2020 : 1% des objets connectés seront des…voitures

2020 : 1% des objets connectés seront des…voitures

Les équipements sans fil s'immiscent dans les véhicules. En 2020, 250 millions de voitures seront connectées au réseau avertit le Gartner. Un véritable écosystème est en train de se créer sur ce mouvement.

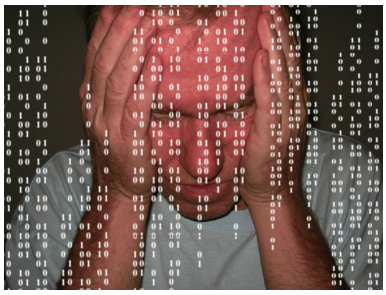
En 2020, 250 millions de voitures connectées parcourront les routes du monde avertit le Gartner. Dans les 5 années qui viennent, les nouveaux véhicules équipés de capacités de conduite automatique vont devenir un segment majeur de l'Internet des objets, assure le cabinet d'étude.
Cette année, le Gartner prévoit unparc de 4,9 milliards d'objets connectés, en croissance de 30% par rapport à 2014. En 2020, il devrait y avoir 25 milliards d'objets connectés. Les voitures connectées devraient donc représenter 1% des objets connectés dans 5 ans.

Un levier de croissance économique
« La voiture connectée est déjà une réalité, et la connectivité sans fil dans les véhicules est en expansion rapide, des modèles de luxe et des marques haut de gamme, au modèles de milieu de gamme » explique James F. Hines, du Gartner. L'Idate confirmait déjà cette tendance en juin dernier.
Par ailleurs, la prolifération de la connectivité automobile doit avoir des implications majeures sur des secteurs tels que la télématique, la conduite automatique, ou encore la mobilité, assure le Gartner.

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

Source : http://www.zdnet.fr/actualites/2020-1-des-objets-connectes-seront-desvoitures-39813698.htm

Le cybervandalisme envahit internet

	**Le cybervandalisme envahit internet**

Après le piratage du site de Sony Pictures et les cyberattaques de nombreux sites internet français, le piratage est de plus en plus présent sur internet. Depuis ces événements, on entend de plus en plus parler de « cyberguerre » ou de « cybervandalisme », mais qu'en est-il vraiment ? Voici quelques réponses.

Le « cybervandalisme » plutôt qu'une « cyberguerre »

Les Etats-Unis contre la Corée du Nord, les Anonymous contre l'Etat Islamique, on pourrait assimiler le piratage informatique à une sorte de guerre virtuelle tant les conséquences sont importantes. Le piratage de Sony Pictures a d'ailleurs pris une tournure politique : Barack Obama a pris officiellement la parole sur ce sujet et a préféré associer ce phénomène à du « cybervandalisme » et non à un acte de guerre. Le hacking de Sony Pictures a été conséquent puisqu'il a retardé la diffusion du film The Interview, une comédie à propos d'un complot fictif de la CIA pour assassiner le leader de la Corée du Nord Kim Jong-Un. De nombreuses informations privées ont également été dérobées.

La lutte contre les cyberattaques ne fait que commencer, mais des moyens sont mis en place pour éviter le piratage de nombreux sites internet ou comptes Facebook. Ce concept recoupe la réflexion sur la guerre économique et la stratégie d'intelligence économique, qui accordent, entre autres, une place prépondérante à la cybersécurité et transformation numérique. L'essentiel pour dominer aujourd'hui serait de posséder l'information, avant de posséder des territoires ; et le web est une mine d'or pour partir à la recherche de données confidentielles et capitales, que ce soit en politique ou pour le lancement d'un nouveau produit.

Comment se prémunir contre les cyberattaques ?

Au travers des entreprises attaquées, c'est tout un chacun qui peut être touché. En effet, le nombre de fraudes à la carte bancaire lors d'un achat sur internet a fortement augmenté ces dernières années. Les entreprises possédant des sites internet ou boutiques en ligne doivent les sécuriser au maximum afin d'éviter toute cyberattaque. Elles stockent et protègent les données personnelles des clients pour que les hackers ne puissent y accéder. Les pirates informatiques tentent en effet de dérober les codes bancaires des internautes par l'intermédiaire de cyberattaques.

Lorsque les internautes se retrouvent sur une boutique en ligne pour acheter un billet d'avion, une voiture ou des vêtements, ils doivent avoir la possibilité de payer en toute sécurité. Si ce n'est malheureusement pas toujours suffisant, plusieurs moyens de payement alternatifs ont été développés et sont mis à la disposition de tout acheteur, afin d'éviter de dévoiler les données personnelles de leurs cartes bancaires.

Plusieurs sites comme Paysafecard.com proposent des cartes prépayées pour faciliter les paiements en ligne. Il suffit de se créer un compte pour obtenir une carte de crédit prépayée qui se recharge à tout moment. Vous pouvez mettre le montant que vous désirez et payer en ligne sur des sites partenaires. Le système 3D Secure est également un bon moyen d'éviter tout piratage lors d'un paiement en ligne. Il vous permet même d'effectuer des achats rapidement sur la toile. Ces systèmes sont donc recommandés pour pallier les attaques des hackers à petite échelle.

Le meilleur moyen également de prévenir tout piratage est de choisir avec soin son mot de passe.

