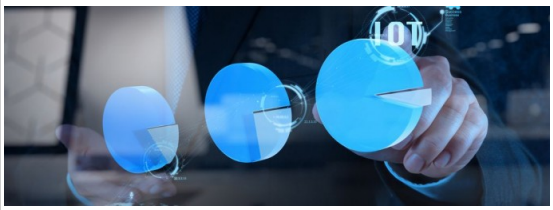
L’Internet des objets boostera-t-il l’Europe ?

L’Internet des objets, boostera-t-il l’Europe ?

En plein CES de Las Vegas, AT Kearney vient de livrer une version rafraîchie de son étude sectorielle sur la high-tech en Europe avec un focus #IoT.



L'Internet des objets donnera-t-il un nouveau souffle au secteur high-tech en Europe ? AT Kearney a publié un focus dans ce sens qui montre tout le potentiel…s'il est bien exploité.
En pleine effervescence du CES organisé à Las Vegas, le cabinet de consulting d'origine américaine vient de présenter à Paris la troisième version de son étude sur les nouvelles technologies en Europe sous l'angle de l'IoT
C'est une véritable opportunité de croissance sur les 10 prochaines années, estime Hervé Collignon, Partner d'AT Kearney, expert en TMT (télécoms, médias et technologies) et co-auteur du rapport.
Ce potentiel économique est estimé à près de mille milliards d'euros d'ici 2025. Il pourrait correspondre à 7 points de PIB à cet horizon.
Et les start-up comme Sigfox, Netatmo ou Withings et les groupes industriels français ont une carte à jouer. Ils ont pris position sur le marché des objets connectés dans le BtoC et le BtoB (historiquement via le M2M).
Dressons d'abord le tableau des perspectives présumées gigantesques de cet Internet des objets, qui va permettre « l'interconnexion du monde physique en facteur 10 par rapport à l'Internet phase 1 ».
Entre les technologies exponentielles (capteurs, bande passante, hardware, stockage & cloud), la population connectée (3 milliards de personnes en 2015), les effets réseaux (peering, IPv6, plateformes, interopérabilité…) et l'essor du big data, tous les ingrédients sont réunis pour assister à une « nouvelle révolution » qui va toucher tous les secteurs d'activité, estime Hervé Collignon.
A l'horizon 2025, le marché des solutions IoT en Europe (hors fabrication des objects connectés) est évalué à 80 milliards d'euros. Les intégrateurs de systèmes (IBM, Accenture, Atos…) remporteraient la plus grosse part du gâteau : plus d'un quart du business généré (22 milliards d'euros), devant les fournisseurs de services et de plateformes (le club GAFA et les opérateurs télécoms) qui pourraient en tirer un business de 18 milliards d'euros….
On retrouverait les opérateurs dans une autre catégorie : les spécialistes de la connectivité pour l'IoT. Un segment qui pourrait peser 15 milliards d'euros à l'horizon 2025 et qui comporte des pure players comme Sigfox.
Toujours selon le cabinet en stratégie qui a présenté mardi midi les résultats de son étude à Paris, on devrait recenser dans dix ans une base installée de 26 milliards d'objets connectés (correspondant à un marché de 10 milliards d'euros pour les fournisseurs de composants et modules comme Sierra Networks, Telit ou Gemalto).
L'essor de la dimension Internet des objets devraient avoir un impact sur 5 secteurs principalement : le transport et l'hôtellerie (250 milliards d'euros), la santé (235 milliards d'euros), la domotique domestique (160 milliards d'euros), le matériel industriel (pour un montant similaire), et la distribution, commerce (hors commerce électronique) et vente en gros (60 milliards d'euros).
Divers paramètres pourraient modifier cette perspective apportée par AT Kearney : le niveau d'adoption des objets connectés par les consommateurs, la politique industrielle associée à l'IoT en Europe (balbutiante en l'état actuel malgré une certaine prise de conscience par la Commission européenne), la guerre d'influence des plateformes (Google, Apple, Samsung…), la rationalisation des standards IoT sur fond de consortiums puissants (Open Interconnect, Allseen Alliance, Industrial Internet Consortium…), l'avancée de la 5G en Europe, l'impact de l'IoT sur l'emploi et la juste appréciation du traitement des données.
Etude « The Internet of Things : a new path to European Prosperity », ATKearney, janvier 2016, co-auteurs : Thomas Kratzert et Michael Broquist (respectivement Partner et Principal à Stockholm), Hervé Collignon et Julien Vincent (respectivement Partner et Principal à Paris)
En savoir plus sur http://www.itespresso.fr/europe-vraie-puissance-internet-objets-117702.html#2t626JMWackx6u04.99

Réagissez à cet article

Source : *L'Europe, une vraie puissance de l'Internet des objets ? | ITespresso.fr*

L'aviation civile n'est pas à l'abri du cyber-terrorisme

L'aviation civile n'est pas à l'abri du cyber-terrorisme

A la demande de l'Agence européenne de sécurité aérienne (Aesa), un hacker pourvu d'une licence de pilote d'avion commercial a démontré qu'il pouvait en quelques minutes entrer dans le système de messagerie des compagnies maritimes.

