Le délit d’usurpation d’identité numérique, un nouveau fondement juridique pour lutter contre la cybercriminalité. Par Betty Sfez, Avocat.

Le délit d’usurpation d’identité numérique, un nouveau fondement juridique pour lutter contre la cybercriminalité. Par Betty Sfez, Avocat.

Bill Gates met en garde au sujet des futurs progrès de l’intelligence artificielle

	Bill Gates met en garde au sujet des futurs progrès de l’intelligence artificielle

Après le chercheur Stephen Hawking et l'entrepreneur Elon Musk, c'est au tour de Bill Gates de demander à ce que chacun réfléchisse aux progrès de l'intelligence artificielle. Le fondateur de Microsoft confie son inquiétude sur le sujet.

« Science sans conscience n'est que ruine de l'âme ». La formule de Rabelais trouve une nouvelle résonance aux yeux de certains chercheurs, entrepreneurs et personnalités reconnues du monde des Sciences. Plusieurs d'entre eux n'hésitent désormais pas à témoigner de leurs inquiétudes au sujet de l'évolution de l'intelligence artificielle.
Bill Gates s'interroge à ce sujet et considère que l'utilisation de ce type de technologie doit provoquer des réflexions en chacun de nous. L'ancien dirigeant de Microsoft rejoint des questionnements déjà entamés par Stephen Hawking ou même par le fondateur de PayPal, SpaceX et Tesla, Elon Musk.

« Je ne comprends pas pourquoi certaines personnes ne s'en préoccupent pas »
Interrogé dans le cadre d'une session de questions/réponses organisée sur le site Reddit, Bill Gates explique : « Je suis dans le camp de ceux qui se préoccupent de l'évolution des super intelligences. Tout d'abord, les machines exécuteront de nombreuses tâches à notre place et n'auront pas besoin d'être réellement dotées d'une intelligence redoutable. Ce doit donc être un mouvement positif si nous les gérons correctement. Mais plusieurs décennies après, cette même intelligence sera suffisamment puissante pour qu'elle représente un problème. Je suis donc totalement en accord avec les propos d'Elon Musk et d'autres à ce sujet, et je ne comprends d'ailleurs pas pourquoi certaines personnes ne s'en préoccupent pas ».
L'ancien dirigeant de Microsoft souhaite donc que les progrès futurs de l'intelligence artificielle puissent être observés et éventuellement interrogés. Il considère cependant la technologie comme un élément important de nos sociétés.
Au cours de la même session ouverte de questions/réponses, Bill Gates précise : « la technologie ne rend pas les gens moins intelligents. […] Elle leur permet de mieux répondre à certaines de leurs questions afin qu'ils demeurent encore plus curieux. De nos jours, il est plus facile d'en savoir plus sur de nombreux sujets importants, ce qui nous permet de résoudre des problèmes complexes ».

Des inquiétudes déjà formulées par Stephen Hawking ou Elon Musk
Dans une tribune co-signée avec trois autres scientifiques, le physicien Stephen Hawking a formulé cette année des inquiétudes similaires au sujet du développement des intelligences artificielles. Leurs propos, repris dans la presse britannique, évoquaient les réalisations actuelles comme des éléments qui « feront sans doute pâle figure par rapport à ce que les prochaines décennies apporteront ».

Elon Musk

« On peut imaginer que cette technologie soit capable de déjouer les marchés financiers, de dépasser les scientifiques humains, de manipuler les dirigeants et développer des armes qu'on ne puisse pas comprendre. L'incidence à court terme de l'intelligence artificielle dépend de celui qui la contrôle, mais, à long terme, cela dépend de la possibilité concrète de la contrôler », ajoutaient les chercheurs.

Plus récemment, Elon Musk, a également livré ses inquiétudes à ce sujet. Le dirigeant de Tesla et SpaceX expliquait qu'avec l'intelligence artificielle, « nous invoquons un démon. Dans toutes les histoires mettant en scène un type avec un pentagramme et de l'eau bénite, il est sûr et certain qu'il va pouvoir contrôler le démon. Sauf qu'il n'y arrive pas. » Là encore, l'entrepreneur en appelait à la prudence.

