Le législateur peut, par exemple, imposer aux constructeurs d'installer sur leurs drones des puces GPS qui limitent l'accès de leurs engins à certaines zones.»

Il reste à mesurer le danger réel que ces petits véhicules font courir à nos sociétés. «Dans toute analyse du genre, deux facteurs doivent être pris en compte, rappelle Alexandre Vautravers: la gravité et la probabilité de l'événement redouté. Sur le premier point, un attentat au drone miniature, s'il aurait sans doute un gros impact médiatique, ne ferait pas un nombre particulièrement élevé de victimes. Sur le second, en revanche, aucun doute n'est permis: nous y sommes.»

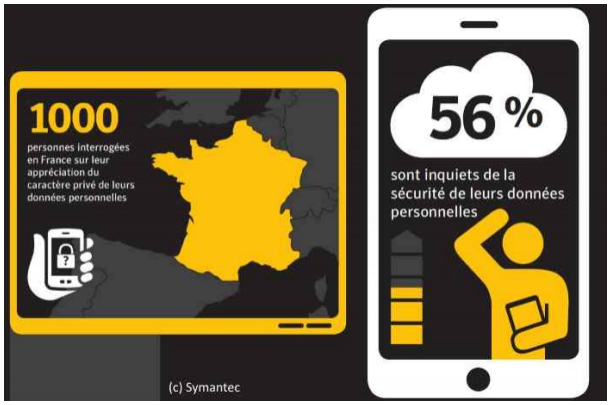
Cibles emblématiques

Que faire? Comme il serait beaucoup trop cher de tout protéger tout le temps, il paraît judicieux de défendre en priorité les cibles les plus emblématiques, tels les centrales nucléaires, les installations militaires et les grands rassemblements. Et pas seulement en raison de leur propre importance. Empêcher les attentats à grand retentissement médiatique revient aussi à rendre les attentats moins attrayants et donc, en principe, à en limiter drastiquement le nombre.

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

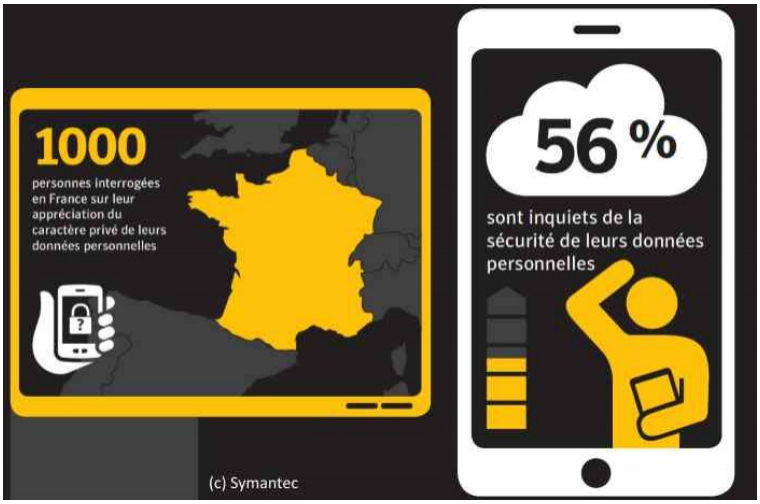
Source : http://www.letemps.ch/Page/Uuid/ed81bf30-c68f-11e4-959d-74804f4bcbe7/Les_drones_miniatures_une_nouvelle_arme_aux_mains_des_terroristes
Par Etienne Dubuis

88% des consommateurs font de la sécurité des données personnelles un élément clé de l’acte d’achat | Le Net Expert Informatique



88% des consommateurs font de la sécurité des données personnelles un élément clé de l’acte d’achat

Selon l'étude « State of Privacy » de Symantec, les consommateurs n'accordent que peu de confiance aux entreprises et administrations pour gérer leurs données personnelles. Au point de mentir.88% des consommateurs font de la sécurité des données personnelles un élément clé de l'acte d'achat, devant la qualité des produits ou le service client. Ce résultat frappant est issu d'une étude réalisée par Symantec auprès de 7000 consommateurs européens. S'il est évident que la sécurité d'un numéro de carte bancaire est un élément clé de l'achat sur un site e-commerce, la défiance des consommateurs va bien au delà. Ainsi, seulement 19% des Européens font confiance au secteur de la distribution pour la protection des données personnelles.
La confiance la plus élevée va aux hôpitaux (71% de confiance) devant les banques (62%) et l'Etat (37%). Les réseaux sociaux sont en queue de peloton avec un petit 8%. D'une manière générale, l'inquiétude à propos des données personnelles concerne 56% des consommateurs. Et 59% ont déjà eu une mauvaise expérience au sujet de leurs données personnelles.