A l'instar des machines industrielles et des objets domestiques connectés, les véhicules et les avions n'échapperont pas aux attaques des cybercriminels. « L'aviation civile doit se préparer aux cyber-risques », prévient d'ailleurs Patrick Ky, le directeur exécutif de l'Agence européenne de sécurité aérienne (Aesa). En poste depuis 2013, ce dernier s'est exprimé lors d'un petit déjeuner organisé par l'association des journalistes de la presse aéronautique et spatiale (Aspae) en octobre dernier. Ses propos ont été rapportés dans de nombreux journaux tels que Les Echos, Le Parisien ou encore l'Usine Nouvelle. Patrick Ky est formel : le piratage informatique d'un avion est possible et la cybercriminalité représente bien une véritable menace pour le transport aérien.

Pour illustrer ses propos, le directeur exécutif de l'Aesa a confié qu'il avait fait appel à un Hacker. Cet expert en informatique – également titulaire d'une licence de pilote d'avion commercial – est parvenu en quelques minutes à entrer dans le système de messagerie Acars (Aircraft Communication Addressing and Reporting System) en se faisant passer pour un des administrateurs du réseau. Lequel sert aux compagnies aériennes à envoyer des messages automatiques et réguliers de l'avion vers le sol pour s'assurer du bon fonctionnement des systèmes critiques de l'avion.
Risque accru. Demain, le risque de cyberattaque va être accru avec la mise en place du système Sesar (Single European Sky ATM Research ; en français : Ciel unique européen) qui vise à harmoniser en Europe le trafic aérien en déployant un réseau et de nouveaux systèmes de gestion d'ici 2025. Ce nouveau réseau européen de contrôle du trafic aérien aura la possibilité de donner directement des instructions aux systèmes de contrôle de l'avion. Pour limiter les risques de piratage, l'agence européenne pourrait, à long terme, se charger de certifier les équipements contre les risques de cyberattaques sachant qu'elle a déjà la responsabilité de certifier les aéronefs en Europe. A court terme, Patrick Ky veut mettre en place une structure en charge d'alerter les compagnies aériennes sur les cyberattaques. Un risque sur lequel Air France, que nous avons contacté, ne s'est pas encore publiquement prononcé.

Réagissez à cet article

Source : *L'aviation civile n'est pas à l'abri du cyber-terrorisme*

Les téléphones cryptés, le casse-tête des enquêtes antiterroristes

Les téléphones cryptés, le casse-tête des enquêtes antiterroristes

Invité à s'exprimer sur France Inter, vendredi 8 janvier, sur les attentats qui ont frappé la France en 2015 et l'attaque, la veille, d'un commissariat du 18e arrondissement de Paris, le procureur de la République à Paris, François Molins, est revenu sur l'une des principales difficultés techniques à laquelle font face les enquêteurs en matière d'antiterrorisme : travailler sur les « téléphones cryptés » retrouvés, dont les codes de verrouillage sont de plus en plus complexes à casser.

« Tous les smartphones qu'on essaie aujourd'hui d'exploiter sont verrouillés et cryptés (…) *toutes les communications passées par les terroristes sont passées à l'aide de logiciel de cryptage »*, a expliqué M. Molins, qui a cependant tu les noms des principaux logiciels utilisés.
« Les évolutions technologiques et les politiques de commercialisation d'un certain nombre d'opérateurs font que si la personne ne veut pas donner le code d'accès on ne peut plus rentrer dans les téléphones », a souligné M. Molins. La totalité des données deviennent ainsi inaccessibles à quiconque ne possède pas le code de déblocage.

PLUSIEURS TÉLÉPHONES N'ONT TOUJOURS PAS ÉTÉ « CASSÉS »

Une difficulté qui rend les enquêteurs *« aveugles »* dans certains cas et les prive de moyens d'investigation, a regretté M. Molins, en citant notamment le cas de Sid Ahmed Ghlam.
L'un des téléphones de l'étudiant algérien soupçonné d'un projet d'attentat contre une église de Villejuif au printemps n'a, en effet, toujours pas été « *cassé* » par les policiers. Mais un iPhone 4S saisi dans le cadre de l'enquête sur le 13 novembre garde également, à ce jour, tous ses mystères.
Dans les jours qui ont suivi les attentats du 13 novembre, la direction centrale de la police judiciaire (DCPJ) a ainsi demandé à tous ses services de résumer les problèmes posés par les *« téléphones cryptés ».« Les téléphones de dernière génération disposent de codes verrous très compliqués à casser ou contourner »*, expliquait au *Monde* le service central de l'informatique et des traces technologiques de la police judiciaire (SCITT) en réponse à la demande de la DCPJ.