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

Source : http://www.clubic.com/mag/culture/actualite-752143-bill-gates-intelligence-artificielle.html

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

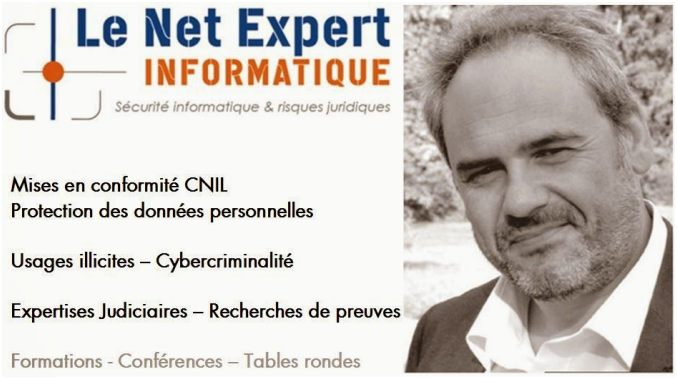
Prévenir les cyber-attaques avec Denis JACOPINI – Conférence le 10 février

	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

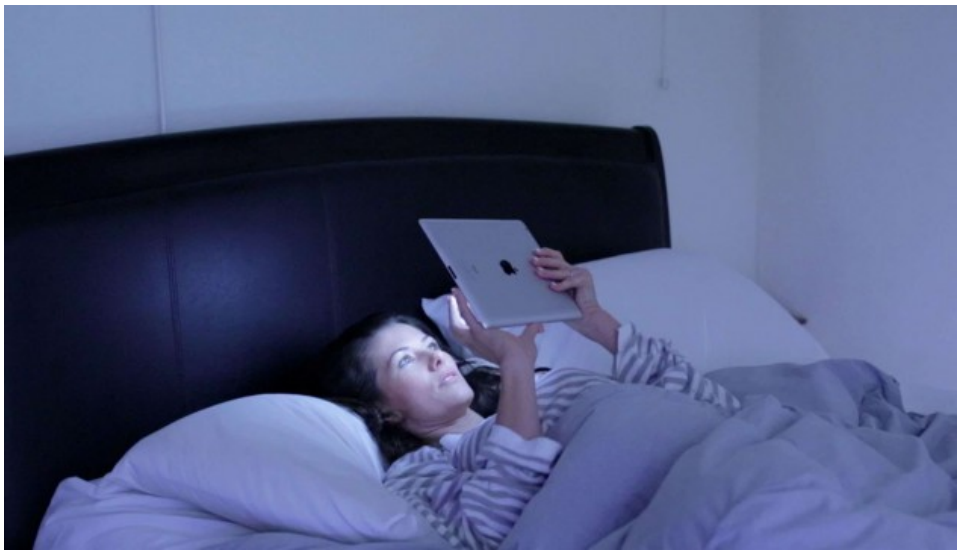
Entrée libre, inscription obligatoire ! 600 m² – 35 stands – 16 conférences – Le rendez vous incontournable du numérique pour votre entreprise.

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…

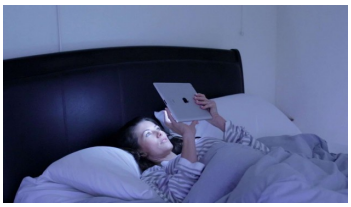
Programme et infos pratiques : http://www.salon-du-numerique.fr/le-programme/

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

Une faille critique permet de

prendre le contrôle des routeurs, des nas, des systèmes Linux…

Une faille critique permet de prendre le contrôle des routeurs, des nas, des systèmes Linux…

L'éditeur Qualys a mis la main sur une vulnérabilité importante qui permettrait de prendre le contrôle à distance de la plupart des distributions Linux. Les appareils de type routeurs-modems ou NAS sont également concernés.