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

Source : http://www.archimag.com/vie-numerique/2015/01/29/fleau-cybercriminalite-comment-se-premunir

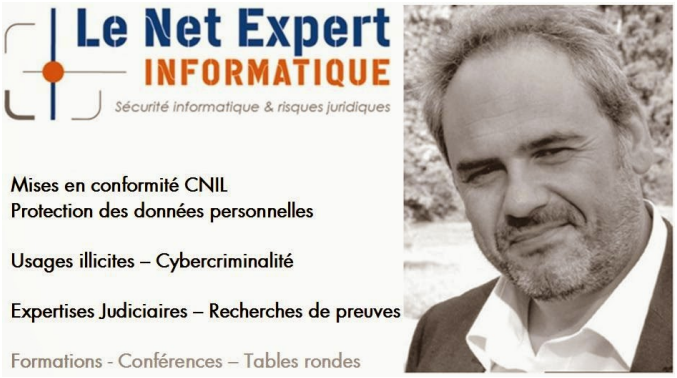
Prévenir les cyber-attaques avec Denis JACOPINI – Conférence le 10 février

	Prévenir les cyber-attaques avec Denis JACOPINI – Conférence le 10 février

La plateforme Initiative Cavare et Sorgues (ICS) accueille dans ses rangs un nouvel expert Denis JACOPINI, diplômé en droit de l'Expertise Judiciaire et en Cybercriminalité, pour sensibiliser les entreprises sur ce sujet d'actualité.

Les attaques informatiques ont toujours existé mais aujourd'hui elles sont très nombreuses.
En effet, que l'on soit une institution, une collectivité, un particulier ou une entreprise nous sommes tous des proies potentielles.
Que cela soit par méconnaissance des risques, sous-estimation des conséquences, ou bien par pure négligence, les faits sont là et nous sommes tous concernés. Piratage de serveurs, vol de données, arnaques financières en tout genre utilisant Internet… Le cyber-crime a couté plus de 327 milliards d'euros dans le monde en 2013.
Plus de 25 000 sites internet récemment défacés. Pourtant, il est possible d'enrayer ce phénomène qui semble incoercible.
Avec un peu de sensibilisation, beaucoup de bon sens et une information bien choisie, les chefs d'entreprises peuvent facilement reconsidérer l'importance de la sécurité numérique dans leurs priorités et ainsi rapidement repousser les principaux vandales du numérique.

« Nous accompagnons et finançons essentiellement des entreprises de moins de 10 salariés sur le territoire des 2 intercommunalités de l'Isle sur la Sorgue et de Cavaillon, quasiment toutes communique par l'intermédiaire entre autre d'un site internet, il nous a semblé important de les sensibiliser car il est possible d'enrayer ce phénomène » précise la directrice Anne-Laure STRETTI BOUSCARLE.
« Nous sommes très heureux que Denis JACOPINI viennent élargir les rangs des professionnels experts qui interviennent chez nous au même titre que les experts comptables, notaires, avocats, assureurs…et qu'il mette au service du plus grand nombre ses compétences pour les aider à lutter contre ces cyber-attaques».



Denis JACOPINI – Le Net Expert Informatique

Cet ancien chef d'entreprise Cavaillonnais d'une entreprise d'informatique, il a choisi après 17ans d'activité de se tourner vers son domaine de prédilection : l'expertise en sécurité informatique et en protection des données personnelles.
Diplômé en droit de l'Expertise Judiciaire et en Cybercriminalité il est à ce titre assermenté auprès des Tribunaux et spécialiste en sécurité informatique, en protection des données personnelles et en Informatique légale.
Il intervient auprès du Master II en Commerce électronique à l'Université d'Avignon, à l'Ecole de Formation des Avocats Centre Sud (EFACS), au CNFPT (Centre National de la Fonction Publique Territoriale) et est Formateur auprès de nombreux organismes dont des Centres de Gestion Agréés.
www.lenetexpert.fr

1ère session de sensibilisation le 10 février 2015 à 18 h30 dans les locaux d'ICS
Conférence débat au cours de laquelle seront évoquées les différentes techniques notamment celles qui consistent à détourner un site internet.
Inscription au préalable auprès de la plateforme
Pour vous inscrire :
Initiative Cavare et Sorgues
111 boulevard Paul Doumer 84300 CAVAILLON
Tel : 04 90 78 19 61

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

Source : Anne-Laure STRETTI BOUSCARLE

« La cyber-assurance devient une priorité pour les dirigeants d’entreprise »

	« La cyber-assurance devient une priorité pour les dirigeants d’entreprise »

Face à la recrudescence de la cybercriminalité, les dirigeants de PME et ETI s'interrogent de plus en plus sur ces nouveaux risques et la façon de s'en protéger. Le point avec Philippe Gaillard, directeur des Risques Techniques chez Axa Entreprises.

Qu'est-ce-que le cyber-risque aujourd'hui ? Comment -a-t-il évolué ces dix dernières années ?
Le cyber-risque prend de plus de plus de place dans notre quotidien. Pourtant les cyber- attaques et virus au sens large ne sont pas vraiment nouveaux. Jusqu'aux années 2000, les cyber-attaques étaient principalement des virus ou des vers informatiques qui étaient le résultat d'une sorte de compétition entre jeunes prodiges de l'informatique qui tentaient de pénétrer des systèmes prestigieux connus pour être inviolables. Autour des années 2005, les cyber-attaques ont évolué et se sont dirigées vers les Etats et les défenses nationales. Depuis 2010, on observe une recrudescence de ces attaques. Elles sont de plus en plus complexes, et prennent des formes de plus en plus variées. On commence à voir de l'espionnage industriel, des attaques entre concurrents, de l'extorsion et de la fraude. C'est toute cette évolution qui fait que les entreprises, quelle que soit leur taille, sont victimes de plus en plus de cyber-attaques. En cinq ans, la cybercriminalité s'est accélérée en nombre, et transformée en complexité et en variété d'objectifs.