De quoi inquiéter ces experts de la police scientifique : *« Les solutions utilisées ne sont pas pérennes, dans la mesure où elles sont basées sur l'exploitation de failles logicielles, le plus souvent corrigées lors des mises à jour. »* C'est le cas de l'iPhone de l'enquête du 13 novembre.

En 2014, sur 141 téléphones analysés par le SCITT, six n'ont pu être explorés. Quant à 2015, *« huit smartphones n'ont pas pu être pénétrés dans des affaires de terrorisme ou de crime organisé »*, a détaillé M. Molins.

Concernant le cryptage, *« il n'existe à ce jour aucune solution permettant aux services techniques de déchiffrer systématiquement les données »*, assure la sous-direction de la lutte contre la cybercriminalité, également sollicitée par *Le Monde*.

UNE ACTION JURIDIQUE POUR REMÉDIER AU PROBLÈME

Deux solutions s'offrent alors aux services d'enquête judiciaire. D'abord faire appel à la direction générale de la sécurité intérieure (DGSI). Mais le centre technique d'assistance du service de renseignement répond dans un délai moyen de trois mois, et sans garantie de succès. De toute façon, reconnaît une source à la DCPJ, *« cette possibilité semble ignorée par de nombreux services »*. Les policiers peuvent aussi, éventuellement, se tourner vers les fabricants, dont certains, comme Apple, acceptent désormais, *« dans le cadre d'une urgence vitale »*, de communiquer les données stockées dans le « cloud ». A supposer qu'une sauvegarde ait été réalisée par le mis en cause.
Autant dire que le pessimisme règne du côté des services d'enquête comme des experts de la police technique et scientifique. *« Il paraît illusoire d'attendre une solution multisupport qui permettrait un accès aux données verrouillées. Seule une action juridique pourrait permettre d'obtenir ces données par le biais d'un instrument légal… Le problème réside cependant dans le poids d'un tel outil juridique face à des opérateurs ou des industriels ayant leur siège à l'étranger »*, conclut le SCITT.

Réagissez à cet article

Source : *Les téléphones cryptés, casse-tête des enquêtes antiterroristes*

Par Laurent Borredon

Est-ce que la réutilisation de données personnelles sera possible dans le nouveau

Règlement vie privée ?

	Est-ce que la #réutilisation de données personnelles sera possible dans le #nouveau Règlement vie privée ?

Tout praticien de la protection des données personnelles a déjà été confronté au problème du changement de finalité d'utilisation des données. Exemple : elles ont été collectées pour une finalité d'exécution d'un service en ligne (accès à un réseau social ou livraison d'un bien acheté) et on voudrait aujourd'hui les vendre en vue d'alimenter une processus de profilage big data. Les conditions de pareils changements de finalité ont divisé les juristes et organes de contrôle depuis la directive de 1995. Le nouveau règlement semble avoir tranché : la poursuite d'une nouvelle finalité incompatible avec la première est interdite, sauf consentement préalable des personnes concernées.

La problématique

On ne peut pas savoir au moment de la collecte des données personnelles à quoi elles pourront servir dans quelques mois ou années. Surtout dans un contexte d'évolution technologique permanente et de plus en plus rapide.

Le gestionnaire des données est donc un jour ou l'autre tenté d'utiliser les données en sa possession, pour une finalité autre que celle annoncée initialement. Du reste, on rappelle que s'il n'utilise plus les données, le gestionnaire doit les effacer après une période qui dépend de la finalité de départ. Choix cornélien donc : soit j'efface les données si je reste dans la finalité de départ et que celle-ci a été exécutée, soit je les réutilise pour une nouvelle finalité si je souhaite conserver les données.

Les processus de Big data offrent un parfait exemple de la problématique. Les outils de profilage demandent par définition de se nourrir de très nombreuses observations issues de traitements de données divers et variés. La plupart du temps, ces traitements n'ont pas été mis en œuvre pour permettre un processus de profilage. Cette finalité n'était pas prévue initialement (par exemple, l'inscription et la gestion d'un jeu en ligne sur internet ; l'inscription et l'utilisation un site d'échanges en vue de vendre certains biens etc.). La nouvelle finalité est souvent incompatible avec la première et, selon les lois sur la protection des données personnelles, elle est a priori interdite.

Deux interprétations semblaient s'affronter :

• Soit on considérait que la nouvelle finalité incompatible ne pouvait être poursuivie qu'à la condition de recueillir le consentement de la personne concernant la nouvelle finalité d'utilisation des données. Dans notre exemple, le responsable qui veut se relancer dans son projet Big data, doit réinterroger chaque personne afin d'obtenir son consentement explicite sur la nouvelle finalité d'utilisation.

