16% des entreprises victimes des Ransomwares. Réagissez !

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	16% des entreprises victimes des Ransomwares. Réagissez !				

Les ransomwares visent de plus en plus les entreprises françaises. Ce phénomène n'est pas près de s'arrêter au regard du business model très lucratif et de l'impunité juridique dont bénéficient les hackers.
Force est de constater que les hacker un plus d'un coup d'avance.
En effet, PC Cyborg, le premier Ransomware, date tout de même de 1989. Pourtant, depuis le temps, le phénomène n'ayant pas été pris au sérieux, il commence désormais à prendre une ampleur phénoménale.
Il est évident qu'aujourd'hui aussi bien les entreprises que les états sont dépassés par ce phénomène. La liste des entreprises, parfois des OIV (Opérateurs d'importance Vitale) ou des OSE (Opérateur de Services Essentiels) ou des services publics touchés ne cesse de s'alourdir.

Que nous annonce le futur ?
Nos télévisions prises en otage par un ransomware (crypto virus ou programme informatique qui rend illisible vos données et inversera l'opération contre paiement d'une rançon, d'où le nom de crypto virus) pourrait bien arriver dans nos foyés dans les prochains mois. Notre auto, notre téléphone et bientôt nos maisons (serrures, lumières, fours, réfrigérateurs… n'importe quel objet connecté essentiel en définitive) pourraient bien nous demander un petit bitcoin en échange de son refonctionnement.

Que pouvons nous faire ?
Les entreprises doivent évoluer selon plusieurs axes :
• Reconsidérer la priorité consacrée à la sécurité informatique pour faire évoluer son infrastructure technique, organisationnelle, reconsidérer les conséquences en terme d'image ou de pérennité que pourraient entraîner une attaque informatique.
• Reconsidérer le personnel en charge du service informatique et former le responsable informatique à la sécurité ou mieux (ce que je recommande), utiliser les services d'un expert en cybersécurité ou en cybercriminalité en appui du service informatique.
• Responsabiliser les utilisateurs par une charte informatique complétée et présentée lors des cessions de sensibilisation.
• Sensibiliser (et former pour certains) les utilisateurs aux différents risques liés aux usages informatiques en partant des ransomwares, jusqu'aux différentes formes d'arnaques aux victimes dépouillées de plusieurs dizaines, centaines milliers d'euros voire des millions d'euros.

Et au niveau international ?
Il est évident que la tâche sera longue et fastidieuse mais il est à mon avis possible de combattre le phénomène en agissant sur plusieurs leviers.
Le voler législatif doit évoluer et s'adapter aux attaques informatiques internationales pour que les coopérations internationales puissent se passer sans délai.
Le volet coordination doit être couvert par une entité internationale qui pourrait devenir un point de contact aussi bien pour les autorités collectant les plaintes de victimes, pour les organismes faisant évoluer les instruments judiciaires, pour les éditeurs et constructeurs d'outils exposés au menaces.

Réagissez à cet article

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été
Les meilleurs conseils pour choisir vos mots de passe
Victime d'un piratage informatique, quelles sont les bonnes

pratiques ?
Victime d’usurpation d’identité sur facebook, tweeter ? Portez plainte mais d’après quel article de loi ?
Attaques informatiques : comment les repérer ?

Quel est notre métier ?

Former et accompagner les organismes à **se mettre en conformité avec la réglementation numérique (dont le RGPD)** et à **se protéger des pirates informatiques**.

Quel sont nos principales activités ?

- **RGPD**
  - FORMATION AU RGPD
  - FORMATION DE DPO
  - AUDITS RGPD
  - MISE EN CONFORMITÉ RGPD
  - ANALYSES DE RISQUES (PIA / DPIA)

- **CYBERCRIMINALITÉ**
  - FORMATIONS / SENSIBILISATION D'UTILISATEURS
  - RECHERCHE DE PREUVES

- **EXPERTISES**
  - EXPERTISES PRIVÉES
  - EXPERTISES DE VOTES ÉLECTRONIQUES
  - EXPERTISES JUDICIAIRES
  - RECHERCHE DE PREUVES
  - RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)

Notre Expert, Denis JACOPINI, est Expert en Informatique assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

« *Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme.*
Denis JACOPINI »

Besoin d'un Expert ? contactez-nous

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).

- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Source : Denis JACOPINI

DU en Investigation Numérique Pénale – Denis JACOPINI témoigne

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer

DU en Investigation Numérique Pénale – Denis JACOPINI témoigne

Vous souhaitez connaître le droit, les éléments théoriques ainsi que les outils liés au métier d'investigateur numérique en matière pénale ? Cette formation de 130 heures qui débouche sur le premier Diplôme Universitaire en Investigation Numérique Pénale de France est faîte pour vous. Attention, les places sont limitées.

Contenu de la formation :
• Acquisition des bases et des fondamentaux en matière informatique dans le cadre d'une expertise pénale ;
• Connaissance de la Procédure pénale ;
• Connaissance des missions, de l'organisation professionnelle et des bonnes pratiques d'un enquêteur numérique ;
• Acquisition des méthodes et pratiques d'extraction de données post mortem :
• *Extraction de données à partir de supports physiques*
• *Extraction de données à partir de terminaux mobiles*
• *Extraction de traces internet*
• *Manipulation d'objets multimédia*
• Acquisition des méthodes de fouille de données

2019 06 14 Plaquette INPA5 v12

Cette formation est réalisée en partenariat avec :
• UFIN (Union Française de l'Investigation Numérique)
• CNEJITA (Compagnie Nationale des Experts de Justice en Informatique et Techniques Associées)
• AFSIN (Association Francophone des Spécialistes de l'Investigation Numérique)
• Gendarmerie nationale

Denis JACOPINI, Expert de Justice en Informatique spécialisé en Cybercriminalité et en Protection des Données Personnelles (RGPD) témoigne :
C'est avec grand plaisir que je vous témoigne ma grande satisfaction à l'issue de cette formation. Même si j'avais déjà une expérience en tant qu'Expert de Justice en Informatique, étalée sur 8 mois, le contenu de cette formation m'a permis d'être désormais mieux équipé (mentalement, organisationnellement et techniquement) et en plus grade confiance pour les futures expertises pénales qui me seront confiées.

Réagissez à cet article

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été
Les meilleurs conseils pour choisir vos mots de passe
Victime d'un piratage informatique, quelles sont les bonnes pratiques ?
Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?
Attaques informatiques : comment les repérer ?

Quel est notre métier ?

Former et accompagner les organismes à **se mettre en conformité avec la réglementation numérique (dont le RGPD)** et à **se protéger des pirates informatiques**.

Quel sont nos principales activités ?

- **RGPD**
  - FORMATION AU RGPD
  - FORMATION DE DPO
  - AUDITS RGPD
  - MISE EN CONFORMITÉ RGPD
  - ANALYSES DE RISQUES (PIA / DPIA)

- **CYBERCRIMINALITÉ**
  - FORMATIONS / SENSIBILISATION D'UTILISATEURS

- RECHERCHE DE PREUVES

- **EXPERTISES**
  - EXPERTISES PRIVÉES
  - EXPERTISES DE VOTES ÉLECTRONIQUES
  - EXPERTISES JUDICIAIRES
  - RECHERCHE DE PREUVES
  - RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)

Notre Expert, Denis JACOPINI, est Expert en Informatique assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

« *Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et*

les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme.
Denis JACOPINI »

Besoin d'un Expert ? contactez-nous

Source : *Diplôme d'Université : Investigation Numérique Pénale – Ametys*

Loi renseignement : une première «boîte noire» activée pour surveiller les communications

	Loi renseignement : une première «boîte noire» activée pour surveiller les communications

Ce dispositif donne aux services de renseignement français un moyen d'analyser automatiquement les métadonnées des communications Internet, notamment pour lutter contre le terrorisme.

De nouvelles oreilles pour le renseignement. Longtemps inactives, les boîtes noires sont désormais en cours de déploiement. Francis Delon, le président de la Commission nationale de contrôle des techniques de renseignement (CNCTR), l'a révélé à l'occasion d'une conférence organisée à Grenoble. Il précise qu'une première boîte noire a été activée «début octobre», à l'issue d'un «travail qui a duré plusieurs mois».

Prévu par l'article 851-3 du Code de la sécurité intérieure, le dispositif a été particulièrement critiqué en amont du vote de la loi renseignement de 2015. Il permet aux services de renseignement d'analyser de grandes quantités de métadonnées (relatives au contexte d'un message, comme son origine ou sa date d'envoi) à la volée, afin de détecter une éventuelle menace terroriste. Francis Delon se veut néanmoins rassurant. «Les données récoltées sont des données de connexion anonymisées, recueillies de façon non ciblée pour être mises dans une sorte de grande marmite étanche», a-t-il résumé, par une métaphore de son cru…[lire la suite]

Réagissez à cet article

Source : *Loi renseignement : une première «boîte noire» activée pour surveiller les communications*

FIC 2018 les 23 et 24 janvier à Lille : à l’ère de l’hyperconnexion, comment s’organise la cyber-résilience ?

