Utilisateurs de Tor identifiés – Le FBI reste muet

Utilisateurs de Tor identifiés – Le FBI reste muet

Le FBI soppose à une demande de la justice qui exige de la police américaine quelle présente sa méthode lui ayant permis didentifier des utilisateurs d'un site pédopornographique, en les piratant.

Le FBI n'a absolument aucune envie de dévoiler la méthode secrète qu'il a employé pour pirater plus d'un millier de membres d'un site pédopornographique. Et cela, même si c'est la justice américaine qui lui demande.
C'est en effet ce qu'est en train de révéler le procès visant une personne accusée d'avoir fréquenté cet espace, dont l'accès ne pouvait se faire qu'à travers le réseau d'anonymisation TOR.
Dans cette affaire, les avocats du prévenu souhaitent connaître la technique utilisée par la police fédérale pour infecter les ordinateurs de ceux qui visitaient Playpen – le nom de ce site pédopornographique – lorsqu'il était encore en ligne.
Pour la défense, il s'agit de tenter de démontrer que le FBI a outrepassé ses prérogatives au cours de l'enquête, en débordant du cadre de son mandat.

Sceau FBI

L'approche du FBI dans l'affaire PlayPen fait polémique outre-Atlantique.
En février, le magistrat a donné suite à cette demande et exigé du FBI qu'il communique à la partie adverse tous les détails de sa méthode de piratage. Mais comme le pointe la BBC, le service de police est particulièrement hostile à cette demande. Un courrier a été adressé cette semaine au juge afin de l'inviter à reconsidérer sa position, estimant que la défense dispose déjà de suffisamment de pièces pour travailler.
En réalité, l'opposition du FBI vise avant tout à préserver l'intérêt de sa technique. En effet, il se pourrait qu'une communication des détails à la partie adverse affaiblisse l'efficacité de cette méthode. Si celle-ci devient publiquement connue, les failles qu'elle exploite seraient tôt ou tard colmatées par TOR, les navigateurs et les serveurs hébergeant des sites web. De même, les utilisateurs se montreraient aussi plus prudents.

LE FBI VEUT PRÉSERVER L'EFFICACITÉ DE SA MÉTHODE EN LA GARDANT SECRÈTE

C'est sans doute ce scénario que le FBI veut éviter, afin de pouvoir l'appliquer de nouveau à l'avenir si le besoin s'en fait sentir. Et si la position de la police fédérale se défend, celle de la défense, qui agit dans l'intérêt de son client, est tout aussi audible : le FBI a-t-il enfreint son mandat au nom de la loi ? Et la méthode employée est-elle vraiment fiable ? Une erreur au niveau de l'identification de l'internaute est toujours possible.
L'affaire Playpen remonte au tout début de l'année 2015, lorsque le FBI réussit à prendre le contrôle des serveurs du site pédopornographique. Plutôt que de le fermer immédiatement, ce qui a aussi provoqué son lot de critiques lorsque l'information a été révélée publiquement, la police opte pour une autre approche, celle du honeypot : le site est demeuré actif pendant près de deux semaines, en utilisant ses propres serveurs, de façon à voir qui se connecte sur Playpen.

Le principe du réseau TOR rappelle celui des couches de l'oignon qui masquent le cœur de la plante.
C'est à ce moment-là que le FBI a utilisé sa fameuse technique pour contaminer le poste informatique des visiteurs, afin, notamment, de récupérer leur véritable adresse IP, qui est habituellement cachée avec le réseau d'anonymisation TOR, puisque la connexion passe par une succession de relais afin de camoufler la géolocalisation du PC d'origine.
Une fois l'adresse IP en main, il a suffit de contacter les fournisseurs d'accès à Internet – en tout cas ceux aux USA – pour avoir l'identité des internautes. Au total, la technique du FBI a permis de collecter pas moins de 1 300 adresses IP… [Lire la suite]

Réagissez à cet article

Source : *Le FBI refuse de dire comment il identifie des utilisateurs de Tor – Politique – Numerama*

Mise à disposition d’un accès Internet au public – Quelles précautions

Mise à disposition d’un accès Internet au public – Quelles précautions ?

Source : *Mise en place de points d’accès public à internet – informations et conseils juridiques*

Sans GPS Google sait d’où vient une photo

Sans GPS, Google sait d’où vient une photo

Ce logiciel PlaNet de Google devine le lieu d'une prise de vue, sans recourir aux coordonnées GPS de la photo.

Les équipes de Google spécialisées en intelligence artificielle mettent actuellement au point un logiciel capable d'identifier le lieu où a été prise une photo, sans avoir besoin d'utiliser les données GPS de la prise de vue.

Baptisé « PlaNet », ce projet de Google n'a pas encore atteint des résultats vraiment fiables, mais le logiciel est déjà meilleur que les humains pour reconnaître la géolocalisation d'une photo.

En se fondant sur une base de données de plus de 2 millions d'images géolocalisées de FlickR, les ingénieurs de Google sont désormais capables de deviner à 48% l'endroit où a été prise une photo. Ce niveau de performance permet à PlaNet de battre des humains 3 fois sur 5 en moyenne.

Sur le site GeoGuessR, les internautes sont invités à se confronter à PlaNet. En 20 secondes, les visiteurs doivent essayer de deviner l'endroit où une photo a été prise, ce qui est un véritable défi quand il s'agit d'un paysage désertique.