Mentir pour se protéger
Face à la défiance générale, les consommateurs n'hésitent pas à mentir pour se protéger. Un répondant sur trois a avoué avoir donné de fausses informations en ligne. Le comportement se développe surtout chez les jeunes : 48% des 18-24 ans ont ainsi déjà menti. Mais un petit tiers accepte de laisser une adresse mail en échange d'avantages. 57% hésitent à laisser des informations personnelles à l'occasion d'un achat. Mais moins d'un sur cinq lisent les conditions d'utilisations des données avant d'n déposer.
La valeur des données est désormais bien prise en compte. 24% des répondants jugent que leurs données personnelles ont une valeur supérieure à 10 000 euros.

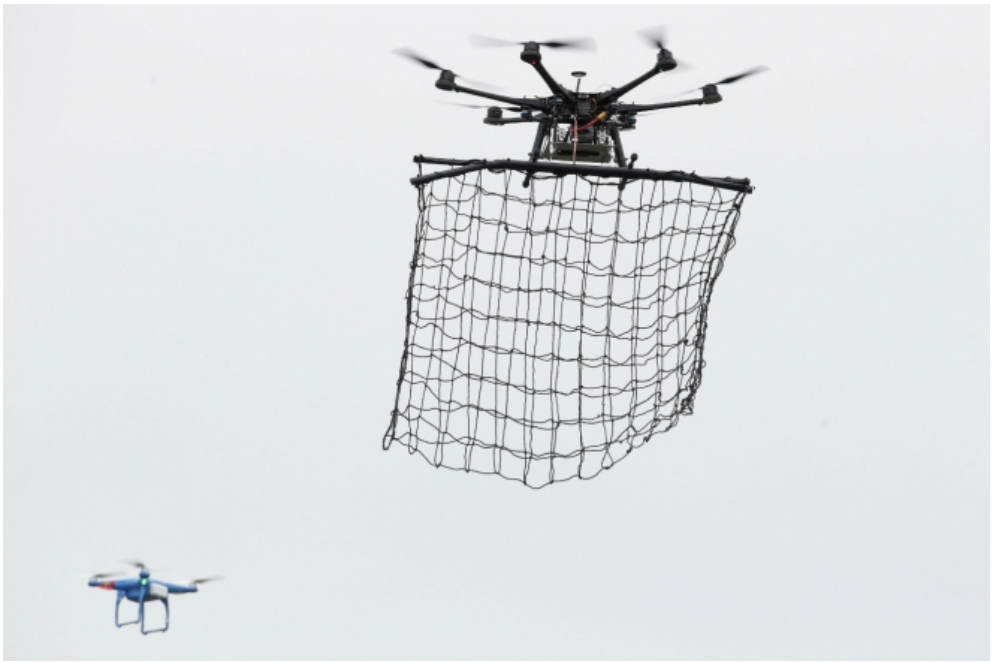
Vers un rôle accru de l'Etat
Qui doit agir pour mieux protéger les données personnelles ? Les résultats sont partagés. 36% des Européens et 37% des Français jugent que c'est à l'Etat d'agir avec plus de sévérité et d'efficacité. 30% des Européens et 36% des Français jugent que c'est aux entreprises avant tout d'oeuvrer pour que les données soient mieux protégées. Enfin, 33% des Européens mais seulement 27% des Français estiment que c'est de la responsabilité des individus eux-mêmes. Autrement dit : les Français sont les plus enclins à se déresponsabiliser au niveau individuel de ce qu'ils font eux-mêmes de leurs propres données personnelles.

