Mobile strategies increase need for data loss prevention technology in Europe

Mobile strategies increase need for data loss prevention technology in Europe

Data loss prevention technology that covers all popular mobile platforms and is easy to use and implement is called for as mobile strategies evolve

Mobile has entered business strategy from two directions. The business wants to grab the opportunity to better serve the mobile masses, while employees want to mobile devices as part of their work
This has created an environment that security teams have had to come to terms with quickly.

Roman Foeckl, CEO at security supplier CoSoSys, says the increasing number of mobile devices in the enterprise, and new versions of an operating system, is forcing organisations to rethink ways of securing corporate data.
It is not just about mobile the applications, he says, but also how employees interact with other organisations and people. Mobile provides low-cost computing power that is available to everyone and enables staff to collaborate with others, but this is a recipe for security breaches in businesses.
Foeckl says traditional security is irrelevant in many cases. For example, he says the shift from open file systems (Windows 7) to application sandboxes (Android, iOS, Windows Phone/Pro/RT), is making traditional antimalware, especially antivirus, less relevant.
For example, on iOS, there is little need for antimalware or antivirus products because neither they, nor any other app on the device, can access another app's storage or memory.
According to Foeckl, when planning a mobile security strategy there is no one size fits all: "Every company has to choose a cross-platform solution that works on Apple iOS, Android mobile devices, Windows, Mac OS X and Linux computers to cover the entire fleet of workstations."
Sufficient resources for data loss protection
But what are companies doing to incorporate endpoint and mobile security tools in applications to make sure they are secure?
"This can be achieved by implementing data loss prevention (DLP) features into applications and more," says Foeckl. "However, the administrators have to be sure that IT resources under their control are ready to co-operate with advanced features like file tracing and file shadowing."

With DLP, the amount of data being monitored and the number of copies stored could quickly absorb a sizeable chunk of the available IT resources.
"In European countries, sometimes we are faced with the situation that a CIO or administrator evaluates resources as insufficient for DLP use," says Foeckl. "In such cases it is recommended to look at cloud-managed DLP and mobile device management [MDM] that offer easy evaluation, implementation and scalability. It's also a good way to safely reap the benefits of the cloud protecting data."
In central and eastern European countries, one obstacle is the fact that many companies still prefer their own datacentres or computing power over cloud services, says Foecki.

Authorisation and security awareness
The software being used in enterprises is changing, so security teams must understand different security features and their limitations.
Foeckl says CoSoSys increasingly supports Macs and iOS devices. It has experience with preventing data breaches that could happen with the use of Google Drive, One Drive, Dropbox, on Windows and Mac OS X computers, for example.

Réagissez à cet article

Source : *Mobile strategies increase need for data loss prevention technology in Europe*

2700 sites Internet suspects passés à la loupe par le ministère de l'Intérieur

2700 sites Internet suspects passés à la loupe par le ministère de l'Intérieur

---

Le ministère de l'Intérieur a présenté au ministère des Technologies de la Communication et de l'Économie Numérique, 2700 requêtes sur des sites et des pages suspectés de prôner le terrorisme, a indiqué ce lundi 28 décembre sur les ondes de Mosaique FM, le ministre des TICS, Noômane Fehri.

Selon le ministre, plusieurs pages sur les réseaux sociaux ont été par ailleurs supprimées sur demandes présentées aux entreprises internationales comme Facebook.
Il a cependant précisé que des sites n'ont pas été supprimés ni masqués afin de pouvoir en extraire des renseignements et de suivre à la trace leurs administrateurs.

Réagissez à cet article

Source : *Cyberterrorisme : 2700 sites suspects ont été passés à la loupe par le ministère de l'Intérieur*

Les juges antiterroristes veulent recourir à des hackers

Les juges antiterroristes veulent recourir à des hackers

Interrogé par les sénateurs, le vice-président chargé de l'instruction à la section antiterroriste du TGI de Paris a demandé que les magistrats puissent recourir à des « experts » (comprendre des hackers) pour installer des mouchards sur les ordinateurs de suspects, puisque l'État ne veut pas fournir ses propres outils utilisés par les services de renseignement.