A ce petit jeu de géolocalisation, le logiciel PlaNet atteint une précision de 1 130 kilomètres, là où les humains n'en sont qu'à 2 320…

Un résultat surprenant pour un logiciel léger, qui pourrait tenir sans problème sur un smartphone, et devenir à terme, un logiciel de reconnaissance d'images que Google pourrait utiliser … [Lire la suite]

Réagissez à cet article

Source : *Sans GPS Google sait d'où vient une photo*

Panorama de la Cybercriminalité en 2015 : Attaques sur tous les fronts !

Panorama de la Cybercriminalité en 2015 : Attaques sur tous les fronts !

La nouvelle édition du panorama de la cybercriminalité du CLUSIF a fait la démonstration que la crise ne touche pas les pirates informatiques bien au contraire. Ils restent toujours aussi inventifs d'autant que leur terrain de jeu s'accroit grâce à l'introduction des nouvelles technologies dans de plus en plus de domaine entre autre avec les objets connectés. En parallèle, le cyber-terrorisme s'il n'est pas encore avéré au sens d'attaque visant à des détruire des entreprises ou des infrastructures critiques se sert du net pour tisser sa toile en recrutant des futurs terroristes, en menant des actions de communication, voir en servant de support pour monter des opération sur le terrain… cette année riche en actions malveillantes laisse augurer du pire pour 2016…

Après l'introduction par Lazaro Pejsachowicz, le président du CLUSIF qui a présenté les différentes activités de l'association, le panorama a débuté. En introduction il a rappelé que le cyber-crime se porte très bien. En outre, il a annoncé qu'en juin prochain aura lieu la conférence sur les résultats de l'enquête MIPS pour Menaces Informatiques et Pratiques de Sécurité.


Fabien Cozic

Quelques astuces utilisés en 2015

Fabien Cozic, directeur d'enquêtes privées Read Team Investigation, a passé en revue quelques astuces utilisées par les pirates a commencé par la Yes Card qui a exercé ses activités en France et en Belgique. Le pirate était un ingénieur qui avait rajouté une petite puce de la carte bancaire qui permettait de valider les transactions en se substituant à la puce déjà installée.
Un groupe de pirate avait mis en place un système astucieux de déposé et de retrait des sommes. Puis une équipe en République Tchèque puis un second groupe effectuait des transactions aux Etats-Unis puis les annulait et récupérait ainsi de l'argent. Le préjudice se chiffrerait autour de 6 millions d'euros.
XCode Ghost qui a détourné le système de contrôle des applications d'Apple. Les pirates ont utilisé une faille humaine de ce système pour déposer des malwares afin de récupérer des informations
Le malwares Turla a utilisé des APT pour réaliser des écoutes en se servant des liaisons des satellites de communication.
Un malware a été conçu pour prendre le contrôle de la lunette de visé d'un fusil afin de déclencher le tir…
Pour conclure il a cité le détournement d'un jouet en utilisant le système de communication pour ouvrir les portes de garages. Ce malware a contribué à plusieurs cambriolages aux Etats-Unis.


Hervé Schauer

Le 0 Days un business juteux pour les entreprises

Loic Samain du CEIS représenté par Hervé Schauer a présenté l'évolution du business des 0 Days. La palme de l'année revient à un 0 Day sur IOS qui a été récompensé par 1 millions de $. Les systèmes de plateforme de 0 Day existent et se développent. Leurs clients sont tout d'abord les gouvernements qui veulent réaliser des écoutes, mener des attaques… Il a donné quelques exemples de prix comme par exemple 2000$ pour un 0 Day ciblant un site de ecommerce, pour Windows le prix est de 150000$… et pour IOS a atteint 1 million de $.
Le 20 mai 2015 la proposition Wassenaar sur les 0 Day a été publié et elle est déjà adopté par plusieurs pays. Une nouvelle proposition pour amender cette proposition devrait être faite en 2016. Aujourd'hui les primes aux 0 Days explosent avec des prix allant de 2000$ à plusieurs milliers de $. Ainsi, les entreprises de Bug Bounty voient leur valorisation exploser.
Ainsi, Vupen est devenu un grossiste en 0 Day et s'appelle aujourd'hui Zerodium. En janvier 2016 une faille de sécurité a été payée 100 000$ par cette entreprise pour la découverte d'une faille sur flash. Pour Hervé Schauer « 2015 est donc l'année de la professionnalisation de ce marché. »


Loïc Guezo

La cyber-diplomatie commence à émerger

Loïc Guezo, Strategist chez Trend Micro, a expliqué que l'on va vers une cyber-diplomatie avec entre autre la remise en cause de l'ICANN qui est au centre de très grandes manœuvres. On a de nombreux pays qui reconnaissent une capacité offensive sur Internet a commencé par les États-Unis, la Grande Bretagne, la Chine, la Russie et maintenant la France. En 2015, il a rappelé le cas du piratage OPM qui est une sorte de RH des agents des services spéciaux américains avec la récupération très personnel sur l'ensemble des collaborateurs. La Chine a été suspectée d'être l'auteur de ce piratage. Suite à cette accusation plusieurs arrestations ont eu lieu en Chine afin de faire diminuer les tensions entre ces deux pays. Aujourd'hui, le doute persiste sur la nature des personnes arrêtées. Le 31 décembre 2015 les autorités américaines ont ressortie une attaque sur 2009 ciblant Microsoft. Par contre Microsoft n'a pas alerté ces clients. Par ailleurs, la Russie a signé un pacte de non-agression avec la Chine mais ne signifie pas l'arrêt des opérations entre ces deux pays, il y a par contre une convergence de doctrine sur l'Internet autour de l'idée de souveraineté.
Quant à l'Iran et dans une moindre mesure à la Corée du Nord, ils ont été pointés par les Etat-Unis comme deux dangereux pays sources de piratages.
Par ailleurs, il a cité l'Accord Umbrella qui a été noté comme une grande avance en particulier Ui permet de facilité les procédures d'extradition. En France, il faut noter la publication de la Nouvelle Stratégie de la sécurité du numérique. A cette occasion, David Martinon a été nommé Ambassadeur pour la cyber-diplomatie et de l'économie digitale.
La cyber-diplomatie est devenue un élément clé de la vie politique dont l'influence géopolitique prévue dans cette nouvelle stratégie.