Quels sont les cyber-attaques le plus souvent répertoriées ?
Il existe trois grandes catégories de cyber-attaques.
Le sabotage, qui peut soit être une vengeance envers un tiers, soit une compétition entre sociétés mal intentionnées à l'instar de ce qui pouvait donner lieu autrefois à un incendie volontaire de la part d'un mauvais concurrent.
Seconde catégorie, l'espionnage, qui consiste à aller chercher de l'information dans les autres entreprises, que ce soit de l'information commerciale ou technologique. Dans ce cas, ce sont les directions générales et les équipe de R&D qui sont les plus ciblées.
Troisième catégorie : la criminalité ou la piraterie qui consistent à voler des données ou à paralyser un système en espérant avoir une rançon en échange. Il est important de savoir que ces cyber-attaques agissent dans la durée. D'abord, elles se préparent longtemps à l'avance, car lorsqu'il s'agit d'espionnage par exemple, les criminels doivent commencer par chercher à comprendre la culture et les points sensibles de l'entreprise qu'ils visent. A la suite de cela, ils injectent un logiciel malveillant dans le système informatique de l'entreprise et le font évoluer pour se rapprocher progressivement de la cible finale. Entre le moment où se font les premières intrusions dans l'entreprise et le moment où est découverte cette action malveillante, il se passe bien souvent un an, voire plus.

Pouvez-vous nous donner un exemple type de cyber-attaque ?
Aujourd'hui, la plupart des comités de direction des grandes entreprises sont sur le réseau Linkedin. La technique utilisée par un cybercriminel pour pénétrer dans le système de l'entreprise est assez simple. Il repère des personnes qui travaillent sur un sujet sur lequel il y a eu un séminaire par exemple ; il envoie un mail piégé aux personnes susceptibles d'avoir été présentes à ce séminaire en leur faisant croire qu'il y participait également. Dans ce mail, il y a une pièce jointe qui annonce par exemple un compte rendu du séminaire. De fait, parmi les personnes réceptionnaires de cet email, il y a en a qui ont réellement participé à ce séminaire. Pour ceux et celles qui ouvrent la pièce jointe, le virus pénètre aussitôt dans leur système informatique. Le mal est fait. Le virus paralyse ensuite l'ordinateur de la personne qui aura ouvert la pièce jointe ; ladite personne appelle alors son help desk, qui bien souvent intervient à distance sur les ordinateurs. Pour prendre la main, l'expert informatique en charge de réparer l'ordinateur saisit le mot de passe administrateur. Il est aussitôt enregistré par le virus qui peut ensuite, tout doucement, progresser dans le système informatique de l'entreprise ciblée jusqu'à parvenir par exemple au serveur de la direction générale ou celui de la R&D.

Comment réagissent les dirigeants de PME-PMI face à la cybercriminalité ?
Il y a encore deux ans, les dirigeants de PME-PMI ne s'inquiétaient pas vraiment des cyber-attaques. Mais depuis douze mois, face aux dernières attaques médiatiques qu'ont pu connaître de grands groupes, l'inquiétude est en train de monter fortement. Selon notre dernier baromètre de juin 2014, sur 500 chefs d'entreprises interviewés, 46% placent le cyber-risque parmi leurs préoccupations majeures. Ce qui était un quasi non sujet il y a encore un an tend à devenir une priorité. D'autant plus que les PME et ETI sont mal protégées et donc deviennent des cibles très vulnérables. Par ailleurs, elles peuvent être des sous-traitants de grosses entreprises et par conséquent être une porte d'entrée pour les cybercriminels qui visent ces grands groupes.

Comment les entreprises peuvent-elle se protéger des cyber-attaques ?
Une bonne protection doit être équilibrée et reposer sur trois piliers. Le premier, c'est bien évidemment la technologie pour empêcher les virus de pénétrer les systèmes informatiques, pour les détecter et les traiter. Cela est nécessaire mais totalement insuffisant ! Le second, c'est l'information et la formation des salariés. Il est primordial de sensibiliser les collaborateurs aux bonnes pratiques afin d'éviter les comportements qui mettent l'entreprise en danger. En troisième lieu, il faut travailler sur la résilience de l'entreprise pour limiter les effets d'une possible attaque notamment en anticipant les capacités de rebond et de continuité d'activité. Les entreprises doivent admettre que, quoi qu'elles fassent, elles peuvent être attaquées. A l'instar d'une porte blindée, si un voleur veut pénétrer dans les lieux, et qu'il peut y mettre les moyens, il finira bien par entrer. Donc, partant du principe que toute entreprise sera attaquée à un moment ou un autre, il est important de proposer des solutions qui aident l'entreprise à limiter les dégâts et redémarrer au plus vite.