Interrogé par les sénateurs, le vice-président chargé de l'instruction à la section antiterroriste du TGI de Paris a demandé que les magistrats puissent recourir à des « experts » (comprendre des hackers) pour installer des mouchards sur les ordinateurs de suspects, puisque l'État ne veut pas fournir ses propres outils utilisés par les services de renseignement.
Le Sénat conduisait le 9 décembre dernier différentes auditions à huis clos dans le cadre du Comité de suivi de l'état d'urgence, mis en place pour s'assurer que l'État n'abuse pas des pouvoirs spéciaux confiés à la suite des attentats du 13 novembre 2015, et pour tirer des enseignements sur les pratiques et les obstacles rencontrés par les spécialistes de l'anti-terrorisme. Le Sénat a rendu public le compte-rendu d'audition, qui permet d'en savoir plus sur les attentes des juges.
Les sénateurs ont en effet entendu David Bénichou, le vice-président chargé de l'instruction à la section antiterroriste et atteintes à la sûreté de l'État au tribunal de grande instance de Paris. Celui-ci a vivement critiqué le manque de moyens des juges pour prévenir les actes de terrorisme, en demandant que les magistrats disposent de pouvoirs légaux et de moyens technologiques beaucoup plus proches de ceux dont disposent la police et en particulier les services de renseignement.

Une justice antiterroriste sert-elle à compter les morts ?

Alors que le rôle premier de la police est traditionnellement d'empêcher la commission des infractions, et le rôle de la justice est de les punir, M. Bénichou réfute l'opposition. « Une justice antiterroriste sert-elle à entraver des attentats ou à compter les morts en offrant à leurs auteurs une tribune, et à leur payer un avocat ? », a-t-il lancé. « Nous préférons prévenir les attentats. Pour cela, il nous faut des moyens opérationnels, performants et actualisés ».
Le magistrat a ainsi formulé deux demandes principales. Tout d'abord, il souhaite que les juges puissent saisir les e-mails archivés des suspects dans le cadre d'enquêtes préliminaires, sans que les personnes concernées soient prévenues. Actuellement les juges doivent se contenter de mettre sur écoute les boîtes emails des suspects pour collecter les correspondances reçues ou envoyées à un instant T, mais ils ne peuvent pas collecter ce qui a été émis ou reçu dans le passé (ce qu'a rappelé la cour de cassation le 8 juillet 2015). Le seul moyen d'obtenir copie des e-mails passés est de réaliser une perquisition, ce qui en droit oblige à prévenir le suspect qu'il fait l'objet d'une enquête, et à lui faire assister à la perquisition.
Ensuite, le magistrat demande à pouvoir installer des mouchards informatiques chez les suspects. En théorie cette capacité à capter à distance des données grâce à un dispositif installé localement (clé USB ou autre) ou injecté par une attaque informatique existe déjà en droit, depuis la loi Loppsi de 2011. Elle autorise les juges d'instruction à faire « mettre en place un dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, les conserver et les transmettre, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données ou telles qu'il les y introduit par saisie de caractères ».

Recourir à des hackers ou aux services de l'État

Mais dans les faits, comme nous l'avions déjà signalé en 2013, les juges n'ont pas accès aux outils théoriques. Les services de l'Agence nationale de sécurité des systèmes d'information (ANSSI) doivent en effet homologuer les outils mais selon le juge Bénichou, seuls deux outils ont été validés depuis 2011, et pour une raison inconnue, « le ministère de la justice ne les a toujours pas mis à notre disposition ».
« Les services de renseignement monopolisent les outils et ne les mettent pas à notre disposition, par crainte de les voir divulgués. Ils ont pourtant une durée de vie très courte », regrette le magistrat antiterroriste.
David Bénichou demande donc que les juges antiterroristes puissent faire appel à des « experts » extérieurs pour développer de tels outils, c'est-à-dire à des hackers à qui le magistrat passerait commande en fonction des besoins du moment. « Un amendement du Sénat autorisant le juge à commettre un expert pour développer un outil a malheureusement été retiré, le ministre de l'intérieur invoquant la sécurité du système d'information de l'administration », rappelle le juge.

Les services de renseignement monopolisent les outils

Or, « contrairement au contre-espionnage, la lutte contre le terrorisme est avant tout un problème judiciaire : nous avons un besoin opérationnel constant de ces éléments ». « C'est pourquoi je vous suggère de redéposer cet amendement », a-t-il demandé aux sénateurs.
Depuis 2014, la loi autorise potentiellement la police judiciaire à faire appel à des hackers, mais uniquement dans un cadre de perquisitions pour obtenir l'accès à des données chiffrées ou inaccessibles sur le matériel saisi. L'article 57-1 du code de procédure pénale permet en effet aux officiers de la PJ de « requérir toute personne susceptible d'avoir connaissance des mesures appliquées pour protéger les données auxquelles il est permis d'accéder dans le cadre de la perquisition » ou pour « leur remettre les informations permettant d'accéder aux données mentionnées ».
À défaut de pouvoir avoir accès à ces mêmes personnes dans le cadre de mises sur écoute ou de piratage à distance des données, le magistrat souhaite pouvoir recourir aux services du Centre Technique d'Assistance (CTA), qui sert déjà aux magistrats dans les affaires les plus graves, lorsqu'ils doivent déchiffrer un contenu saisi par les enquêteurs. Le CTA met à la disposition de la justice ses analystes et ses supercalculateurs pour décrypter les contenus, sans que la justice ne sache quels moyens techniques ont été utilisés pour obtenir la version en clair.