François Paget

Le Djiad Numérique : recrutement, endoctrinement…

François Paget a présenté pour sa part le Djiad Numérique. Lors du panorama 2004, il avait été évoqué l'utilisation d'Internet par les terroristes. Aujourd'hui, ils utilisent les réseaux sociaux et adressent plusieurs milliers de Tweet par jour. Daesh offre des conseils pour se dissimuler via par exemple les réseaux Tor, mais aussi Telegram. Ce dernier réseau social est dominant en Russie. Il permet de communiquer de façon chiffrée mais aussi de détruire les messages une fois lus. Les djihadistes se servent aussi du darknet, peut-être de Bitcoins… pour acheter des armes. Sans compter que les réseaux sociaux sont utilisés pour recruter des membres mais ce n'est pas le seul vecteur d'enrolement.
En novembre, les Anonymous se sont réveillés pour attaquer les djihadistes avec des actions parfois intéressantes, mais ils aussi ont réalisé des bévues qui ont parfois ralenties les actions des forces de police, voire aussi en attaquant des sites qui étaient en arabes mais sans aucun lien avec les terroristes.
En janvier dernier, il y a eu des défacements de sites surtout en janvier en particulier par Isis. Par contre, il y en a eu très peu après les attentats de novembre. Durant ces moments tragiques, Google a été particulièrement sollicité. Par contre, les réseaux sociaux ont servi à des élans de solidarité surtout en novembre. En revanche, Facebook a mis parfois beaucoup de temps pour fermer des sites malveillants. Quant à tweeter il a agi un peu plus rapidement, mais a laissé courir de nombreuses rumeurs. En ces périodes, il y eu de nombreuses fausses rumeurs qui ont circulé avec même des chevaux de Troie dissimulés dans certaines images.


Amélie Paget

Vers une limitation des libertés ?

Amélie Paget, consultante juridique SI HCS by Deloitte a fait le point sur les deux nouvelles lois publié en 2015 pour renforcer les pouvoir de l'Etat : la loi sur le renseignement et l'Etat d'urgence. Pour ce qui concerne l'état d'urgence il a été prorogé jusqu'au 26 février 2016. Désormais, lors des perquisitions, les agents peuvent accéder aux données stockées sur les systèmes Informatiques ou l'équipement terminal ou accessible à partir du système initial. En outre, ils auront la possibilité de copier les donner et d'effectuer des saisies en cas d'infraction. Par ailleurs un projet de loi souhaite insérer à notre Constitution, un nouvel article consacré à l'état d'urgence.
En ce qui concerne la Loi sur le renseignement, elle donne des prérogatives pour accéder aux données de connexion en les demandant aux opérateurs, aux FAI et hébergeurs.. Les agents peuvent utiliser des outils de géolocalisation et demander en temps réel aux FAI des information et documents qui transite sur le réseau. Bien sûr toutes ces actions ne peuvent s'effectuer que pour protéger les intérêts fondamentaux de la Nation, notamment pour la prévention du terrorisme. Les agents peuvent collecter des informations en échangeant sur la toile. Quant au chiffrement les opérateurs auront 72 heures pour offrir un système de déchiffrement ou directement les documents en clair.


Gérôme Billois

Objets connectés : la sécurité doit être intégré by design

Gérôme Billois, Manager Sécurité de Solucom a traité des attaques sur les objets connectés en rappelant qu'en juillet dernier deux chercheurs ont pris le contrôle à distance d'une voiture connectée. En fait, les consoles de bords sont connectées à un premier Réseau dit de confort et un second pour la conduite comme celui qui gère le régulateur de vitesse, la boite de vitesse, le volant… En fait, la console de bord est assez facile à pirater et permet de prendre le contrôle de la console de confort. Par contre, la console de sécurité est plus difficile à pirater. Par contre, avec du temps et un peu de chance selon les dires de ces deux chercheurs, la prise de contrôle sur la console de sécurité est faisable. Cette démonstration a eu des impacts médiatiques mais aussi financiers pour les constructeurs avec l'envoi de clés USB aux utilisateurs pour faire des mises à jours, heureusement à ce jour, toujours pas d'attaque sur les voitures… Toutefois il est possible d'envisager la diffusion de ramsowares qui bloqueraient les voitures…
Au delà des voitures, les jouets connectés ont fait l'objet d'attaques plus ou moins amusants avec par exemple Barbie, les téléviseurs… Par contre, d'autres attaques seraient plus graves comme celle sur des pompes à insuline, des fusils, voir des avions…
En fait, en matière de sécurité des objets connectés il y a 4 dimensions à prendre compte : ceux qui les conçoivent, ceux qui les achètent, ceux qui les conseillent et tous ceux qui vont les accueillir en particulier dans les entreprises. Il faut donc réagir en intégrant la sécurité, en protégeant notre vie privée, sans oublier les spécificités de ces objets. Demain, nous allons voir arriver les objets autonomes qui vont demain faire partie de notre quotidien avec par exemple des robots qui vont être mis dans les boutiques Nespresso, à bord des bateaux de Costa Croisières… Cela pose, de nombreuses questions juridiques.