Existe-t-il des assurances qui protègent les entreprises de la cybercriminalité ?
Axa Entreprises est l'assureur d'une PME sur trois en France ; nous mettons un point d'honneur à les accompagner pour répondre à leurs besoins. Face aux cyber-risques, nous avons conclu un partenariat avec le département cyber sécurité du Groupe Airbus, qui est la référence dans le domaine.
Pour les ETI et les grandes entreprises, nous proposons de réaliser un audit de risques, mené par un ingénieur d'Axa et un ingénieur d'Airbus qui interviennent en binôme. Cet audit donne lieu à un diagnostique complet de la situation de l'entreprise face aux cyber-risques. Sur cette base, en fonction des situations, nous pouvons proposer une solution d'assurance qui combine deux volets complètement imbriqués : un contrat d'assurance qui couvre toutes les conséquences des cyber-attaques ainsi qu'un accompagnement dans le temps en ingénierie pour aider l'entreprise à maitriser son risque cyber et à l'améliorer.
Pour les PME, nous avons élaboré une approche simplifiée. Aussi bâtie en collaboration avec l'expertise du groupe Airbus, cette approche repose sur un questionnaire très simple, accessible à tous. A partir des réponses à ce questionnaire, nous pouvons réaliser une mesure du risque cyber et ainsi proposer une offre d'assurance avec des garanties et un tarif adaptés. Sur cette même base un diagnostic cyber est remis au client d'AXA Entreprises pour l'accompagner dans ses actions de prévention contre les risques cyber. Les PME ayant rarement les contacts nécessaires, se trouvent bien souvent démunies quand survient un sinistre cyber. Par conséquent, au-delà des garanties de dommage, de responsabilité civile, de protection des données personnelles et d'accompagnement à la gestion de crise, la valeur de l'offre d'assurance réside beaucoup dans sa capacité à proposer un accompagnement global de proximité de l'entreprise, en amont et en aval, avec des services pragmatiques, rassurants et réactifs.

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

Source :
http://www.latribune.fr/loisirs/la-tribune-now/20150128tribd355efe7a/la-cyber-assurance-devient-une-priorite-pour-les-dirigeants-d-entreprise.html

Denis JACOPINI Intervient au Salon du numérique 2015 le 3 février et coanime une conférence avec Orange

	Denis JACOPINI Intervient au Salon du numérique 2015 le 3 février et coanime une conférence avec Orange

10h00 – 10h45 – Cybercriminalité, protection des données personnelles et Réputation
Imaginez un instant que vous soyez consommateur. Vous découvrez soudain que vos données (coordonnées personnelles, bancaires ou encore médicales) se trouvent diffusées sur le net, sans votre accord, à cause de la négligence d'un professionnel.
Imaginez maintenant que ce professionnel c'est vous, malgré la mise en application imminente du projet de règlement Européen sur la Protection des données personnelles, le risque d'anéantir votre réputation et de vous sanctionner lourdement. Certes, le mal est fait mais pire, les Cybercriminels sauront en profiter !
Venez découvrir, comment ne pas être ce professionnel négligeant en protégeant le patrimoine le plus précieux de votre entreprise : Votre réputation
Présenté par Denis JACOPINI (Le Net Expert) et Eric Wiatrowsi d'Orange

Le 3ème Salon du Numérique en Vaucluse c'est Mardi 3 février 2015 de 9 h à 20 h à la salle polyvalente de Montfavet – Rue Félicien Florent, 84000 Avignon

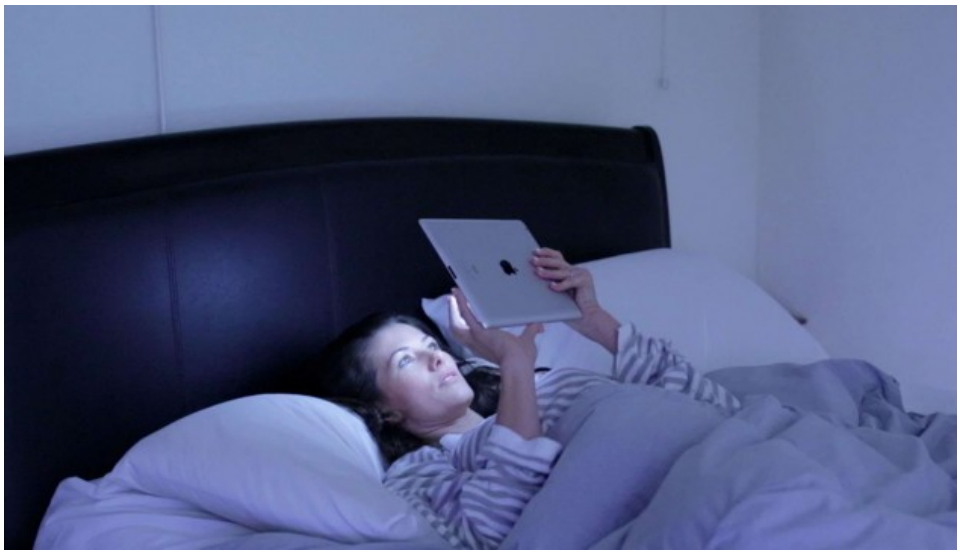
Entrée libre, inscription obligatoire ! 600 m² – 35 stands – 16 conférences – Le rendez vous incontournable du numérique pour votre entreprise.