Réagissez à cet article

Source : *Les juges antiterroristes veulent recourir à des hackers – Politique – Numerama*

Quels sont les gadgets de la NSA utilisés par la police ?

Quels sont les gadgets de la NSA utilisés par la police ?

The Intercept a pu mettre la main sur un catalogue de périphériques utilisés par les agences américaines de renseignement pour espionner et collecter des données. Un inventaire digne de James Bond. Des questions se posent quant à la légalité de ces appareils et la nécessité d'encadrer leur utilisation par la justice.

A vos portefeuilles ! En effet, les équipements présentés par *The Intercept* et que l'on peut découvrir à cette adresse ne sont accessibles ni à toutes les bourses ni à tous les quidams. Il s'agit en effet d'appareils particulièrement sophistiqués qui permettent aux agences américaines, et tout particulièrement la NSA, de se livrer à leurs activités d'écoute et de surveillance. Certains de ces appareils sont fixes alors que d'autres peuvent être installés dans des automobiles, avions ou drones. Ces différents appareils portent des noms évocateurs comme Cyberhawk, Yellowstone, Blackfin, Maximus, Cyclone ou encore Spartacus. Selon notre confrère, un tiers de ces équipements n'auraient jamais été décrits publiquement jusqu'à présent.

Les possibilités sont différentes selon les appareils. Certains sont destinés à cibler 10000 identifiants téléphoniques différents. La plupart sont capables de géolocaliser les personnes ciblées et, selon les modèles, des fonctions plus avancées comme l'écoute des appels ou la capture des SMS sont proposées. Deux modèles permettent de récupérer les fichiers contenus sur les smartphones ainsi que les carnets d'adresses, notes ou encore récupérer les messages préalablement supprimés.

Spoofing d'adresses

L'un des appareils les plus répandus est le StingRay qui est utilisé pour récupérer les conversations en se faisant passer pour les relais officiels des opérateurs mobiles comme Verizon, AT&T et autres. Cette technique d'interception, baptisée Spoofing, est aujourd'hui largement répandue non seulement par les agences de renseignement mais également par la police fédérale ou municipale. Et c'est là que les défenseurs des libertés individuelles commencent à se faire entendre, arguant que l'utilisation de ces appareils n'est pas suffisamment encadrée et que des dizaines de milliers de personnes voient leurs conversations espionnées au seul motif qu'elles se trouvent dans une même zone géographique qu'une personne suspectée et écoutée.

Stingray I/II

Ground Based Geo-Location (Vehicular)

"Ensnares bystanders, drains batteries, blocks calls"

Review by Nathan Wessler

$134,952.00

Le 4ème amendement mis à mal

Les défenseurs de la vie privée expliquent que l'utilisation de ces appareils, dans des conditions pas ou trop peu encadrées, viole le 4ème amendement de la constitution américaine. En effet, dans un premier temps, ces différents appareils, et tout particulièrement le StingRay commercialisé par la société Harris, était essentiellement utilisé à des fins militaires ou par des agences fédérales. Cependant à partir de 2007, l'usage croissant fait par les polices municipales a commencé à poser problème car cette utilisation semble s'effectuer hors de tout cadre juridique. *The Intercept* prend l'exemple de la police de Baltimore qui a utilisé le StingRay plus de 4300 fois depuis 2007. Comme à l'habitude, la lutte contre le terrorisme sert de viatique à l'emploi de ces appareils et techniques de surveillance. Toutefois, cet argument laisse trop souvent à désirer. En effet, nos confrères citent le cas de la police de l'Etat du Michigan qui a employé 128 fois le StingRay l'année dernière dans le but d'identifier la localisation physique d'une personne suspectée de terrorisme mais l'Association de défense des libertés civiles a précisé que sur les 128 utilisations aucune n'avait un quelconque rapport avec un acte terroriste.