Garance Mathias

Objets connectés : les premiers procès à l'horizon 2016

Garance Mathias en préambule de son intervention explique que nous sommes tous concernés par les objets connectés car nous en avons tous. Le droit à déjà prévu le fait que l'on est responsable de nos objets. Un grand classique du droit est qu'il s'impose à tous les acteurs : le concepteur, l'utilisateur… Par exemple, le Cloud qui relie les objets connectés n'est qu'une externalisation avec toutes les contraintes liées.
Concernant les objets connectés, il faut aussi prendre en compte les analyses d'impacts d'où la nécessité pour les fabricants d'embarquer la sécurité y design. Elle a pris l'exemple de Vtech qui avait fait l'objet d'une plainte par « UFC Que Choisir » du fait de la non-prise en compte de la protection de la vie privée.


Le Colonel Éric Freyssinet

Téléphonie mobile : le protocole SS7 mis à mal…

Le Colonel Éric Freyssinet a évoqué en premier lieu la sécurité des téléphones mobiles. Fin 2014, une conférence lors du CCC a mis en lumière une vulnérabilité dans le protocole SS7 qui permettait de rediriger des communications et d'intercepter des SMS (chiffrés). En ce qui concerne les logiciels malveillants, il y a eu peu de nouveautés. Toutefois, parmi les nouveautés on trouve Pornbroid qui bloque le téléphone sous Android qui est un logiciel assez avancés capable de se relancer une fois désinstallé. Il a aussi cité Xcode qui exploite une vulnérabilité sur IOS.
… et des attaques aux effets collatéraux redoutables
Puis, le Colonel Eric Freyssinet a présenté les conséquences d'une attaque. Il a pris l'exemple de Target dont l'attaque a coûté environ 67 millions de $ avec Visa, la même somme avec MasterCard au final cette attaque devrait coûter environ 100 Millions de $ dont 90 sont pris par son assurance.
L'attaque contre OPM qui ciblait les personnels de l'état américain par la Chine a obligé la CIA a retiré des agents basés en Chine, sans compter la notification à plusieurs millions de personnes.
Hello Kity a aussi été visé par une attaque ciblée pour récupérées données Bancaires des parents.
TV 5 Monde a été une des premières véritables attaques pour détruire une entreprise. Au final l'impact sur le SI a été faible par contre les ventes de publicité se sont effondrées et son budget sécurité a été augmenté de façon conséquente. Son PDG a témoigné dans plusieurs conférences ce qui a un effet plutôt positif.
Ashley Madison est une affaire assez complexe. On a noté quelques retombées tragique comme le suicide d'un pasteur, des démissions, des chantages… De ce fait, la CNIL a demandé aux sites de rencontre français de renforcer leur sécurité.
Pour finir, il a recommandé de prévenir les risques, être capable de décréter la survenance d'un incident et être en mesure de maitriser leur impact.
François Paget a pour sa part rappelé que les forces de police rencontrent quelques succès en arrêtant des cybercriminels partout dans le monde.

Jean-Yves Latournerie

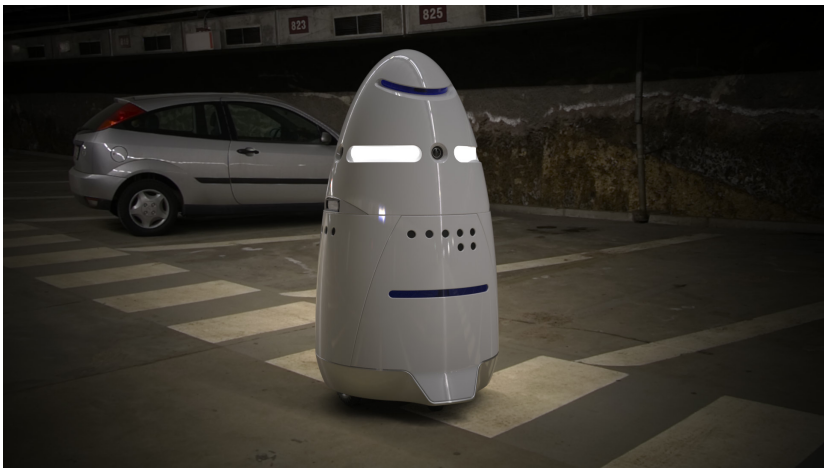
Nous passons à lutte anti-terroriste 2.0

La conclusion a été assurée par le cyber-préfet Jean-Yves Latournerie qui a félicité les intervenants et les organisateurs de ce panorama. Selon lui, il n'y a pas à ce jour d'actions en cyber-terrorisme à proprement parler. Par contre, le cyber joue un rôle très important dans la radicalisation, le recrutement et le passage à l'acte. Dans ces périodes tragiques, on apprend vite et on est en train de passer dans la lutte antiterroriste 2.0. Dans ce cadre le panorama du CLUSIF est important afin de mieux comprendre la nature de la menace de façon systémique et analytique et pouvoir ainsi anticiper les développements des actions terroristes. Il s'est félicité de voir le travail entre les forces de police et les entreprises privées se renforcer en particulier avec les principaux acteurs d l'Internet. Il note de réel progrès opérationnel entre janvier et novembre dernier. En effet, un travail méthodologique a été effectué entre ces deux périodes qui porte ces fruits aujourd'hui.
Il a conclu son intervention en rappelant que même s'il a quelques arrestations, le crime pour le moment sort le plus souvent des confrontations avec les forces de polices, toutefois, il semble que tous les acteurs d'Internet sont de plus en plus sensibiliser à ces attaques ce qui donne des espoirs pour améliorer cette situation.