Entrée gratuite, inscription obligatoire
http://www.salon-du-numerique.fr/reservez-votre-place

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

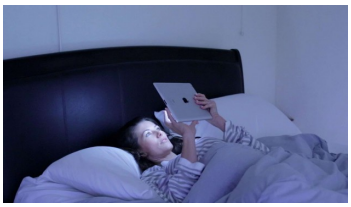
Programme et infos pratiques : http://www.salon-du-numerique.fr/le-programme/

Twitter, Facebook… Peur de manquer quelque chose ? Vous souffrez peut-être de fomo



Twitter, Facebook… Peur de manquer quelque chose ? Vous souffrez peut-être de fomo

Vous parcourez votre fil d'actualités sur les réseaux sociaux et, au fur et à mesure, l'angoisse s'empare de vous. Et si vous loupiez la soirée de l'année ou si vous laissiez passer le message de votre vie ? Cette angoisse s'appelle la fomo, ou la « fear of missing out ». En français : la « peur de louper quelque chose ». Explications de Michael Stora, psychologue clinicien.



Une femme utilise une tablette électronique dans son lit. Image d'illustration (Sprayable Sleep/REX/REX/SIPA)

La **fomo** n'est pas une pathologie officiellement reconnue. L'outil de classification psychiatrique, le DSM 5 (http://fr.wikipedia.org/wiki/DSM-5), ne répertorie pas la « peur de manquer quelque chose » sur les réseaux sociaux, ni, d'ailleurs, l'addiction virtuelle de manière générale.

Le portable devient le prolongement du bras

Pourtant, avec des outils comme Twitter ou Facebook, beaucoup d'internautes vivent dans l'angoisse de louper la soirée de l'année, l'information du siècle ou le message le plus important de leur vie. Avec cette idée, fausse, que les réseaux sociaux permettent d'être à la fois partout et nulle part, les usagers tombent rapidement dans l'angoisse et la peur quand ils se rendent compte que ce n'est pas possible.

La nomophobia, ou peur de se retrouver sans son téléphone portable n'est pas non plus répertoriée dans le DSM 5. Ces pathologies, liées aux outils de communication, sont pourtant bien réelles, même si elles découlent de troubles antérieurs qui ne trouvent pas leur origine dans le virtuel.

Jamais un patient n'est venu me voir pour me parler de sa nomophobia ou de sa fomo. Mais, j'ai constaté des comportements, lors de séances, qui témoignent de l'attachement maladif que certains patients ont envers leur téléphone portable. Comme un prolongement de leur bras, ils ne le quittent jamais.

Il m'est arrivé de devoir expliquer à un patient qu'il ne pouvait pas décrocher son téléphone en pleine séance avec moi. Le problème n'est pas l'outil en lui-même mais ce qu'il représente. Dans ce cas précis, le patient entretenait une relation extrêmement fusionnelle avec sa mère. Couper son téléphone, c'était, pour lui, couper avec sa mère.

Peur de l'abandon et du rejet

Ces pathologies virtuelles bien réelles ne sont pas nouvelles.
Qu'est-ce qui se cache derrière la peur de ne pas être retwitté sur le réseau social ou de ne pas avoir de « like » sur Facebook ? La peur de l'abandon et du rejet.

Ces angoisses sont courantes, surtout à l'adolescence. Il s'agit davantage d'une addiction à l'autre, qu'une addiction à son téléphone portable. Parce que derrière l'outil, se cache autrui. Les sujets qui fétichisent leur téléphone sont dans un rapport narcissique avec l'autre. Un peu comme en amour, ils sont dans une passion et une dépendance. L'objet qu'ils ne veulent pas perdre, n'est pas leur téléphone portable, mais la relation à l'autre.

Le problème des réseaux sociaux, est que l'autre n'existe pas dans une entité et une individualité mais dans une masse, dans laquelle le quantitatif l'emporte. Ce qui compte, ce n'est pas d'avoir un « like » d'un ami, mais plutôt d'en avoir 100 de n'importe qui.

Vers neuf mois, au moment de sa naissance, l'enfant réalise pour la première fois qu'il est « un ». C'est à dire, qu'il existe en dehors de sa mère. La fin de cette relation fusionnelle peut être criblée de traumatismes qui resurgissent sous la forme d'une addiction aux autres.

La fomo est une sorte de Prozac interactif

Dans mon premier livre, il y a dix ans déjà, je compare le téléphone portable à un doudou sans fil. Le but est le même : pallier l'absence de la mère. Ce genre de pathologies existaient aussi avant les réseaux sociaux.

Ainsi, on se retrouvait face à des individus incapables de rester seuls ou inactifs. Le besoin permanent d'être entouré, d'être en contact ou connecté se traduit aujourd'hui par une présence démesurée sur les réseaux sociaux. Je dirais que les premières personnes touchées par la fomo, la peur de louper quelque chose, sont les journalistes.

Avec un journaliste, j'ai réalisé un documentaire pour une chaîne de télévision sur le sujet. Son défi : se passer de son téléphone pendant un mois. Même lui a été surpris de la difficulté de la tâche.

Plus dramatique encore, il y a aujourd'hui des individus qui ne sont pas sortis de chez eux pendant 5 ou 6 ans. Figés derrière leur ordinateur à jouer à des jeux en réseaux, ils se sont coupés du reste du monde. La fomo n'est pas un problème, tant qu'elle n'empêche pas de vivre et d'entretenir des relations, dans le réel. Ce qu'il faut craindre, c'est la rupture des liens sociaux « in real life ». Dans ce cas, il ne faut pas hésiter à consulter.