Des fonds douteux utilisés pour les acquérir

Plus ennuyeuses encore sont les modalités d'acquisition de ces appareils. En effet, puisqu'ils sont achetés « hors la loi », les fonds utilisés sont également hors la loi et proviendraient de saisies financières lors des découvertes de trafics en tous genres, de drogue notamment. *The Intercept* écrit que les forces de police de l'Illinois, du Michigan et du Maryland ont utilisé des fonds d'origine crapuleuse pour procéder à leurs achats. L'accusation est particulièrement grave puisque cela revient à accuser les services de police de blanchiment d'argent sale pour mener des opérations notoirement illégales.

Dans ces conditions, un certain nombre de juges américains s'alarment des dérives et souhaitent une évolution de la loi encadrant l'utilisation de ces appareils. Au mois de novembre dernier, le juge fédéral de l'Illinois, Iain Johnston a publié un mémorandum sur la manière dont avaient été utilisées ces techniques de spoofing dans une enquête autour d'un trafic de drogue. « *Un simulateur de ce type est simplement trop puissant et les informations capturées sont trop vastes pour que l'autorisation d'emploi ne soit pas délivrée par une cour dûment habilitée* ».

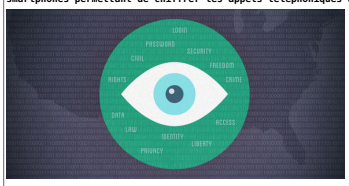
Réagissez à cet article

Source : *Les gadgets de la NSA utilisés par toute la police*

Des communications téléphoniques sécurisées avec Signal

Des communications téléphoniques sécurisées avec Signal

A 23 ans, Frederic Jacobs est déjà une célébrité dans le milieu de la cryptologie. Ce jeune Belge, étudiant-chercheur à l'Ecole polytechnique de Lausanne (Suisse), est l'un des trois créateurs de Signal, une application gratuite pour smartphones permettant de chiffrer les appels téléphoniques et les SMS.



À 23 ans, Frederic Jacobs est déjà une célébrité dans le milieu de la cryptologie. Ce jeune Belge, étudiant-chercheur à l'Ecole polytechnique de Lausanne (Suisse), est l'un des trois créateurs de Signal, une application gratuite pour smartphones permettant de chiffrer les appels téléphoniques et les SMS.

Les communications entre deux appareils équipés de Signal passent par l'Internet ouvert, mais restent indéchiffrables pour tout observateur extérieur. N'importe quel possesseur de smartphone peut ainsi disposer, sans formalités ni inscription, d'un service naguère réservé aux chefs d'Etat, aux PDG de multinationales et aux agents secrets.

La nouveauté de Signal est que l'on n'a pas besoin d'être un « geek » pour s'en servir : une fois l'application chargée, tout se fait automatiquement. « Les systèmes précédents en demandaient trop aux utilisateurs, relève Frédéric Jacobs. C'est pour ça que jusqu'à présent, le grand public a très peu utilisé le chiffrement. » Il fait allusion à PGP (Pretty Good Privacy), inventé il y a 25 ans par l'Américain Philip Zimmermann, pionner mondial du chiffrement sur Internet.

PALLIER LA DIFFICULTÉ DU CHIFFREMENT

Outre la facilité d'utilisation, l'autre objectif prioritaire de Signal était de proposer un chiffrement intégral, de bout en bout. « Le cryptage et le décryptage se font à l'intérieur de votre téléphone, explique Frederic Jacobs. Quand vous chargez l'application, elle crée automatiquement une centaine de clés de chiffrement, qui restent stockées dans l'appareil. »

Le système permet une rotation systématique : « Chaque clé servira une seule fois. Quand vous recevez un message, vous utilisez une clé qui se détruira aussitôt, et quand vous envoyez un message, l'application crée une nouvelle clé. De cette façon, si un attaquant voulait casser le chiffrement de vos communications, il serait obligé de recommencer le travail pour chaque message. Et s'il s'emparait d'une clé, il ne pourrait pas lire vos vieux messages. »

Frédéric Jacobs travaille avec deux développeurs américains installés à San Francisco : Moxie Marlinspike, un vétéran du chiffrement sur mobile qui a vendu sa première startup à Twitter, et Lilia Kai, ex-militante de l'Electronic Frontier Foundation, association de défense des libertés numériques. Au total, l'équipe permanente de Signal se compose de cinq personnes. Elle est financée par des fondations américaines engagées dans la défense des libertés sur Internet, notamment la Freedom of the Press Foundation et l'Open Technology Fund.