Réagissez à cet article

Source : *Panorama 2015 de la Cybercriminalité du CLUSIF : Attaques sur tous les fronts ! – Global Security Mag Online*

Des robots sentinelle contre le crime dans la Silicon Valley



Des robots sentinelle contre le crime dans la Silicon Valley

Une start-up de Palo Alto, Knightscope, déploie dans les rues de la Silicon Valley des robots pour lutter contre le crime.

Non, ce n'est pas le pitch d'un nouveau film d'anticipation ou de science-fiction, mais bien une réalité d'aujourd'hui. Ces robots, les Knightscope K5 Security Robot, sont déjà dans les rues et patrouilles pour dissuader ou récolter des données.

Bardés de capteurs

Ces robots ne sont pas armés, ce qui pourrait arriver aux États-Unis vu les lois en vigueur dans certains états. Par contre, ils sont équipés de multiples capteurs qui leur permettent de voir à 360°, d'entendre, de sentir et de ressentir. Le système de guidage et de pilotage est le même que celui des Google Car.

Ils mesurent un peu plus d'un mètre cinquante, pèsent près de 137 kg, sont de forme ovoïde et de couleur blanche. Ils téléchargent en temps réel ce qu'ils voient et entendent et sont conçus pour réagir à des bruits significatifs comme le bris de glace ou des coups de feu. Si cela se produit, le K5 enregistre alors beaucoup d'informations sur son environnement comme la géolocalisation, photos, vidéos, plaques d'immatriculation des véhicules à proximité et même les visages des personnes proches dans l'éventualité d'une reconnaissance faciale.

Les K5 peuvent donner l'alerte aux autorités compétentes en cas de « détection » crime via une plateforme Internet accessibles aux forces de l'ordre.

Le K5 est déjà en fonction dans des centres commerciaux ou des campus universitaires comme assistant de sécurité et, selon Stacy Stephens cofondatrice de Knightscope, ils ont un très bon accueil et reçoivent même des câlins.

Le business model de Knightscope pour les K5 est MaaS, Machine-as-a-Service, et coûte 4 500 dollars par mois, pour un service 24h/24 et 7jr/7 soit 6,25 dollars de l'heure.

Toutes ressemblances avec Dalek de Docteur Who est fortuite…

Réagissez à cet article

Source : *Des robots contre le crime dans la Silicon Valley – Ere Numérique*

FIC 2016 les 25 et 26 janvier 2016 sur le thème de la sécurité des données

#FIC 2016 les 25 et 26 janvier 2016 sur le thème de la sécurité des données

Pendant longtemps, la sécurité des données se confondait avec celle de la sécurité des systèmes d'information. Or la décorrélation croissante entre le contenant (support physique ou applicatif) et le contenu en raison de l'émergence des technologies de virtualisation, du « cloud computing » et de nouveaux modèles économiques change aujourd'hui la donne. La donnée est devenue un « objet » à part entière qui s'appréhende indépendamment de son support.

Axe 1 : les données, carburant de la transformation numérique.

Les données sont omniprésentes et multiformes : on peut citer les données personnelles, sociales, médicales, bancaires, d'entreprises, de géolocalisation, de sécurité, de dossiers passagers (PNR) etc. Cette compartimentation en fonction des usages ou des secteurs d'activité a-t-elle cependant encore un sens ? Comment gérer l'information indépendamment des supports utilisés ? Au-delà de la métaphore, les données constituent-elles véritablement un « nouvel or noir » ?

Axe 2 : la maitrise des données, enjeu de souveraineté

Posséder une « industrie de la donnée » puissante est un atout essentiel dans la compétition mondiale et une composante importante de toute stratégie de puissance. Or l'Europe apparait de ce point de vue en net retrait par rapport aux Etats-Unis. Forte consommatrice de numérique, la faiblesse de son offre locale la conduit à exporter massivement ses données, principalement aux Etats-Unis. Comment passer d'une « Europe offerte » à une Europe « ouverte » ? Quelle est la situation des autres continents ? Peut-on parler de « géopolitique des données » ?

Axe 3 : les données, un capital menacé

Si les attaques en déni de service visent les infrastructures elles-mêmes, les données sont souvent l'objectif ultime des attaquants, qu'il s'agisse de cybercriminalité (vol d'information, crypto-locking…) ou d'espionnage. Quelles sont les dernières tendances observées ? Quels sont les modes opératoires des cybercriminels ? Comment calculer la valeur de ses données pour engager des poursuites ?

Axe 4 : droit et données

La donnée est une notion immatérielle qui soulève de nombreuses questions au plan juridique. Peut-on appliquer la notion de propriété à la donnée, notamment à la donnée personnelle ? Quel lien entre données et territoire ? Comment mettre en œuvre efficacement le droit à l'oubli aujourd'hui consacré dans certains pays ? Comment définir le vol de données au plan pénal ?

Axe 5 : quelles stratégies de sécurité des données pour l'entreprise ?

Pour les entreprises, la sécurité des données repose sur une approche globale impliquant : classification des données, évaluation des données, analyse de risques, définition et mise en œuvre d'une stratégie de sécurité. Le développement du cloud computing et l'externalisation croissante de l'IT soulèvent à cependant de nombreuses questions. Peut-on utiliser « en toute sécurité » un CRM ou un ERP dans le Cloud ? Quelles conséquences en termes de maîtrise des données ? Comment assurer les risques liés aux données ?

Axe 6 : quelles technologies pour sécuriser les données ?

Le responsable sécurité des systèmes d'information dispose aujourd'hui d'une vaste bibliothèque d'outils et de technologies lui permettant de sécuriser ses données, qu'il s'agisse d'outil de protection, de destruction sécurisée, de détection de fuites d'information ou d'investigation. La vitesse du progrès technologique et le « time to market » imposé par le marché aux éditeurs sont-elles compatibles avec les cycles d'adoption relativement lents des organisations ? Compte tenu de ce même « time to market », comment intégrer la sécurité de façon native (security by design) dans les applications à disposition des utilisateurs ?