A l'adolescence, ce genre de refuge est normal. Passé un certain âge, la dimension addictive et la peur panique d'être seule peuvent cacher un terrain dépressif. Etre atteint de fomo, c'est une manière de lutter contre la dépression à coup de Prozac interactif.

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

Source : http://leplus.nouvelobs.com/contribution/1313983-twitter-facebook-peur-de-manquer-quelque-chose-sur-le-web-vous-etes-peut-etre-fomo.html
Par Par Michael Stora, Psychologue clinicien

Sommes-nous invisibles sur les réseaux sociaux anonymes ? Denis JACOPINI répond à une journaliste de l'émission « On n'est plus des pigeons »

sur France 4

Sommes-nous invisibles sur les réseaux sociaux anonymes ? Denis JACOPINI répond à une journaliste de l'émission « On n'est plus des pigeons » sur France 4

Denis JACOPINI interviewé par une journaliste de l'émission « On n'est plus des pigeons » a répondu à la question « Sommes-nous invisibles sur les réseaux sociaux anonymes ? »Secret, Whisper ou Yik Yak… Ces nouveaux réseaux sociaux promettent l'anonymat à leurs utilisateurs. Sauf que rien n'est invisible sur le net.Rumeurs, mots doux, coup de gueule… Publier tout ce qui vous passe par la tête sans dévoiler sa véritable identité, c'est la promesse des réseaux sociaux anonymes comme Whisper.sh, chuchotement en français, Secret.ly, Rumr ou encore Yik Yak, une sorte de Twitter. Conçues essentiellement pour les smartphones, ces plates-formes gratuites incitent leurs membres à se lâcher sans compromettre leur e-réputation. Elles disent garantir des discussions avec des amis ou de parfaits inconnus sans qu'on puisse, dans certains cas, retrouver l'identité de l'émetteur, ou bien, les messages envoyés.

Doit-on féliciter ces applications en matière de protection de la confidentialité de ses utilisateurs ?
Mouais. Avant tout, à donner la possibilité de tout dire sous couvert d'anonymat, ces réseaux se livrent aux dérives de racisme, d'harcèlement et de diffamation. Au niveau technique, quelques incohérences. En octobre dernier, le quotidien britannique The Guardian, sur le point à l'époque de conclure un partenariat média avec Whisper, a eu accès aux coulisses de l'éditeur. Le journal a accusé l'application de collecter des données personnelles et de géolocalisation de ses utilisateurs. D'après The Guardian, Whisper gardait un œil sur les publications et les localisations de ses utilisateurs pour sa collaboration avec les médias. Le but : recouper le contenu des messages pour vérifier si une information était avérée.

Un réseau social qui ne laisse pas de traces, impossible ?
Pour Denis Jacopini, expert judiciaire en informatique, Whisper, comme les autres réseaux sociaux anonymes « se revendiquent dans leur communication comme une forme de réseau social anonyme. Sauf que la souscription n'est pas anonyme. Tous les éléments pour identifier une personne sont là au moment de l'inscription via son smartphone. »
Même si ce type d'applications ne donne pas directement accès à l'identité d'une personne, l'adresse IP du terminal utilisé pour la connexion Internet permet de récolter les informations du téléphone.
Pourtant, la garantie de l'impossibilité de « tracer » les utilisateurs a été mise en avant notamment par le réseau Whisper. Sur Twitter, son éditeur Neetzan Zimmerman garantissait mi-octobre 2014 qu'il est techniquement impossible de déterminer la localisation des utilisateurs qui n'activaient pas leur localisation GPS. Pour l'expert en informatique Denis Jacopini, « désactiver la localisation GPS est inutile » pour éviter tout traçage. En effet, l'adresse IP du téléphone permet de remonter au fournisseur d'accès à Internet puis de déterminer la localisation de l'utilisateur.
Des informations que les fournisseurs peuvent communiquer aux autorités sur demande. D'autant que le droit applicable en matière de protection des données est celui du pays du propriétaire des plates-formes, souvent américaines. « L'anonymat n'est pas garanti vis-à-vis des autorités, c'est bien pour les copains », conclut Denis Jacopini. Et encore. Alors, pour vider son sac en public sans problème, parlez-en à une proche. Tout s'arrange avec l'écoute et la parole.
Marie Dagman

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

Source :
http://www.france4.fr/emissions/on-n-est-plus-des-pigeons/enquete/sommes-nous-invisibles-sur-les-reseaux-sociaux-anonymes_294315
Par Marie Dagman

La CNDP va-t-elle finir par

prendre le taureau par les cornes ?

	La CNDP va-t-elle finir par prendre le taureau par les cornes ?

Au Maroc, la loi 09-08 sur la protection des données à caractère personnel sur Internet enregistre encore des carences dans son application. En effet, tout le monde s'accorde à dire qu'il y a matière à faire et des lacunes sont encore à combler. Ce constat a été corroboré dans le dernier rapport de la Commission nationale de contrôle de la protection des données personnelles (CNDP).