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://www.cio-online.com/actualites/lire-donnees-personnelles%C2%A0-l-etat-de-defiance-7435.html
Par Franck Salien, Journaliste

La guerre des drones a commencé… | Le Net Expert Informatique



La guerre des drones a commencé…

Face à ces engins robotisés qui nous épient depuis le ciel, la riposte s'organise. Mais pour l'heure, les solutions envisagées sont dignes d'un épisode de Fantômas ! Et les inspecteurs Juve sont sur les dents…

La nouvelle menace qui agite les médias depuis quelque mois a quelque chose de furieusement rétro, comme un roman de SF des années 60. De mystérieux engins robotisés nous survolent, épient nos moindres faits et gestes. Qui les contrôle ? S'agit-il de pirates s'amusant à braver les autorités, pour le simple frisson que procure la provocation ? Ou la menace est-elle plus sérieuse, provenant d'une firme, d'un Etat, voire d'une organisation terroriste ? Les forces de l'ordre semblent en tout cas impuissantes à endiguer cette prolifération de drones qui bourdonnent au-dessus de nos villes et centrales nucléaires, réduites qu'elles sont à en à recenser leurs apparitions. Certains policiers ont bien tenté de suivre les engins, sans arriver pourtant à mettre la main sur leurs propriétaires.
En vérité, il peut s'agir de n'importe qui. Loin d'être réservés à une élite friquée, les drones sont aujourd'hui accessibles au grand public. Bien sûr, leurs performances dépendent du prix que l'on est prêt à débourser pour en obtenir un. Mais même en se contentant d'un appareil d'entrée de gamme, c'est-à-dire 300 euros environ, il est possible de filmer de superbes vues des calanques marseillaises… ou Scarlett Johansson en petite tenue, pour peu qu'elle ait oublié de fermer les volets de sa résidence parisienne. Tout comme Internet, les drones ont dévié de leur fonction originelle, militaire, pour s'adapter à un usage mercantile mettant leur utilisation à la portée des civils. Tout comme Internet, les drones permettent de décupler nos capacités créatrices lorsqu'ils sont utilisés avec sagesse, mais aident également les terroristes à planifier leurs attaques lorsqu'ils sont employés par exemple par Daech pour glaner des informations sur les bases de l'armée syrienne.

COMMENT DÉTRUIRE UN OBJET SURVOLANT UNE ZONE HABITÉE SANS METTRE LA POPULATION EN DANGER PAR LES RETOMBÉES DE DÉBRIS ?
Bien entendu, c'est l'emploi des drones avec de mauvaises intentions qui intéresse les médias et inquiète la population. Et cette inquiétude est justifiée, puisque la riposte anti-drone en est aujourd'hui à ses balbutiements alors que les utilisateurs se multiplient à une vitesse folle. La France a pourtant rapidement légiféré en créant deux arrêtés au mois d'avril 2012, afin d'encadrer les utilisateurs de drones. Mais force est de constater que presque trois ans plus tard, malgré le cadre mis en place, les possesseurs de drones n'ont droit, en guise de mise en garde, qu'à une simple brochure de deux pages publiée en décembre dernier par la Direction générale de l'aviation civile (DGAC) et qui leur est remise lors de l'achat de leur appareil. A cela vient s'ajouter les recommandations des vendeurs. Autant dire que la loi n'est quasiment jamais respectée… Il suffit de se promener sur les sites de partage de vidéo pour voir le nombre de films amateurs ou même professionnels qui font fi de toutes les interdictions, notamment celle de voler au-dessus d'une zone peuplée…
Le gouvernement aimerait pouvoir riposter, mais les solutions manquent. Comment détruire un objet survolant une zone habitée sans mettre la population en danger par les retombées de débris ? L'Agence nationale de la recherche a ainsi été dotée d'un budget d'un million d'euros pour trouver une parade fiable à ces aéronefs invasifs. Mais à l'heure actuelle, aucune méthode véritablement efficace ne semble s'imposer. Il suffit pour s'en convaincre de faire un petit tour d'horizon des pistes explorées pour contrer les bourdons robotisés.

– Le bouclier anti-drone :
« DroneShield » est un projet américain de module personnel, que l'utilisateur peut installer chez lui (ou tout autre endroit où il se sentirait menacé par les petits robots espions) et qui est équipé d'un microphone permettant de détecter la signature acoustique de drones dans les alentours. L'utilisateur est ensuite prévenu par un message envoyé sur son téléphone. Bref, ça ne permet pas de neutraliser un drone, mais c'est un début de riposte que de savoir que l'on est observé depuis les cieux…