Axe 7 : données et enjeux sectoriels

La transformation numérique et les données qui la nourrissent irriguent l'ensemble des secteurs économiques et des activités humaines. Les données sont ainsi au cœur de la « smart revolution » qui touche aussi bien l'individu dans sa vie quotidienne, la collectivité ou l'entreprise au travers des objets connectés et de « l'informatique omniprésente ». Quels sont les enjeux liés aux données dans la « ville intelligente », « l'usine du futur », le monde médical etc. ?

Axe 8 : enjeux sociétaux et éthiques liés aux données.

La transformation numérique, et la croissance exponentielle des données qu'elle génère, constituent à n'en pas douter des opportunités. Mais la rapidité de cette évolution et ses conséquences majeures sur l'Homme militent également pour une certaine prise de recul et un questionnement éthique et philosophique. Au plan individuel, que signifie désormais la notion de « vie privée » ? Est-il également possible de replacer l'utilisateur au cœur de cette transformation en lui permettant de se réapproprier « ses » données ? Faut-il enfin imaginer, sur le modèle de la loi bioéthique, une loi sur l'éthique numérique fixant un cadre pour l'exploitation des données à des fins prédictives ou à des fins de surveillance ?

Réagissez à cet article

Source : *Le FIC 2016 aura lieu les 25 et 26 janvier 2016 sur le thème de la sécurité des données | Observatoire FIC*

Retard pour la plateforme nationale des interceptions judiciaires

Retard pour la plateforme nationale des interceptions judiciaires

---

plateforme nationale des interceptions judiciaires (PNIJ) a du plomb dans l'aile. Pour remédier au retard de son déploiement, le gouvernement a décidé de reporter l'abrogation du STIJ, le système de transmission des informations judiciaires qu'elle doit remplacer.

Créé par un décret du 30 juillet 2007, le fichier STIJ permet « *aux magistrats et aux officiers de police judiciaire de disposer des données de trafic des correspondances interceptées (numéros de téléphone, date, heure et durée de l'appel, etc.) ainsi que des contenus des messages (SMS, MMS) émis ou reçus par un numéro de téléphone dont la ligne est surveillée* » , résumait la CNIL en 2014.

Ce dispositif n'était que temporaire. Il devait être remplacé par la plateforme nationale des interceptions judiciaires six mois après l'entrée en vigueur de celle-ci et au plus tard au 31 décembre 2015. La PNIJ a en effet pour mission de centraliser le recueil des données de connexion et des interceptions de correspondances décidés par un juge. Elle tranche avec les pratiques jusqu'alors en vigueur « *où les dispositifs d'interception des communications électroniques et les réquisitions de données de connexion reposaient sur un système hétérogène et décentralisé* » dixit la CNIL.

Report d'un an

Seulement, il faut croire que le passage de relais ne se passe pas aussi bien que prévu. Hier, au Journal officiel, le gouvernement a en effet décidé de reporter l'abrogation du STIJ au 31 décembre 2016. Pour comprendre pourquoi, il faut lire la délibération de la CNIL publiée à cette occasion.

Selon la Commission, la version actuelle de la PNIJ « *ne permet pas techniquement de traiter les données prévues à l'article R. 40-46-2° du Code de procédure pénale* », c'est-à-dire les données faisant l'objet d'une mesure de géolocalisation en temps réel. Autre fonctionnalité en souffrance, dont la Commission révèle l'existence : « *la fonction de reconnaissance vocale du locuteur n'est pas disponible* ». Bref, de nouveaux développements sont nécessaires pour parfaire ce chantier, des travaux qui prendront plusieurs mois.

Un passage de relais délicat

Le basculement du STIJ à la PNIJ devra aussi être l'occasion d'un gros ménage puisque la CNIL a interdit que les données de l'un soient reprises par l'autre. Il faudra donc organiser un effacement, en tenant compte des différentes durées de conservation. Un exercice rendu d'autant plus complexe par l'éparpillement des informations sur les postes de travail des enquêteurs.

Rappelons que la plateforme nationale des interceptions judiciaires, située dans les locaux du géant Thales, est placée sous le contrôle d'une personnalité qualifiée (article R40-53 du Code de procédure pénale). C'est Mireille Imbert-Quaretta, l'ancienne présidente de la commission de protection des droits à la Hadopi, qui occupe désormais ce poste pour une durée de cinq ans. Elle devra établir un rapport annuel qu'elle adressera au garde des sceaux, ministre de la justice. Sur cette question, la CNIL a déploré ne pas être destinataire de ce rapport, mais le ministère de la justice lui a promis de lui en adresser un exemplaire.

Réagissez à cet article

Source : *Du retard pour la plateforme nationale des interceptions judiciaires – Next INpact*

Le français Seolane détecte et neutralise les drones malveillants

Le français Seolane détecte et neutralise les drones malveillants

L'entreprise a développé une station fixe au sol qui détecte la signature électromagnétique de ces engins volants. Sa solution intègre aussi un drone volant fourni par le groupe Eca qui se chargera d'identifier et de filmer le pilote avec une caméra embarquée.