Le budget reste serré, et les salaires modestes. Pour gagner correctement sa vie, Frederic Jacobs travaille comme consultant informatique pour des entreprises. A court terme, cet arrangement le satisfait : « A aucun moment je n'ai pensé à m'enrichir grâce à Signal. Auparavant, j'ai travaillé dans des startups, mais j'ai vite été dégoûté par l'ambiance. Aujourd'hui, je fais partie d'une organisation libérée de l'influence perverse de l'argent. Et rassurez-vous, nous n'allons pas nous vendre à Google. »

UN LARGE PUBLIC EN ALLEMAGNE ET AUX ÉTATS-UNIS

En ces temps d'état d'urgence et de guerre contre le terrorisme, les créateurs de logiciels de chiffrement se sont fait des ennemis puissants, depuis le directeur du FBI jusqu'au premier ministre britannique. De plus en plus, les responsables politiques et policiers exigent que les développeurs créent des backdoors (portes de derrière), par exemple des systèmes permettant de récupérer les clés de chiffrement d'utilisateurs visés par des enquêtes.

Frederic Jacobs assure que Signal ne possède aucune backdoor, et qu'il peut le prouver : « Notre code est en open source, disponible librement sur Internet. Tous les experts peuvent l'analyser et le décortiquer à loisir. » Il affirme aussi qu'à ce jour, Signal n'a subi aucune pression, officielle ou autre : « Personne n'est venu nous voir, peut-être parce que nous sommes encore peu connus. »

Signal ne donne pas de chiffre précis sur son nombre d'utilisateurs, mais l'application a été chargée plusieurs millions de fois. Les plus gros contingents sont aux Etats-Unis et en Allemagne : « Signal a été adopté par des hauts fonctionnaires, y compris à Washington, mais aussi par des familles ordinaires qui veulent protéger les communications de leurs enfants, ou des jeunes couples qui s'échangent des photos intimes… »

Signal dispose de dizaines de relais sur tous les continents. Fin décembre, les principaux se trouvaient aux Etats-Unis (côte est et côte ouest), en Allemagne, en Irlande, au Brésil, en Australie et à Singapour : « Leur nombre exact varie en fonction des besoins, explique Frederic Jacobs, ce sont des serveurs ordinaires, qui se louent à la minute. Si par exemple, le trafic est important en Allemagne vers 17 heures, nous ajoutons des relais locaux, et s'il baisse à 18 heures, nous en retirons. »

Signal possède aussi un serveur central, installé aux Etats-Unis, qui envoie les notifications aux appareils avant un appel. De ce fait, le système n'est pas complètement invulnérable. Si un attaquant réussit à avoir accès à un serveur, par effraction ou lors d'une perquisition, il ne pourra pas déchiffrer le contenu des messages, mais pourra s'emparer des informations techniques dont le réseau a besoin – origine et destination des messages, date et durée des appels… En ce sens, Signal n'a pas été pensé pour les lanceurs d'alerte qui doivent rester totalement inconnus des autorités.

Pour le reste, les cryptologues célèbres qui ont audité le code de Signal se sont dit impressionnés par sa qualité. La consécration la plus éclatante vient de Philip Zimmermann qui travaille aujourd'hui pour Silent Circle, société américaine offrant un service payant de chiffrement des communications, dont le siège social est en Suisse depuis 2014. Créée par des anciens membres des commandos d'élite de l'US Navy et visant une clientèle haut de gamme, ainsi que les militaires et les humanitaires en mission, Silent Circle, pour les messages-texte, a abandonné son ancien protocole de chiffrement, et a adopté celui de Signal.

Réagissez à cet article

Source : *Signal, une application pour téléphoner de manière sécurisée*

Un décret autorise les captations de données et de conversations Skype en temps réel

Un décret autorise les captations de données et de conversations Skype en temps réel

Dans le calme d'un dimanche précédent le début des vacances de Noël, le gouvernement a publié au Journal officiel un décret autorisant les forces de l'ordre à surveiller toutes les informations apparaissant sur l'ordinateur d'un suspect (de ses conversations Skype à ses sites consultés), dans le cadre de procédures judiciaires.
Permettre à des enquêteurs de capter en temps réel (et à distance) les données informatiques de suspects, c'est possible. Depuis le vote de la LOPPSI de 2011, l'article 706-102-1 du Code de procédure pénale autorise en effet les officiers et agents de police judiciaire à accéder et enregistrer des données « telles qu'elles s'affichent sur un écran » ou telles que l'utilisateur d'un ordinateur « les y introduit par saisie de caractères » – et ce à partir du moment où un juge d'instruction a émis une ordonnance motivée en ce sens, prise après avis du Procureur de la République.
Cette procédure, activable uniquement pour des crimes et délits relativement graves (terrorisme, association de malfaiteurs, meurtre, crime de fausse monnaie, escroquerie ou prêt illicite de main d'œuvre en bande organisée, etc.), a même été élargie suite à l'adoption de la loi anti-terroriste de novembre 2014 aux données « reçues et émises par des périphériques audiovisuels ». L'objectif ? Pouvoir capter aussi les sons, comme ceux d'une conversation Skype par exemple.