Pour rappel, il y a quelques mois, cette dernière a commandité une opération de contrôle qui a concerné environ 104 sites web. Figuraient parmi les catégories de sites, ceux d'annonces, de voyage et d'hôtellerie, de cabinets de recrutement et d'emploi, de vente en ligne, de deals, de marketing, ainsi que des sites d'organismes publics, de banques, de transport et logistique, de santé, de télécoms et de location de voitures.
A travers cette campagne, il a ainsi été démontré que seulement 22% des sites web au Maroc affichent une mention relative à la protection des données personnelles conformément aux exigences de la loi.
C'est, en effet, grâce à cette campagne de contrôle qu'il a été également possible de constater que dans 28% des cas, la mention est présente, mais incomplète. Dans ce sens, la CNDP a précisé que 50% des sites contrôlés n'affichent pas de mention relative à la protection des données à caractère personnel.
Les résultats dudit contrôle ont ainsi dévoilé que très peu de sites web au Maroc (1%) se soucient de recueillir le consentement des internautes à collecter et traiter leurs données personnelles.
Dans la foulée, la commission a révélé que 71% des sites ne communiquent aucune «information sur l'identité du responsable du site web, les finalités du traitement, les destinataires des données collectées et autres renseignements ». Elle a, aussi, précisé que même pour le reste des sites (29 %), lesdites informations ne sont que partielles. Et d'ajouter qu'en matière de «demande de consentement des internautes à collecter et traiter leurs données personnelles», tandis que 80% des sites web ne l'évoquent pas, cette demande est même aléatoire pour 19%.
Le rapport fait état aussi des internautes qui sont, somme toute, privés de leurs droits. En effet, les résultats obtenus sont loin d'être reluisants en montrant que les internautes sont privés de l'exercice de leurs droits d'accès, de rectification et d'opposition auxquels la loi accorde pourtant une importance particulière. De ce fait, ces droits ne sont malheureusement pas assurés par l'écrasante majorité des sites web au Maroc, à savoir 95%. En ce qui concerne l'hébergement des sites à l'étranger (transfert de données personnelles à l'étranger), il est constaté qu'aucun des sites concernés n'a obtenu l'autorisation requise auprès de la CNDP.
Toujours est-il, ce contrôle a permis de porter sur le haut du pavois d'autres irrégularités qui concernent le principe de proportionnalité (collecte excessive de certaines données et injustifiée par le traitement) ainsi que les règles de la prospection directe et l'utilisation des cookies.
Ce faisant, la CNDP a décidé de prendre les mesures légales qui s'imposent à l'encontre des différents responsables de traitements qui ne procèdent pas à la mise en conformité de leur site web. Même si ces procédures disciplinaires peuvent déboucher sur un avertissement, un avertissement public, un blâme, voire le transfert du dossier à la justice, elles ne sont pas pour effaroucher certains, loin de vouloir se mettre au diapason de la loi n° 09-08.
Et sachant que dans l'article premier de cette dernière, il y est clairement stipulé que l'informatique est au service du citoyen (…), qu'elle ne doit pas porter atteinte à l'identité, aux droits et aux libertés collectives ou individuelles de l'Homme et qu'elle ne doit pas constituer un moyen de divulguer des secrets de la vie privée des citoyens, c'est dire qu'au Maroc, l'application de la présente loi traîne encore le pas.
D'où l'importance de susciter le débat qui aura donc le mérite de discuter des questions que soulève réellement cette loi.
Dans ce sens, l'AMISE (Association marocaine des Instituts de sondages et études de marché) co-organise une conférence-débat en collaboration avec la Fédération de commerce et de service de la CGEM et qui aura lieu dans la matinée de demain mercredi, au siège de la CGEM à Casablanca. Cette rencontre sera animée par la responsable de la communication de la CNDP, et a pour objectif premier de permettre aux participants de mieux comprendre les tenants et aboutissants de la loi 09-08 et d'examiner l'applicabilité de certaines dispositions de cette loi aux études de marché et sondages d'opinion, ainsi que leurs impacts sur les relations entre les instituts d'études et leurs clients.

Pour rappel, Denis JACOPINI, spécialisé en protection des données personnelles est mobile et disponible pour venir assurer des actions de mise en conformité ou de supervision de mise en conformité des traitements informatiques par rapport aux mesures de sécurité à mettre en place pou rassure rune meilleure sécurité et protection des données à caractère personnel.

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

Source : http://www.libe.ma/La-CNDP-va-t-elle-finir-par-prendre-le-taureau-par-les-cornes_a58378.html
Par Meyssoune Belmaza

Des failles de sécurité aussi dans les drones ?

28

Des failles de sécurité aussi dans les drones ?

Un chercheur indien croit avoir décelé une faille de sécurité lui permettant de prendre le contrôle d'un drone Parrot. Il a mis au point un malware capable de prendre le contrôle de l'appareil à distance et de modifier les instructions de vol.

Les drones, comme à peu près tout ce qui repose de près ou de loin sur les technologies numériques, ne sont pas exemptés de failles de sécurité. Le chercheur indien Rahul Sasi s'est lancé le défi de prendre le contrôle à distance d'un drone fabriqué par Parrot et pense y être parvenu, à l'aide d'un malware conçu par ses soins et sobrement baptisé Maldrone.
Rahul Sasi n'a pas encore publié de prototype détaillé de sa méthode, mais explique sur une page web la façon dont il a procédé et accompagne le tout d'une petite vidéo de son programme en action.
La faille trouvée par le chercheur indien lui permet de prendre dans une certaine mesure le contrôle de l'appareil en profitant d'une faille de sécurité du programme d'autopilotage du drone. En jouant avec les processus d'échanges d'informations entre les différents capteurs du drone et le programme d'autopilote, le pirate est capable de prendre la main sur un drone, et ce à distance.