• Soit on admet y voir un nouveau traitement pouvant être poursuivi comme tel, c'est-à-dire en le soumettant à l'intégralité de la protection légale (information des personnes concernant la nouvelle finalité, nouvelles mesures de sécurité ou de sauvegarde si nécessaires, détermination d'une nouvelle base de licéité qui n'est pas forcément le consentement de la personne mais par exemple un équilibre d'intérêts avec droit d'opposition, nouvelle déclaration auprès de l'autorité de protection des données etc.). Cette deuxième opinion, plus souple, permet d'admettre une évolution inévitable des finalités d'utilisation, tout en garantissant les droits et libertés de la personnes.

Le système sévère du futur Règlement

La disposition finale du projet de Règlement ne comprend plus aucune disposition concernant le problème du changement de finalité et les conditions dans lesquelles il aurait pu intervenir.

L'évolution du texte témoigne d'un véritable débat sur ce point.
Le texte initial ne contenait aucune règle spécifique.

La seconde version a introduit un nouveau paragraphe ayant cet objet (article 6§4). Si les données étaient collectées par le même responsable du traitement, la poursuite d'une finalité ultérieure aurait été permise malgré l'incompatibilité des finalités, pour autant que l'on ait pu justifier celui-ci par une des hypothèses générales de licéité prévue au §1er(consentement, exécution d'un contrat, intérêt vital de la personne etc.).

En d'autres termes, selon la deuxième version du texte, le responsable aurait toujours pu remédier à une incompatibilité entre la finalité initiale et les finalités ultérieures du traitement, en identifiant une nouvelle base de licéité du traitement. En fin de compte, le responsable pouvait toujours prendre le risque de fonder la licéité du nouveau traitement sur la fameuse balance des intérêts, et gérer les soucis a posteriori.

La dernière version du Règlement, ayant fait l'objet du dernier vote en commission, a purement et simplement retiré ce paragraphe.

Le Groupe Article 29 a donc obtenu satisfaction, lui qui avait fortement critiqué cette disposition qui, à ses yeux, mettait à mal et vidait de sa substance le principe de finalité (cfr. Article 29, Opinion 03/2013 on purpose limitation, 2 avril 2013, p. 36 et 37).

Le principe de base est dès lors celui de l'exigence de la compatibilité des finalités nouvelles avec les finalités initiales, sauf consentement de la personne concernée ou un texte légal spécifique le permettant pour des finalités spécifiques (sécurité nationale, défense, sécurité publique etc.) En cas d'incompatibilité, la poursuite de la finalité incompatible est donc prescrite et le changement de finalité rendu illicite.

Des conséquences pratiques importantes

Le Règlement choisit donc la sévérité concernant le régime de changement des finalités.

L'interdiction de traitement en cas d'incompatibilité des finalités s'oppose à l'évolution d'un traitement de données qui est en quelque sorte « figé » par sa finalité réelle de départ. Si des données ont été traitées pour les besoins d'exécution d'un contrat, elles ne pourront la plupart du temps pas être traitées pour une communication à un tiers en vie d'alimenter un processus de profilage big data car ce sera considéré comme finalité incompatible, sauf à obtenir a posteriori le consentement de chacune des personnes concernées.

Sans aller jusqu'à autoriser le changement de finalité sans garantie particulière, un moyen terme était possible si on était parti du principe que la seconde finalité générait un « nouveau » traitement qui devait être soumis au respect de l'intégralité des dispositions de la loi (nouvelle information des personnes, identification d'un nouveau critère de licéité, identification des mesures de sécurité spécifiques, le cas échéant, etc.) et pas seulement à la seule exigence de la licéité.

La solution du Règlement est autre : on ne peut pas modifier une finalité annoncée sans le consentement préalable de la personne. Ce qui pose non seulement problème pour le traitements futurs mais aussi question pour les traitements antérieurs ou qui seront en cours au moment de l'entrée en vigueur du futur Règlement. Le Règlement ne prévoit en effet pas de régime transitoire.

Réagissez à cet article

Source : *Nouveau Règlement vie privée : la réutilisation de données sera-t-elle encore possible ?*

Vol et fuite de données, comment les éviter ?

Vol et fuite de données, comment les éviter ?

Les données, tout le monde le sait désormais, sont d'une importance capitale et d'une valeur inestimable. En tant qu'entreprise, comment les valoriser et surtout comment bien les protéger ?