Captation de tout ce qui apparaît à l'écran, les conversations Skype, etc.
Avec ce décret entré en vigueur ce lundi 21 décembre 2015, le gouvernement vient de permettre l'application de ces dispositions en autorisant la création de traitements de données à caractère personnel, destinés à recevoir les fameuses informations extirpées par les forces de l'ordre dans ce type de procédures. « Les traitements autorisés par le présent décret permettent de collecter, enregistrer et conserver les données informatiques ainsi captées et de les mettre à la disposition des enquêteurs de la police et de la gendarmerie nationales comme de la douane judiciaire », précise le texte.
Les opérations, bien que placées sous le contrôle du juge, permettront aux services de se pencher sur « l'ensemble des données captées », y compris s'il s'agit de données personnelles sensibles. Toutes les informations enregistrées devront être « conservées dans le traitement jusqu'à la date de clôture des investigations ». À ce moment, poursuit le décret, elles seront « placées sous scellés fermés et effacées ». Une transcription des enregistrements effectuée par les forces de l'ordre devra néanmoins être transmise à l'autorité judiciaire, pour être versée au dossier de la procédure – en vue d'un éventuel procès.
En donnant son avis sur ce qui n'était alors qu'un projet de décret, la Commission nationale de l'informatique et des libertés (CNIL) prévenait l'exécutif que l'utilisation de tels dispositifs de surveillance risquait de conduire à la collecte de « données relatives à d'autres personnes que l'utilisateur [suspecté], telles que, par exemple, l'identité des personnes en relation avec l'utilisateur du système d'information surveillé ».

La gardienne des données personnelles affirmait par ailleurs que le gouvernement ne faisait pas explicitement référence à la mise en œuvre de dispositifs de reconnaissance vocale ni d'analyse comportementale des dynamiques de frappe au clavier (keylogging). « Si de tels mécanismes devaient à l'avenir être mis en œuvre, la commission devra être saisie pour avis sur un projet de décret modificatif prévoyant expressément le recours à de tels dispositifs » mettait-elle en garde.

Un dispositif qui n'était pas encore totalement opérationnel en avril dernier
Tout en regrettant « de ne pas avoir été destinataire de l'ensemble du dossier technique (…), certains éléments n'ayant été communiqués qu'à l'Agence nationale de la sécurité des systèmes d'information (ANSSI) », la CNIL soutenait qu'au moment de rédiger son avis, le dispositif prévu par le ministère de l'Intérieur « ne permet[tait] pas encore la captation de données émises ou reçues par des périphériques audiovisuels ». La délibération de l'autorité administrative indépendante date toutefois du 2 avril 2015, ce qui signifie que les choses ont pu grandement évoluer depuis…
La CNIL ajoutait néanmoins qu'elle prenait acte « que lorsqu'un nouveau dispositif aura été développé dans cette perspective, des informations complémentaires ser[aient] portées à sa connaissance ». Nous n'avons cependant pas réussi à joindre l'institution afin de savoir si elle avait depuis obtenu de nouveaux éléments.

Sur un plan technique, la CNIL expliquait qu'au regard des éléments à sa disposition, « la solution retenue pourra s'adapter à l'environnement applicatif des utilisateurs visés par une enquête (système d'exploitation, applications tierces, etc.). Des tests de fonctionnement seront exécutés afin de s'assurer de la correcte adaptation de l'outil à l'environnement de chaque utilisateur. Une procédure de suppression automatique de l'outil sur les terminaux informatiques visés est prévue. L'architecture de collecte sera en outre pourvue de mesures visant à assurer la sécurité et le cloisonnement des données collectées. »
Rappelons enfin que la récente loi sur le renseignement permet à de nombreux services d'utiliser des dispositifs intrusifs à l'insu des personnes surveillées (à l'image des ISMI catcher), sans toutefois qu'un juge soit cette fois mis dans la boucle…

Réagissez à cet article

Source : *Un décret autorise les captations de données et de conversations Skype en temps réel*

La SNCF va épier ses

voyageurs

La SNCF va épier ses voyageurs

Plutôt que de surveiller ses millions de passagers de la même façon, la SNCF va tenter de les filtrer au moyen d'un logiciel qui prétend isoler les comportements présentant un risque.