Ce drone intervient dès lors que la station fixe a détecté un drone malveillant. © Seolane

Le survol illégal de drones au-dessus de bases militaires, centrales nucléaires et autres sites sensibles a mis à jour la nécessité d'identifier et de neutraliser les intrus. « *Ce marché devrait peser d'ici cinq ans entre 500 millions et un milliard d'euros* », estime Wilfrid Rouger, le fondateur et directeur général de Seolane une PME française créée en 2007 à Maisons-Laffitte (Yvelines).
Constituée d'une dizaine de personnes, l'entreprise est spécialisée dans l'intégration de systèmes de détection de signaux et de géolocalisation pour le transport et la sécurité. Le mois dernier, elle a remporté la première édition du concours Startup Challenge organisé le mois dernier par le salon Milipol, dédié à la sûreté des Etats.
Le prix récompense sa solution Dronelnt qui détecte, caractérise, traque et neutralise les drones malveillants avec une station fixe au sol. En cas de survol illégal d'un site, cette dernière va détecter la signature électromagnétique du drone et le localiser par radiogoniométrie. Une technique qui recourt à plusieurs capteurs pour localiser la position du drone par triangulation.

Drone fourni par Eca.

« *Nous avons lancé ce développement technologique il y a deux ans* », indique Wilfrid Rouger. Ce dernier a noué un partenariat avec le groupe Eca qui fournit un drone d'intervention. Fonctionnant de concert avec la station au sol, ce dernier dispose d'une autonomie allant jusqu'à 1h30 selon le modèle. Pour identifier le pilote et le filmer, l'engin volant embarque une caméra qui fonctionne de jour comme de nuit.
« *Plusieurs tests ont été réalisés avec succès avec la Gendarmerie nationale sur différents sites dont une centrale nucléaire* », fait valoir le directeur général de Seolane qui reçoit des demandes provenant de sites Seveso, aéroports et autres bases militaires qui s'inquiètent de l'explosion annoncée des vols illégaux de drones et des menaces terroristes.

Réagissez à cet article
Source : http://www.expoprotection.com/site/FR/L_actu_des_risques_malveillance__incendie/Zoom_article,I1602,Zoom-c1901a7c9c9d76e3b257db6e81734942.htm
Par Eliane Kan

Géolocalisation des véhicules professionnels des employés : que faire si mon employeur ne respecte pas les règles ? | Le Net Expert Informatique

Géolocalisation des véhicules professionnels des employés : que faire si mon employeur ne respecte pas les règles ?

Vous avez plusieurs recours :
• Adresser une plainte à la CNIL : la CNIL peut contrôler tous les systèmes de géolocalisation installés en France. Si le contrôle confirme que l'employeur ne respecte pas les règles, il sera mis en demeure de respecter la loi, sous peine de sanctions ;
• Saisir les services de l'inspection du Travail de votre département ;
• Déposer une plainte pénale auprès du procureur de la République, des services de police ou de gendarmerie.
• Vous avez demandé à avoir accès aux informations de géolocalisation qui vous concernent et votre employeur a refusé ?

Vous pouvez, après un délai de 2 mois, adresser une plainte à la CNIL.

Même si remplir un formulaire de déclaration à la CNIL est gratuit et enfantin, il vous engage cependant, par la signature que vous apposez, à respecter scrupuleusement la loi Informatique et Libertés. Cette démarche doit d'abord commencer par un Audit de l'ensemble de vos systèmes de traitements de données. Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

S o u r c e :
https://cnil.epticahosting.com/selfcnil/site/template.do;jsessionid=06EF1A234FB5C655BF980F0F5D5C31E9?name=G%C3%A9olocalisation+des+v%C3%A9hicules+professionnels+des+employ%C3%A9s+%3A+que+faire+si+mon+employeur+ne+respecte+pas+les+r%C3%A8gles+%3F&id=339

Les objets connectés

deviendraient des témoins ? | Le Net Expert Informatique

Les objets connectés deviendraient des témoins ?

Aux Etats-Unis, on commence à produire les données de bracelets connectés pour démentir ou renforcer un témoignage. Ces données pourraient aussi entrer dans nos tribunaux, ce qui n'est pas sans poser question.

A quoi servent les objets connectés « portables », ces bracelets ou ces montres qui permettent de mesurer votre activité physique, vos dépenses en calories et même parfois votre humeur ?
A mieux se connaître, répondent les amateurs. A mener une vie plus saine. Mais une histoire récente, aux Etats-Unis, montre que ces objets peuvent aussi servir lors de votre procès.

Et là, son FitBit a lâché le morceau
Une femme de 43 ans qui avait porté plainte pour viol a été démentie par les données de son FitBit (bracelet connecté mesurant l'activité et le sommeil). L'histoire a été rapportée la semaine dernière par la chaîne d'information locale ABC 27 News.
La femme avait affirmé aux enquêteurs qu'un homme s'était introduit au milieu de la nuit dans sa chambre et l'avait menacée avec un couteau avant de la violer. Mais son gadget a contesté ses dires :
« Elle avait affirmé qu'elle avait perdu sa montre de fitness en résistant à son agresseur, mais l'objet a été retrouvé intact dans le couloir, près de la salle de bains [où elle avait dit que s'était déroulé le viol, ndlr].
Selon le chef d'inculpation, quand les enquêteurs ont téléchargé son activité de fitness, ils se sont aperçus que la femme n'avait pas dormi cette nuit-là et qu'elle avait marché tout le temps, au lieu de dormir comme elle l'avait affirmé. »
En plus de ces données, les enquêteurs n'ont trouvé aucune trace de pas dans la neige autour de la maison (les faits se sont déroulés en mars) ni aucune trace d'intrusion. En conséquence, la femme a été inculpée pour fausse déclaration et altération de preuves.