Et si vous possédiez déjà l'argile des futurs développements de votre entreprise ? En effet, en travaillant les données récoltées par les différents services de votre société, vous pouvez déjà optimiser vos produits et services actuellement commercialisés notamment via l'analyse des données liées à la satisfaction des clients. Mais, plus encore, vous pouvez également faire évoluer vos produits et services voire en créer de nouveaux. **L'étude des data permet de comprendre les usages et de modifier les produits et services en fonction de ces usages**.
Citons les statistiques sur les données révélant les besoins des usagers des transports publics. Citons plus précisément la compréhension des verbatims-clients grâce au logiciel d'analyse sémantique de Dictanova. Citons encore les données issues de l'analyse des cultures agricoles récoltées par les sondes de Weenat.

Déclaration à la CNIL obligatoire

Pour réussir parfaitement cette utilisation, certaines précautions doivent être prises et en tout premier lieu, lorsque votre base de données contient des données personnelles, il est absolument nécessaire de procéder au préalable aux déclarations CNIL (simplifiées, normales voire demande d'autorisation). Outre les potentielles sanctions administratives et pénales, un fichier non déclaré est considéré comme illicite et ne peut donc être ni vendu ni loué. Les juges ont clairement déclaré qu'**un tel fichier non déclaré constituait un objet illicite, hors commerce, insusceptible d'être vendu** (Com. 25 juin 2013). Rappelons également que l'introduction dans un fichier d'une donnée personnelle nécessite le consentement éclairé et préalable de la personne concernée.
Mais, la Data, c'est également une multitude d'informations qui n'ont aucun rapport avec les données personnelles. On peut les appeler « données objectives » ou « données brutes ». Or, au cœur de votre entreprise, il y a aussi de telles informations qui sont certes, plus ou moins organisées. Sachez qu'une fois optimisée en base de données, la data est une véritable mine d'or.

Droit d'auteur ou droit du producteur ?

En organisant vos données, vous valorisez à la fois le contenu (la data) et le contenant (la ou les bases de données). La base de données peut être protégée par le droit d'auteur si le choix ou la disposition des matières constitue une création intellectuelle originale c'est-à-dire lorsque son auteur ou son concepteur fournit un effort personnalisé, éloigné de toute logique automatique et contraignante (cf. article L112-3 du Code de la propriété intellectuelle).
La base de données peut également être protégée via la reconnaissance de la qualité de **producteur de bases de données**. Ici, il s'agit de démontrer en particulier le risque des investissements sur la base de données lors de sa constitution, sa vérification ou sa présentation : investissement financier, matériel ou humain substantiel relevant des moyens consacrés à la recherche de données existantes, à leur rassemblement et le suivi de la base (cf. article L341-1 du Code précité).
Par conséquent, droit d'auteur ou droit du producteur de base de données, vous pouvez être titulaire d'un véritable droit de propriété sur vos données via l'existence de véritables bases de données.
A ce titre, vous pouvez vous en **réserver l'exclusivité** et délivrer à vos clients des prestations de service ou des licences d'utilisation, issues de l'exploitation des données. La seule réserve dégagée par les juges est l'abus de position dominante de telle manière qu'un monopole sur certaines données ne doit pas être préjudiciable aux autres acteurs économiques (Com. 4 décembre 2001 – France Télécom et son fichier d'abonnés).
Sans l'organisation de la data au sein de bases de données, votre data est de libre parcours. Elle relève du bien commun. Titulaire d'un droit de propriété intellectuelle, vous pouvez interdire certaines formes d'extraction et d'utilisation du contenu de votre base et donc de votre data. Dans ces conditions, invoquer un acte de contrefaçon est plus aisé que de démontrer un acte de concurrence déloyale ou de parasitisme.
Parce qu'une fois organisées, les données de votre entreprise ont de la valeur, il faut cultiver votre data, sans trop dénaturer la maxime de Voltaire « Il faut cultiver notre jardin » !

Réagissez à cet article

Source : *Startup : Comment bien protéger sa data, ce précieux patrimoine immatériel ? – Maddyness*

Par Marie-Pierre L'hopitalier, avocat associé.

Crédit photo : Shutterstock

Une nouvelle norme Wi-Fi destinée aux objets connectés

Une nouvelle norme Wi-Fi destinée aux objets connectés

La Wi-Fi Alliance a présenté un nouveau standard baptisé Wifi Halow (ou IEEE 802.11ah pour les intimes.) Celui-ci est spécialement pensé pour le marché des objets connectés et promet une consommation énergétique moindre ainsi qu'une meilleure portée.

La Wi-Fi Alliance n'entend pas rester sur la touche sur le marché des objets connectés : l'organisme, qui rassemble les principaux acteurs et industriels spécialisés ayant recours aux technologies Wi-Fi, a annoncé l'arrivée d'un nouveau standard baptisé Halow. Celui-ci misera principalement sur deux aspects pour s'imposer sur les objets connectés : d'une part, la Wi-Fi Alliance met en avant une consommation énergétique réduite pour les machines ayant recours à Halow,. Basé sur la norme IEEE 802.11ah, Halow est encore en attente de validation.