Face à la menace terroriste, la SNCF teste la réponse technologique. Dans quelques gares, la compagnie ferroviaire s'est déjà équipée d'un logiciel d'analyse du comportement des voyageurs au travers des caméras de vidéosurveillance existantes. À défaut de filtrer tous les passagers avec des portiques de sécurité tels que proposés par la ministre de l'Écologie, la société publique va essayer de détecter les attitudes suspectes.

Stéphane Volant, le secrétaire général de l'entreprise publique, a expliqué dans les grandes lignes à l'AFP le fonctionnement de ce logiciel, dont l'analyse se base sur « le changement de température corporelle, le haussement de la voix ou le caractère saccadé de gestes qui peuvent montrer une certaine anxiété ». Une vidéosurveillance qui se veut donc intelligente, mais qui risque de générer énormément de faux positifs.

Vers un nouveau cap dans la surveillance

Avec cette expérimentation – qui s'étendra aux colis abandonnés -, la SNCF veut aussi mesurer le niveau d'acceptabilité des voyageurs pour ce genre de technologie. Mais au quotidien, personne ne verrait jamais ces logiciels, puisque les caméras elles-mêmes ne différeront pas. Le seul changement perceptible pour le public sera peut-être le nombre d'interpellations préventives de gens à l'attitude jugée suspecte…

Vidéosurveillance gare

Alors que ces tests auraient vocation à durer et que ce logiciel – dont le nom n'a pas été révélé – pourrait être étendu aux 40 000 caméras de la SNCF, se pose la question de la protection de la vie privée. Sur ce point, la compagnie ferroviaire a déjà répondu que ces expérimentations sont menées sous le contrôle de la Cnil.

Dans sa boîte à outils sécuritaire, la société lancera au printemps prochain une application mobile pour les voyageurs afin qu'ils signalent un danger. La SNCF imagine aussi équiper ses agents de caméras. Quant aux portiques, ils seront adoptés pour l'accès aux trains Thalys, en réponse à l'attentat déjoué au mois d'août. Gageons que les trains qui arrivent en retard ne génèrent pas trop de hausse de température corporelle.

Réagissez à cet article

Source : *Surveillance : la SNCF va épier ses voyageurs*

Les objets connectés doivent-ils vraiment recueillir autant de données personnelles pour fonctionner correctement ?

	Les objets connectés doivent-ils vraiment recueillir autant de données personnelles pour fonctionner correctement ?

Télévision, pèse-personne, thermostat et autres hubs domotiques… les objets connectés tentent d'envahir nos maisons et de s'infiltrer au coeur même de leur réseau numérique.

Pourtant, malgré leur objectif de nous simplifier la vie, leur développement semble encore assez poussif ; en raison sans doute de leur manque criant de sécurité. C'est ce que révèle une étude menée par la division Sécurité de Hewlett Packard : rien de moins que 250 vulnérabilités ont été relevées par les experts d'HP Fortify au sein des 10 objets connectés les plus populaires.

Ces failles de sécurité seraient, selon Mike Amistead, le manager général d'HP Fortify, le symptome de la ruée des entreprises sur le créneau des objets connectés. Il estime en effet que les start-ups se lançant sur ce marché tenteraient de commercialiser leur produit le plus rapidement possible avant la concurrence… au mépris de la garantie d'un niveau de sécurité suffisant des réseaux et des données personnelles.

Vos données personnelles en clair sur la toile

Parmi les failles de sécurité relevées, HP a constaté que :

– 90 % des objets connectés étudiés solliciteraient une information personnelle sensible (ex : adresse email ou postale, nom, date de naissance, etc) ; une information ensuite véhiculée en clair sur la toile ;

– 70 % des objets connectés ne crypteraient pas les données échangées avec le réseau ;

– 80 % des objets connectés ne nécessiteraient pas de mot de passe complexe pour identifier les demandes de connexion tierces ;

– 60 % des objets connectés seraient vulnérables aux attaques dites de « cross-site scripting » (type de faille de sécurité permettant d'injecter du contenu dans une page, et provoquant ainsi des actions sur les navigateurs web visitant la page).

Réagissez à cet article

Source : http://www.archimag.com/vie-numerique/2014/07/30/objets-connectes-internet-failles-securite

Les CNIL européennes haussent le ton contre le pistage de Facebook

Les CNIL européennes haussent le ton contre le pistage de Facebook

Après une décision de la justice belge, d'autres pays européens réclament que Facebook cesse de traquer les internautes en dehors de ses pages.

Facebook n'est pas encore sorti du bourbier européen.

L'autorité française de protection des données (la CNIL) a publié lundi une déclaration commune avec quatre de ses homologues européens concernant les règles de confidentialité du réseau social.