– Le drone anti-drones :
Une entreprise française basée à Vitry-sur-Seine a créé un drone appelé « Interceptor MI200 » (on ne rigole pas). Le principe de celui-ci est d'embarquer un filet permettant d'intercepter et capturer un drone. Mais outre le fait qu'on imagine mal une flopée d' « Interceptor » envahir le ciel pour parer à chaque drone civil volant dans des zones illégales, il est intéressant de noter que la DGAC n'a pas encore donné son accord pour autoriser ce dernier à voler (exception faite aux professionnels). Bref, le citoyen lambda n'est pas près de pouvoir mener des combats de robots au-dessus de son jardin. Et puis si l'on lance des drones pour intercepter des drones, il faudra peut-être demain envisager des drones pour intercepter des drones qui interceptent des drones… Bref, une transposition futuriste de l'ambiance chassé-croisé des vacances d'été sur l'Autoroute du Soleil, mais dans le ciel.

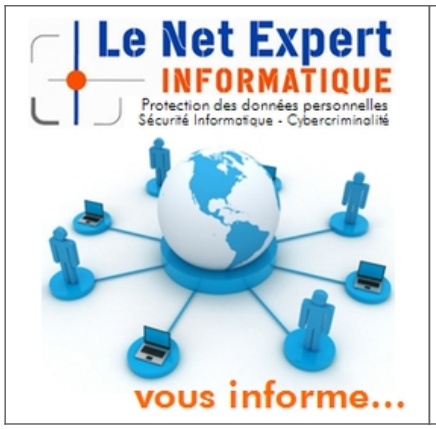
– Le canon-laser :
L'Académie chinoise de génie physique a mis au point un laser permettant de neutraliser « à 100% » de petits drones dans les cinq secondes suivant leur détection. Mais malgré une précision que l'on imagine plus élevée que celle des armes de la gendarmerie, le laser ne résout pas la question des débris pouvant retomber sur les civils.

Michèle Rivasi, députée EELV, préconise quant à elle une solution moins fantasque : « Il faut une traçabilité du drone. Comme on a des numéros d'immatriculation sur les voitures […], il y aurait un numéro typique pour les drones. Comme quand on possède une arme, on saurait à qui appartient le drone ». Du côté des constructeurs, il a été convenu d'intégrer des zones d'exclusion dans les GPS des drones vendus dans le commerce empêchant les appareils de décoller si la destination programmée est interdite. De bonnes idées, même si on imagine que les hackers trouveront rapidement le moyen de contourner ces contraintes…

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

Source : http://www.marianne.net/drones-peur-ville-impunite-les-airs-100231820.html
Par Francois Mori

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

E-commerce: ce que la loi Hamon a changé dans la vente en ligne – | Le Net Expert Informatique

E-commerce : ce que la loi Hamon a changé dans la vente en ligne

La loi Hamon relative à la consommation encadre les pratiques des cybermarchands en matière d'information et de droits du consommateur. Le point sur les règles à respecter pour éviter les sanctions.
La loi Hamon sur la consommation est entrée en vigueur le 14 juin dernier. Elle renforce l'information et la protection du consommateur et permet de mieux encadrer le commerce en ligne à l'échelle européenne. Objectif : sécuriser les ventes par internet. Voici les principales mesures à mettre en place pour respecter la loi, éviter des pénalités et gagner en fiabilité donc augmenter les ventes.

L'information du consommateur est primordiale. Exemple. Le client doit se voir notifier au plus tard au début de la commande les moyens de paiement acceptés (CB, chèques, cartes cadeaux) mais pas seulement. Si aucun délai de livraison n'est indiqué, les produits doivent être livrés au plus tard 30 jours après la commande.
Autre point de vigilance lors du récapitulatif de la commande : l'interdiction des cases pré-cochées (suggestion d'achat, emballage cadeau, livraison express, assurance annulation). Le droit de rétractation du client est allongé à 14 jours (si cette information est absente, il bénéficiera de 12 mois) et son remboursement après rétractation doit se faire dans les 14 jours suivant le retour. Un rappel des Conditions Générales de Vente (CGV) doit aussi apparaître avant validation. Celles-ci sont essentielles. Elles doivent être disponibles dans un format imprimable standard non modifiable (type pdf). Pensez à les modifier sur les points suivants: délais de livraison, garanties et SAV, moyens de paiement, politique de rétractation, responsabilité du commerçant. En cas de non respect, le e-commerçant peut être jugé pour clause abusive.