Halow, it's me

Ce protocole fonctionne sur la bande de fréquence 900 Mhz et promet une portée maximale doublée par rapport aux protocoles actuellement utilisés. A titre de comparaison, la portée de la norme 802.11ac, déployée en 2011, est évaluée à environ 35m. Le Wi-Fi Halow promet également une meilleure robustesse du signal, afin d'assurer une meilleure connectivité au sein des environnements urbains ou domestiques. En revanche, celui-ci offrira un débit moindre, ce qui n'est pas forcement un défaut dans le secteur des objets connectés, qui cherchent plutôt à transmettre de petites quantités de données à intervalles fréquents.

Celui-ci sera également compatible avec les principaux protocoles Wi-Fi actuellement utilisés par les différents constructeurs et sera évidemment conçu pour prendre en charge nativement les connexions IP. Un processus de certification des objets exploitant ce nouveau protocole sera lancé d'ici 2018, mais les premiers produits ayant recours à Halow devraient être disponibles dès 2016.

Le marché des objets connectés reste pour l'instant chaotique, mais de nombreux compétiteurs tentent de mettre en avant leurs propres protocoles afin de prendre les devants sur la concurrence. L'objectif est de devenir un standard dans un secteur qui, plus que beaucoup d'autres, à un grave besoin d'interopérabilité. On a ainsi vu Sigfox présenter sa propre technologie, rapidement suivi par LoRa tandis qu'Archos ou d'autres développent eux aussi leurs propres alternatives.

Réagissez à cet article

Source : *Wi-Fi Halow : Une nouvelle norme destinée aux objets connectés*

Un malware soupçonné d’être à l’origine d’une coupure de courant en Ukraine

Un malware soupçonné d’être à l’origine d’une coupure de courant en Ukraine

Le 23 décembre, les habitants de la ville ukrainienne d'Ivano-Frankivsk ont subi une importante panne de courant. Celle-ci a été provoquée par une défaillance provenant de la centrale électrique régionale et a affecté plusieurs milliers de foyers de la région. Mais cette soudaine panne n'était pas un accident : en effet, la société chargée de l'exploitation de la centrale a précisé que celle-ci avait été causée par des « interférences » sur leurs systèmes.

Mais pour plusieurs médias locaux, la piste d'une cyberattaque visant les infrastructures énergétiques du pays est à privilégier. La société de cybersécurité ESET a d'ailleurs publié plusieurs informations en ce sens : la société explique avoir récupéré des samples de malware ayant affecté plusieurs centrales ukrainiennes, et explique que ceux-ci ont pu être utilisés dans le cadre d'une cyberattaque à l'encontre des équipements ukrainiens.

Des nouvelles du cyberfront

ESET se dit en mesure d'affirmer que plusieurs entreprises Ukrainiennes du secteur de l'énergie sont victimes de cyberattaques. Les attaquants ont notamment recours à une famille de malware baptisées BlackEnergy, dont les traces ont été détectées à plusieurs reprises en 2015 dans des entreprises ukrainiennes liées au secteur de l'énergie.
BlackEnergy est un malware connu, qui a déjà été repéré plusieurs fois par le passé. Celui-ci se présente sous la forme d'un malware modulaire : une fois la cible infectée, les attaquants peuvent exploiter la porte dérobée ainsi créée afin de télécharger des modules différents permettant au malware d'accomplir diverses actions sur la machine cible.
Parmi les modules identifiés de ce malware, l'un d'entre eux permet notamment de s'attaquer aux systèmes SCADA, des postes utilisés pour le contrôle et la surveillance des installations industrielles. BlackEnergy permet également le téléchargement d'un autre malware, baptisé cette fois killdisk, et dont l'objectif est la destruction de données. Un arsenal qui laisse ESET penser que ces outils ont pu être mis en œuvre dans l'attaque dont semble avoir été victime la centrale électrique d'Ivano-Franivsk.
Les services de sécurité ukrainiens accusent la Russie d'être à l'origine de l'attaque selon Reuters, mais ces derniers n'ont émis aucun commentaire venant confirmer ou infirmer cette théorie. Une enquête a été ouverte par les autorités nationales pour déterminer les circonstances exactes de cette coupure de courant.