Elle fait suite à une décision de la justice belge, qui a demandé à Facebook de ne plus tracer les internautes non-inscrits sur le site américain. L'entreprise a finalement obtempéré il y a une semaine, en empêchant toute personne sur le territoire belge déconnectée du site d'accéder à ses pages.

Pas encore suffisant pour les cinq CNIL des Pays-Bas, de la France, de l'Espagne, de Hambourg et de la Belgique, qui réclament la généralisation du dispositif. «Le groupe de contact attend de la société qu'elle se conforme à ce jugement sur tout le territoire de l'Union européenne», précise le communiqué.

Mesures de sécurité

En Belgique, la justice contestait l'utilisation par Facebook d'un «cookie», un micro-fichier qui conserve les données ou habitudes des internautes, baptisé «datr».

Principale critique: cette collecte concerne les personnes ne disposant pas de compte Facebook, et qui ne consentent donc pas à ce suivi. Il suffit de visiter une page du site (par exemple un évènement public) pour se voir déposer ce cookie sur son ordinateur et mobile. Facebook est ensuite capable de connaître les fréquentations en ligne de l'internaute, s'il se rend sur des sites contenant des modules du réseau social, comme le bouton «like».

De son côté, Facebook affirme qu'il collecte des cookies pour des raisons de sécurité. «Nous les utilisons afin de distinguer les véritables visites des fausses», expliquait la semaine dernière Alex Stamos, en charge de la sécurité chez Facebook. «Depuis cinq ans, ces cookies nous servent à empêcher la création de faux comptes, d'empêcher le vol de données ou l'organisation d'attaques par déni de service.» Facebook précise que ces cookies sont utilisés afin de surveiller le comportement d'un navigateur Web, et non d'un utilisateur précis. Pour Alex Stamos, «si le cookie nous informe qu'un navigateur a visité des centaines de sites en cinq minutes, cela nous indique qu'il s'agit probablement d'un robot».

Facebook a ajouté qu'il comptait faire appel de la décision de la justice belge et qu'il était prêt à discuter du sujet du cookie «datr» avec les autres autorités de protection des données.

Le groupe des CNIL européennes dénonce lui une «ingérence dans la vie privée des internautes» qui «n'est pas acceptable». Il réclame à Facebook de «prendre les mesures nécessaires pour se mettre en conformité avec la législation européenne, et ce sur tout le territoire de l'Union européenne.»

Le groupe enquête depuis presque un an sur les règles de confidentialité de Facebook. Ces investigations sont menées par chacune des CNIL, mais coordonnées par le groupe de contact. Leurs conclusions ne devraient pas être rendues avant l'année prochaine.

Réagissez à cet article

Source : http://www.lefigaro.fr/secteur/high-tech/2015/12/07/32001-20151207ARTFIG00299-les-cnil-europeennes-haussent-le-ton-contre-le-pistage-de-facebook.php

Vuvuzela, une messagerie qui cache les métadonnées

Vuvuzela, une messagerie qui cache les métadonnées

Vuvuzela est une nouvelle messagerie qui prétend qu'elle peut cacher les métadonnées. Le concept est encore très expérimental, mais il est assez prometteur.

Vuvuzela est un concept de messagerie qui permet de communiquer en cachant les métadonnées. Elle est développé par David Lazar, un doctorant du MIT qui travaille sur le chiffrement et les systèmes distribués. Il a publié un papier qui décrit les principes de Vuvuzela.
Des protocoles comme TOR permettent d'avoir un certain anonymat, mais il reste vulnérable à une analyse du trafic. Avec Vuvuzela, la messagerie est spécialement conçue pour se protéger contre la surveillance gouvernementale sur les métadonnées. La NSA a admis a plusieurs reprises qu'il ne sert à rien de chiffrer les données si les métadonnées sont en clair.

Les métadonnées englobe de nombreuses informations, mais on peut les résumer par le fait qu'elle pointent vers l'identité d'une personne et les contacts de cette personne. Vuvuzela veut cacher les métadonnées, mais elle ne peut pas cacher 2 métadonnées. La première est le nombre d'utilisateurs connectés sans une conversation et la seconde concerne les utilisateurs actifs dans une conversation. Mais Vuvuzela réduit également ce problème en ajoutant des nuisances aux métadonnées.
Le concept est intéressant, mais il n'est pas prêt pour le déploiement. On peut suivre le projet sur Github.

Réagissez à cet article
Source : http://actualite.housseniawriting.com/technologie/2015/12/04/vuvuzela-une-messagerie-qui-cache-les-metadonnees/11327/