Les chercheurs en sécurité de la société Qualys ont mis la main sur une faille critique (CVE-2015-0235) qui touche tous les systèmes Linux. Baptisée « Ghost », elle permettrait aux pirates de prendre le contrôle à distance « de tout un système, en se passant totalement des identifiants système », explique l'entreprise dans un communiqué. Un patch a été développé en concertation avec les éditeurs Linux. Il est en cours de diffusion et d'ores et déjà disponible sur certaines distributions, telles de Debian, Red Hat ou Ubuntu.
Cette terrible faille est logée dans une librairie GNU/Linux baptisée« glibc », qui est intégrée dans toutes les distributions Linux et qui permet de gérer les appels système de bas niveau, comme l'allocation d'espace mémoire, l'ouverture de fichiers, etc. Seules les versions antérieures à glibc 2.18 sont vulnérables. « Malheureusement, très de peu distributions Linux ont intégrés les versions récentes de glibc, pour des raisons de compatibilité. C'est pourquoi la plupart sont vulnérables », explique Wolfgang Kandek, directeur technique de Qualys.

Quid des routeurs ou des NAS ?
Comment fonctionne Ghost ? Cette vulnérabilité se caractérise par un dépassement de mémoire tampon (buffer overflow) dans les fonctions gesthostbyname et gethostbyaddr. Ces fonctions sont appelées par les applications Linux quand elles doivent gérer des connexions Internet, comme par exemple les serveurs de messagerie. C'est d'ailleurs la cible sur laquelle se sont penchés les chercheurs de Qualys pour développer un exemple de code d'exploitation : ils ont conçu une attaque dans laquelle il suffit d'envoyer un email vers le serveur pour accéder à l'interface ligne de commande (shell). C'est aussi simple que ça !
Qualys recommande aux administrateurs de mettre à jour leurs systèmes Linux aussi rapidement que possible. Mais une question reste en suspens : quid des nombreux objets connectés que nous possédons tous à la maison, tels que les routeurs-modems ou les disques durs en réseau (NAS) ? « Ils intègrent tous la librairie glibc. Mais pour créer une attaque, il faut également que ces appareils utilisent les fonctions vulnérables. Il faut ensuite trouver le bon vecteur d'attaque. Ce n'est pas évident à priori », souligne Wolfgang Kandek. En somme : pas la peine de paniquer tout de suite. Les pirates vont certainement se pencher sur la question, mais ils vont mettre du temps à développer leurs attaques. Pour réduire le risque, il est conseillé de mettre à jour les firmwares des appareils dès qu'ils seront disponibles.

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

Source : http://www.01net.com/editorial/643126/ghost-la-faille-critique-qui-permet-de-prendre-le-controle-des-systemes-linux/
Par Gilbert Kallenborn

La cybercriminalité à l’encontre des entreprises s’industrialise

	La cybercriminalité à l’encontre des entreprises s’industrialise

Un écosystème professionnalisé de cybercriminels mène la danse.
Pas d'électrochoc dans les entreprises après l'affaire Sony : les investissements restent insuffisants.
Sony débordé par les cybercriminels
Phishing, escroquerie, espionnage, vol de secrets industriels… Si ces phénomènes ne sont pas nouveaux, la cybercriminalité ne s'est jamais aussi bien portée.
Bernard Cazeneuve n'a pas manqué de rappeler la réalité de cette menace au Forum international de la cybersécurité, qui s'est tenu à Lille la semaine dernière. « Des attaques de plus en plus sophistiquées touchent principalement les entreprises et visent à leur voler des données stratégiques, parfois en très grande quantité », a fait valoir le ministre de l'Intérieur. Si le phénomène est difficile à chiffrer, il connaît une montée en puissance. Pourquoi ? « La technologie explose. Il y a de plus en plus d'applications. Plus on développe vite, plus le risque de bugs augmente», explique Jean-Michel Orozco, président de CyberSecurity chez Airbus Group (ex-Cassidian).
Au quotidien, les entreprises doivent lutter contre la petite délinquance, peu sophistiquée mais rentable. « Les entreprises ont été fortement touchées par les "cryptolockers" », explique Eric Freyssinet, chef de la division de lutte contre la cybercriminalité de la Gendarmerie nationale. Des pirates bloquent des PC, et exigent des rançons pour les débloquer. Bien sûr, celui qui paie ne récupère pas pour autant ses données.
« Les anciennes menaces s'industrialisent. Les banques, par exemple, souffrent beaucoup d'attaques en déni de service [rafale d'attaques dont le but est de bloquer les systèmes] ou de phishing », explique Michel Van Der Berghe, à la tête d'Orange Cyberdefense. Plus élaboré, « le "spearphishing" permet d'envoyer des e-mails ultraciblés personnalisés par secteur identifié, l'armement, le transport… » dit Eric Freyssinet. C'est grâce à un e-mail très bien personnalisé que la Syrian Electronic Army a réussi, ces derniers jours, à pirater « Le Monde ».