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://lentreprise.lexpress.fr/marketing-vente/ebusiness/infographie-e-commerce-ce-que-change-la-loi-hamon_1650150.html

Sur les réseaux sociaux, il y aura bientôt plus de morts que de vivants | Le Net Expert Informatique

(Photo : Dado Ruvic/archives Reuters)	**Sur les réseaux sociaux, il y aura bientôt plus de morts que de vivants**

Un utilisateur sur cent de Facebook est décédé. Comment est prise en compte la mort sur Internet ? La Commission nationale de l'informatique et des libertés lance le débat.

« Dans quelles conditions les héritiers peuvent-ils récupérer les données d'un défunt ? », « Comment résoudre les conflits entre héritiers qui n'ont pas toujours la même perception de la volonté post-mortem du défunt ? » Autant de questions délicates, posées de plus en plus régulièrement à la Cnil (Commission nationale de l'informatique et des libertés) dans ses échanges avec les internautes.
Ces interrogations risquent de se poser encore plus souvent dans les années à venir. Car à terme, si la loi n'évolue pas, il pourrait y avoir sur les réseaux sociaux plus de morts que de vivants…

La mort est-elle suffisamment prise en compte sur Internet ? La Commission nationale de l'informatique et des libertés (Cnil) est régulièrement confrontée à des questionnements d'héritiers concernant le décès d'un proche et la gestion de sa vie numérique. Le débat sur « la mort numérique » est lancé.

« Dans quelles conditions les héritiers peuvent-ils récupérer les données d'un défunt ? », « Si rien n'est prévu dans les conditions générales d'utilisation des sites, quels sont les héritiers qui pourront demander la mise à jour ou la suppression des données ? », « Comment résoudre les conflits entre héritiers qui n'ont pas toujours la même perception de la volonté post-mortem du défunt ? » Autant de questions délicates, posées de plus en plus régulièrement à la Cnil (Commission nationale de l'informatique et des libertés) dans ses échanges avec les internautes.

Ces interrogations risquent de se poser encore plus souvent dans les années à venir. Car à terme, si la loi n'évolue pas, il pourrait y avoir sur les réseaux sociaux plus de morts que de vivants !

Sur Facebook, un mort sur cent
Actuellement, un utilisateur sur cent de Facebook est décédé. Le réseau social ne peut supprimer lui-même les comptes, en l'absence de demande des proches ou familles : comment peut-il savoir si l'utilisateur est décédé ou tout simplement inactif ? De ce contexte a émergé le concept de « mort numérique », à la fois porteur d'interrogations juridiques et sociétales.

La Cnil ayant pour rôle de contrôler la protection des données personnelles ainsi que de veiller à ce que le développement des nouvelles technologies ne porte atteinte « ni à l'identité humaine ni aux droits de l'homme, ni à la vie privée ni aux libertés individuelles ou publiques », s'est penchée sur le sujet en fin d'année 2014, afin d'ouvrir un débat sur les enjeux de la mort numérique.

Référencé à vie ?
Actuellement, si la personne concernée par le décès n'a pas programmé l'effacement de ses données, un profil numérique continue de vivre après la mort. Il reste visible sur la toile et référencé sur les moteurs de recherche. L'objectif de la Cnil est alors de savoir comment concilier le droit à l'oubli numérique et les possibilités d'atteindre l'éternité numérique offerte par la vie en ligne.

Au regard de la loi Informatique et libertés, les héritiers d'une personne décédée justifiant leur identité peuvent exiger du responsable d'un site internet qu'il « prenne en considération le décès et procède aux mises à jour qui doivent en être la conséquence ». Mais la loi ne prévoit aucune transmission des droits du défunt aux héritiers. L'héritier en question ne peut donc avoir accès aux données numériques du proche décédé.

Cependant, d'après la Cnil, les familles des personnes disparues qui s'adressent à elle « veulent pouvoir accéder aux données concernant le défunt ou exigent au contraire leur suppression ». La commission se trouve face à des problématiques techniques et juridiques : sans expression de la volonté du défunt, il est difficile d'agir.

La loi n'évoluant pas encore, faute de cas de jurisprudence, des start-up et les réseaux sociaux eux-mêmes commencent à proposer des fonctionnalités pour paramétrer sa mort numérique.

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

Source : http://www.ouest-france.fr/sur-les-reseaux-sociaux-il-y-aura-bientot-plus-de-morts-que-de-vivants-3194974
Par Jeanne HUTIN