Nos drones sont-ils dignes de confiance ?
Selon Rahul Sasi, la backdoor ainsi mise en place est du genre tenace et un simple reboot du drone ne suffit pas à s'en débarrasser, conférant à l'attaquant un accès persistant au système de contrôle du drone. Rahul Sasi explique que son malware est également capable de s'auto-répliquer et de se propager à d'autres drones.
Potentiellement inquiétant, le malware développé par le chercheur ne cherche néanmoins pas à nuire particulièrement aux utilisateurs mais a été crée dans un simple but de recherche et par pure curiosité selon Rahul Sasi. On peut donc écarter pour le moment la possibilité de voir un groupe de cybercriminels pirater à distance une armée de drones civils afin de faire passer de la drogue en douce à la frontière à l'insu de leurs propriétaires.
Mais pour l'instant, on prendra quelques pincettes : il faudra attendre le 7 février pour disposer de plus d'informations techniques sur le sujet, date à laquelle Rahul Sasi prévoit de revenir plus en profondeur sur son hack à l'occasion de la conférence Nullcon. Nous avons contacté Parrot à ce sujet et nous mettrons à jour cet article si la société souhaite réagir à cette annonce.

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

Source : http://www.zdnet.fr/actualites/les-drones-aussi-ont-des-failles-de-securite-39813694.htm
Par Louis Adam

Les entreprises doivent construire un modèle d’exploitation de leurs données

	Les entreprises doivent construire un modèle d’exploitation de leurs données

Face au Big Data, monétisation, confidentialité et gouvernance sont au menu des préoccupations des entreprises françaises en 2015.

En 2014 déjà, 43% des décideurs français interrogés considéraient la gestion des données et leur analyse comme une priorité selon une étude réalisée par MARKESS*. Aujourd'hui, les directions générales de nombreuses entreprises françaises le clament : l'année 2015 sera l'année du Big Data. Dans le rapport Data & Analytics Trends 2015 élaboré par le cabinet Deloitte, ces dernières voient en effet se dessiner un grand potentiel économique derrière la masse de données qu'elles génèrent. Les sociétés ressentent le besoin d'analyser les données qu'elles collectent pour créer de la valeur : anticiper des événements futurs, gérer les ressources, limiter les risques voilà autant de finalités à l'exploitation de ces données pour l'entreprise. Reste à savoir comment les exploiter au mieux. Et les solutions technologiques ne manquent pas.

En milieu hospitalier notamment, où l'expérience du patient occupe une place centrale, rassembler des données, sous la forme d'un tableau de bord offrant une visualisation modulable de l'information, sur les temps d'attente des patients ou encore les facteurs d'attribution d'une chambre, peuvent permettre au personnel infirmier, aux médecins et aux administrateurs d'optimiser leur capacité de traitement des patients, note Edouard Beaucourt, account manager chez Tableau Software.

L'Open Data, soit le partage de données, reçoit un écho favorable auprès des acteurs du secteur privé et ceci à des fins d'amélioration de la qualité des services offerts. Deloitte constate d'ailleurs une recrudescence des actions collaboratives entre les sociétés et leurs partenaires en matière de partage de données. Et plusieurs discussions naissent autour de la création de centres de partage de données inter-entreprises. Ce processus de démocratisation du partage de données encore faiblement structuré est amené à se rationaliser selon Reda Gomery, spécialiste des données et de l'analyse de données chez Deloitte, auteur de l'étude.

Preuve de l'émergence d'une collaboration accrue entre les parties prenantes, Deloitte relève le projet d'une compagnie d'assurance, l'«hackathon », compétition ouverte aux développeurs de tous horizons. Leur mission consiste à réfléchir à de nouvelles applications de scoring des clients de l'entreprise à partir de données qui leur sont confiées.

Il est d'usage de dire que les crises s'accompagnent souvent d'un regain de créativité. Raison pour laquelle les entreprises cherchent une monétisation adéquate de leurs données. Les secteurs des télécoms et des services financiers ont été d'ailleurs été pionniers dans le développement de services de vente de données.
Deloitte met en avant dans son rapport l'initiative d'un opérateur téléphonique qui d'après les données fournies par ses antennes relais a su analyser la fréquentation de sites touristiques par des visiteurs étrangers, données qui ont pu être vendues par la suite à des offices de tourisme, générant ainsi de nouveaux revenus pour l'entreprise.

En 2015, les entreprises réalisent complètement la valeur des informations qu'elles possèdent pour les acteurs avec qui elles interagissent et expérimentent de nouveaux modèles. Non sans interrogations sur la confidentialité de ces données. Se pencher sur les modèles de protection pour sécuriser l'information et préserver l'anonymat des clients conduit à son corollaire : le mode de gouvernance. Les entreprises se préoccupent en effet également de chercher le cadre le plus adapté pour maîtriser ses flux gigantesques et continus d'informations.

*Etude MARKESS : Meilleures approches pour tirer parti du Big Data, France, 2014

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

Source : http://www.atelier.net/trends/articles/entreprises-doivent-construire-un-modele-exploitation-de-leurs-donnees_433304