Des grosses balances, ces Google Glass
Déjà, en novembre 2014, à Calgary (Canada), une femme, qui demandait à être indemnisée pour préjudice corporel après un accident, a utilisé les données de son bracelet connecté pour prouver que son activité physique était réduite depuis son accident. (Une histoire alors analysée par Olivier Ertzscheid.)

Les objets connectés arrivent donc dans les tribunaux. Et selon les avocats cités dans la presse américaine (ici ou ici, par exemple), cette tendance est appelée à grandir. Dans Wired, un avocat américain se demandait ainsi :
« [Les données des objets connectés] pourraient-elles être utilisées comme alibi ? »
Ou encore :
« Est-ce qu'on pourrait utiliser les données d'un FitBit pour prouver qu'un cardiologue avait fait preuve de négligence, en ne restreignant pas l'exercice d'un patient ? »
Ces objets peuvent donner des indications sur les activités de celui ou celle qui le porte, mais aussi sur le lieu où il ou elle se trouve, grâce à des fonctions de géolocalisation. Les plus sophistiqués, comme les Google Glass, font aussi des photos ou des vidéos, ainsi que des recherches sur le Web.
On voit bien l'usage que policiers, assureurs ou autres pourraient faire de ces données, en les retournant contre son propriétaire.

Bientôt dans nos prétoires
En France, le cas ne s'est encore jamais présenté, mais, explique Me Clarisse Le Corre, avocate au cabinet Vigo, il est tout à fait envisageable :
« Selon la loi, les infractions peuvent être établies par tous modes de preuve et c'est le juge qui décide ensuite selon son intime conviction. »
A cheval entre données personnelles et données médicales, ces informations sont souvent appelées « données de bien-être ». Elles sont protégées par la loi « Informatique et libertés », mais dans le cas d'un procès, cette protection peut être levée par l'instruction.
Pourvu qu'elles soient légalement recevables et qu'elles soient ensuite soumises au contradictoire, c'est-à-dire être débattues par les deux parties, les données des objets connectés peuvent tout à fait être présentées devant un tribunal.

Leurs données sont-elles fiables ?
Pourtant, ces données sont loin d'être totalement fiables.
Les objets connectés buguent.
Comme l'a récemment montré notre collègue Thibaut Schepman, les appareils connectés peuvent buguer et les données récoltées ne reflètent pas forcément vos activités.

Ils sont faciles à duper.
Pas besoin de réfléchir longtemps pour voir comment on pourrait duper le bracelet connecté : il suffit de le faire porter par un complice ou de l'apposer à un animal domestique au comportement pas trop erratique. Ou encore de rester assis à son bureau en bougeant les pieds très vite pour faire croire qu'on fait un jogging.

Ils « mesurent » selon des critères qui changent de machine en machine et sont déterminés par des algorithmes inaccessibles.
Comme le rappelle la chercheuse américaine Kate Crawford dans The Atlantic, les mesures qu'effectuent ces outils dépendent de la façon dont ils ont été programmés et sont souvent imprécises.

« Le Jawbone UP, Nike Fuelband, FitBit and Withings Pulses [différents modèles de bracelets connectés, ndlr] ont chacun des modes de fonctionnement particulier : certains comptabilisent les mouvements de bras comme de la marche (merveilleux, si vous voulez comptabiliser l'écriture comme de l'exercice), d'autres comptabilisent difficilement le vélo comme une activité physique.

La fonction de mesure du sommeil emploie des méthodes assez grossières pour faire la différence entre sommeil léger et sommeil profond. […] »

Un bracelet Jawbone Up (Ashley Baxter/Flickr/CC)

La chercheuse ajoute, faisant référence à l'exploitation de ces données :
« Ces données sont rendues encore plus abstraites par des entreprises d'analytique qui créent des algorithmes propriétaires, pour les comparer à leur standard de ce qu'est une personne normale "en bonne santé." »

Effectivement, explique Me Le Corre, à mesure que l'on s'interroge sur le statut de ces objets, on découvre leurs limites :

« La question de la fiabilité des données de ces objets va se poser de façon aiguë. Pour l'instant, nous manquons de recul sur ces choses-là parce qu'elles sont très récentes. D'où l'intérêt de le soumettre à la discussion des deux parties, qui sert de garde-fou. »

Les données par elles-mêmes ne signifient rien : elles s'intègrent dans un faisceau de preuves, et doivent toujours être contextualisées.

Au-dessus des témoins humains…
En voyant les données de bien-être utilisées contre leur propriétaire, on comprend aussi mieux ce que sont vraiment les objets connectés.
Ainsi, réfléchissant sur ce thème, la chercheuse Kate Crawford, qui travaille sur les implications du big data et des objets connectés, rappelle l'ambiguïté fondamentale des objets connectés :

– ils se présentent comme les instruments d'une meilleure connaissance de soi,
– mais sont aussi des « informateurs », qui collectent des données et les transmettent au fabricant et à des tiers – potentiellement à des assureurs et des employeurs.
Plus profondément, c'est le statut que l'on veut donner à ces données qui est en jeu. Kate Crawford met en garde contre la tentation d'une « vérité fondée sur les données », où celles-ci finiraient par sembler plus fiables – parce que plus neutres – que l'expérience des témoins.

« Donner la priorité aux données, qui sont irrégulières et peu fiables, sur les témoignages humains, cela signifie que l'on donne le pouvoir à l'algorithme. Or ces systèmes sont imparfaits – comme peut l'être le jugement humain. »

Les données des objets connectées ne sont que ça, des données : des mesures qu'il faut contextualiser et comprendre, et surtout ne pas prendre pour argent comptant.

Source : http://rue89.nouvelobs.com/2015/07/01/quand-les-objets-connectes-temoignent-a-proces-contre-260040