Des PME très exposées
Les PME sont particulièrement exposées aux faux placements, où la victime verse de l'argent à un tiers soi-disant spécialisé dans les placements à haut rendement. Selon la gendarmerie, ce type d'attaque représente les « trois quarts des escroqueries » qui concernent les entreprises. Plus connue, « l'arnaque au président » consiste à extorquer de l'argent à une entreprise en se faisant passer pour son dirigeant. Parmi les victimes, Michelin, qui a perdu 1,6 million d'euros.
L'espionnage – de secrets industriels ou commerciaux –, un fléau auquel font face les entreprises depuis deux ou trois ans, ne requiert pas non plus de techniques ultrasophistiquées. « Un mot de passe faible, type 1 2 3 4 5 6, sur un équipement de réseau ou une application peut suffire », estime Stanislas de Maupeou, directeur-conseil cybersécurité chez Thales. Dans ce cas-là, la difficulté consiste surtout à identifier les intrusions.

Cellules « N-Tech » : la gendarmerie aussi s'arme face à la cybercriminalité

Pas facile de lutter contre ces attaques à grande échelle. Car, en face, on a affaire, non pas à des groupements organisés, mais à un écosystème criminel. « Sur le "dark Web", on trouve des publicités pour des attaques en kit. Il y a même des réductions ! » explique Michel Van Der Berghe. « Ceux qui vendent les virus ne sont pas ceux qui les collectent. Deux personnes différentes à deux bouts de la France peuvent se mettre d'accord pour développer un virus. Elles communiquent sur Tor, sur certains forums ou sur des messageries instantanées comme Jabber », explique le lieutenant-colonel.
De leur côté, les entreprises restent insuffisamment armées. Le piratage massif de Sony, victime d'un vol à grande échelle de données, n'a pas créé d'électrochoc. Chez Thales, un seul client exerçant dans le même domaine que Sony, et expliquant qu'il ne pourrait supporter une attaque d'une telle ampleur, a appelé, chez Airbus aucun.

Pas seulement des moyens
Beaucoup de dirigeants n'ont pas encore fait grand-chose. « Les moyens seuls ne suffisent pas. Il faut aussi un plan, avec une gouvernance qui sait quoi faire en cas de problème », détaille Jean-Michel Orozco, d'Airbus CyberSecurity, qui estime qu'un grand groupe devrait dépenser entre 8 et 11 % de son budget informatique en sécurité. On est loin du compte. « Aujourd'hui, on est à 3 ou 4 %. Or, en cas de problème, si l'on doit remonter entièrement un système, cela peut coûter 20 % du budget IT », estime Stanislas de Maupeou, qui rappelle qu'au regard des outils existants, la lutte contre le fléau est à la portée de tous.

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

Source : http://www.lesechos.fr/tech-medias/hightech/0204110358637-la-cybercriminalite-a-lencontre-des-entreprises-sindustrialise-1087050.php
Par Sandrine Cassini