Réagissez à cet article

Source : *Ukraine : un malware soupconné d'être à l'origine d'une coupure de courant*

Les 5 dangers pour vos ordinateurs, smartphones et données en 2016

Les 5 dangers pour vos ordinateurs, smartphones et données en 2016

Les 5 tendances qui motiveront leurs actions envers votre ordinateur, votre smartphone, vos données…

Ecartelée entre la démocratisation de l'Internet des objets (thermostat intelligent, balance connectée…), la prise de pouvoir du stockage dans le « cloud » et l'émergence des nouveaux smartphones vedettes, la sphère des nouvelles technologies subira en 2016 les assauts des virus virulents, des arnaques en ligne, des cybercriminels.
Comme un caméléon virtuel, la cybercriminalité s'adaptera plus que jamais à l'air du temps pour exploiter les nouveaux territoires en friche.
Entre prudence et clairvoyance, voici les 5 tendances cybercriminelles qui se développeront ces 12 prochains mois, selon les experts de l'éditeur de solution de sécurité BullGuard.

1. La montée en puissance du « ransomware »
Impitoyable méthode d'extorsion, le « ransomware » bloque votre ordinateur, crypte vos fichiers personnels et vous réclame un paiement en ligne pour les libérer.
La menace brandie en cas de refus de payer la rançon : l'extermination de vos données (photos, vidéos, documents…).
Alors que les virus à l'ancienne et les chevaux de Troie accusent une certaine perte de vitesse, le « ransomware » est appelé à les dribbler.
Ces logiciels malveillants s'attrapent en visitant un site préalablement « hacké » (piraté) ou un obscur site volontairement malveillant, en téléchargeant des fichiers vérolés, notamment sur les plateformes d'échange de fichiers illégaux…

2. Le smartphone, cette cible indiscrète
Connecté à Internet 7 jours sur 7, 24 heures sur 24 dans le scénario le plus extrême, le smartphone concentre une myriade de données personnelles, des adresses email de vos contacts au numéro de votre carte de crédit.
Le téléphone est par conséquent une cible de choix pour les cybercriminels, qui rivalisent d'ingéniosité pour contourner les nouvelles barrières de sécurité régulièrement déployées par Apple pour ses iPhone et Google pour son système d'exploitation mobile Google Play.
Après avoir concentré leurs efforts sur la Chine et l'Extrême-Orient, les cybercriminels devraient viser tout particulièrement l'Europe en 2016.
Certes, nos smartphones étaient déjà menacés par le virus et les logiciels malveillants. Hélas, le niveau d'alerte devrait grimper de quelques degrés.

3. L'Eldorado inquiétant de l'Internet des objets
Nouvelle marotte des constructeurs, l'Internet des objets entend envahir notre quotidien pour évaluer et prédire nos besoins, mesurer notre activité, adapter l'éclairage et le chauffage de notre habitation en fonction de nos usages…
Qu'il s'agisse d'un pèse-personne connecté ou d'un thermostat intelligent, ces appareils vulnérables de par leur connexion constante à Internet récoltent au kilo les données personnelles.
Imaginons le cas d'une caméra de sécurité connectée. Elle pourrait simplement être détournée par un cybercriminel pour détecter les moments où vous quittez votre maison.
Toujours en quête d'un standard, notamment pour la sécurité, la galaxie de l'Internet des objets, tout juste née de son Big Bang historique, ne manquera pas de révéler en 2016 ses failles et ses vulnérabilités.

4. Des nuages dans le ciel du « cloud »
Inexorable lame de fond qui modifiera à jamais le monde du stockage, le « cloud » éparpille données et fichiers dans un nuage de serveurs (ordinateurs) répartis dans d'immenses « data center » aux quatre coins du monde.
Ces « fermes » informatiques dédiées au stockage et au traitement des données présentent un double intérêt pour les cybercriminels.
Leur puissance peut être détournée à d'autres fins, tandis que les données stockées constituent un sérieux trésor de guerre au cœur duquel il est tentant de piocher.
Objet de toutes les attentions des esprits mal intentionnés, la vulnérabilité du « cloud » risque d'être régulièrement soulignée ces prochains mois.

5. Les gangs sous les projecteurs
Les cybercriminels se structurent en gangs d'une efficacité redoutable, souligne BullGuard.
« Ils passent des semaines, voire des mois, à effectuer des missions de reconnaissance avant d'attaquer des organisations », témoignent les experts de l'éditeur. « Ces entreprises ont été conçues dès le départ pour se spécialiser dans les crimes informatiques et ont des hiérarchies cloisonnées qui incorporent des programmeurs spécialisés dans le piratage, de vendeurs de données et des gestionnaires, tous supervisés par un cadre supérieur. Ces équipes de cybercriminels occuperont le devant de la scène en 2016. »

Réagissez à cet article

Source : *Virus, arnaques en ligne, cybercriminalité : les 5 dangers de l'année 2016 – L'Avenir Mobile*

Google corrige 5 failles critiques d’Android

Google corrige 5 failles critiques d’Android

Pratiquement tous les terminaux tournant sous une version récente d'Android sont affectés par au moins une des cinq failles critiques corrigées par Google dans l'OS mobile.

Google a remédié à une douzaine de vulnérabilités d'Android, dont cinq sont qualifiées de « critiques ».
Parmi les failles critiques identifiées et corrigées dans cette nouvelle série de correctifs, la firme de Mountain View signale qu'une des vulnérabilités pourrait permettre à un attaquant d'exécuter du code distant – comme un malware – en exploitant la manière dont Android traite certains fichiers médias.

Nexus, puis smartphones Samsung, LG et BlackBerry

Google précise par ailleurs qu'Android 5.0 et les versions ultérieures – dont « Marshmallow » 6.0 – sont affectées par ces différentes vulnérabilités.
Et si la nature de ces failles vous évoque quelque chose, ce n'est pas une coïncidence. Mois après mois, le service « mediaserver » reste le composant le plus problématique d'Android. Au point que Google a copié-collé le même message dans ses bulletins de sécurité à chaque fois que le composant a été affecté.
La vulnérabilité critique porte sur une partie centrale du logiciel Android et qui dispose de permissions auxquelles les applications tierces n'ont normalement pas accès. D'autres failles se situent elles dans la gestion du Bluetooth et du Wi-Fi, ou encore au niveau du kernel.
Les terminaux Nexus sont les premiers appareils Android à recevoir les correctifs de sécurité. D'autres fabricants, parmi lesquels Samsung, LG et BlackBerry, déploieront des mises à jour dans les prochains jours.

Réagissez à cet article

Source : *Google corrige 5 failles critiques d'Android*

2/3 des Français ont peur de l’intelligence des machines

2/3 des Français ont peur de l’intelligence des machines

Une étude réalisée par l'Ifop révèle qu'une grande majorité des Français appréhendent la montée en puissance de l'intelligence artificielle liée au Big Data. Une crainte paradoxale et un peu irrationnelle.

L'intelligence artificielle est-elle un danger pour l'humanité? De grands noms du monde scientifique ou de la high-tech semblent craindre en tout cas l'émergence d'une intelligence autonome des machines. Comme Elon Musk, le fondateur de Tesla, qui incitait en 2014 des étudiants à la prudence. « L'intelligence artificielle est plus dangereuse que le nucléaire », affirmait-il ainsi lors d'un **symposium**. Une crainte partagée par Bill Gates ou encore Stephen Hawking. Le grand physicien britannique affirmait même il y a un an à la BBC que « le développement d'une pleine intelligence artificielle pourrait signifier la fin de la race humaine. » Rien que ça.

Et les messages de ces personnalités semblent porter auprès de la population française. Selon une étude réalisée par l'Ifop pour l'Observatoire B2V des Mémoires, près des 2/3 de nos concitoyens (65%) seraient inquiets de la montée en puissance des machines autonomes. Les romans et films d'anticipation comme Terminator qui dépeignent un monde dominé par les machines intelligentes n'y sont sans doute pas pour rien.

L'intelligence c'est bien, à condition de garder le contrôle

Pourtant, et c'est paradoxal, les Français sont plutôt confiants quant à l'essor du Big Data qui serait à l'origine du développement de l'intelligence artificielle (I.A.) des machines. Ainsi, 69% d'entre eux pensent cette I.A. va croître avec le développement exponentiel de la production de données (Big Data). Et surtout que ce Big Data présente des avantages à court terme pour la santé et le bien-être (meilleure prévention des maladies, découvertes scientifiques…). 67% des Français sont plutôt enthousiastes quant aux promesses du Big Data.

« Pour les personnes sondées, le Big Data présente des avantages: il est considéré comme un facteur de progrès, notamment pour la recherche scientifique, la prévention et le traitement des maladies, analyse Francis Eustache, neuropsychologue et président du Conseil scientifique de l'Observatoire B2V des Mémoires. En même temps, l'intelligence artificielle inquiète, en particulier avec l'autonomie croissante des machines. » En d'autres termes, l'intelligence des machines c'est bien, mais à condition de ne pas les laisser agir seules, de garder le contrôle.

Des peurs un peu irrationnelles

Car derrière cette crainte de l'intelligence artificielle, il y a en fait deux peurs bien distinctes. Celle de machines trop intelligentes dotées d'une conscience, qui décideraient de se passer de l'humanité. Scénario très peu crédible à en croire de nombreux scientifiques comme le chercheur Jean-Gabriel Ganascia, spécialiste de ces questions. Une autre peur, plus crédible celle-là, est liée à **l'autonomie croissante de machines** (automobiles, drones, logiciels de trading…) trop peu fiables. Mais là aussi, les craintes sont sans doute exagérées tant les pouvoirs publics encadrent de plus en plus ce type de technologies.

Réagissez à cet article

Source : *2/3 des Français ont peur de l’intelligence des machines*