FIC 2018 les 23 et 24 janvier à Lille : à l’ère de l’hyperconnexion, comment s’organise la cyber-résilience ?

Organisé conjointement par la Gendarmerie Nationale, CEIS et EuraTechnologies, et co-financé par la Région Hauts-de-France, la 10è édition du Forum International de la Cybersécurité entre dans l'ère de l'hyperconnexion.

« Les individus et les machines sont connectés en permanence et communiquent sans discontinuer entre eux et les uns avec les autres. Cette imbrication de réseaux expose le système aux effets dominos sur l'une de ses composantes et pose d'abord la question de la résilience, c'est à dire la capacité du système à faire face aux conséquences d'une attaque ou d'une défaillance sur l'un des maillons de la chaîne, et à récupérer ses aptitudes à opérer normalement. Cette nouvelle configuration bouleverse aussi les modes de fonctionnement et d'organisation de nos sociétés, et nécessitera d'adapter nos comportements, pratiques, technologies de sécurité et corpus législatifs et règlementaires. A l'ère de l'hyperconnexion, la cyber-résilience suppose donc une approche systémique de la sécurité impliquant à la fois les individus, les processus et les techniques » explique le Général Marc Watin-Augouard, fondateur du Forum International de la Cybersécurité….[lire la suite]

Denis JACOPINI :

C'est sur ce thème que le FIC 2018 ouvrira. Conférences, démonstrations, ateliers seront au rendez-vous. Le FIC 2018 est aussi le point de rencontre international des principaux acteurs de la cybersécurité. Donnons-nous donc rendez-vous les 23 et 23 janvier à Lille Grand Palais. Consultez le Pré Programme du FIC 2018 au 02/09/2017.

Réagissez à cet article

Source : *23 et 24 janvier Lille – FIC 2018 : à l'ère de l'hyperconnexion, comment s'organise la cyber-résilience ? – Global Security Mag Online*

Comment fonctionnent les Interconnexions d'Internet à travers le monde ?

Comment fonctionnent les Interconnexions d'Internet à travers le monde ?

Etats, citoyens et entreprises sont la cible de cyberattaques de plus en plus régulières et sophistiquées. Les infrastructures mises en place pour nous permettre de communiquer à travers toute la planète n'ont pas que des avantages…

NOTRE MÉTIER :

PRÉVENTION : Vous apprendre à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) sous forme de conférences, d'audits ou de formations ;

RÉPONSE A INCIDENTS : Vous aider à rechercher l'origine d'une attaque informatique, recueillir les preuves pour une utilisation auprès de la justice ou des assurances, identifier les failles existantes dans les systèmes informatiques et améliorer la sécurité de l'existant ;

SUPERVISION : Assurer le suivi de la sécurité de votre installation pour la conserver le plus possible en concordance avec l'évolution des menaces informatiques.

MISE EN CONFORMITÉ CNIL : Vous assister dans vos démarches de mise en conformité avec le RGPD (Réglement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS

: https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles (Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle)

Réagissez à cet article

Non, NotPetya n’est pas un ransomware… mais un logiciel de sabotage

	Non, NotPetya n’est pas un ransomware… mais un logiciel de sabotage

Le déchiffrement des machines impactées est impossible. La demande de rançon n'était donc qu'un leurre pour camoufler un cybersabotage. La piste d'un acte politique, probablement réalisé par une agence gouvernementale, émerge.

Mauvaise nouvelle pour toutes les victimes de NotPetya. Les dernières analyses des chercheurs en sécurité montrent que ce malware est en réalité un logiciel de sabotage déguisé en ransomware. Les victimes ne pourront donc retrouver leurs données, à moins qu'un expert arrive à détecter une faille dans le processus de chiffrement.

Plusieurs indices prouvent que les auteurs de NotPetya n'ont jamais eu l'intention d'envoyer une quelconque clé de déchiffrement. Le premier concerne l'identifiant unique affiché dans le message de rançonnage et que la victime doit envoyer aux pirates après avoir effectué le paiement en bitcoins. En théorie, cet identifiant doit permettre aux auteurs de NotPetya d'identifier la victime. Il doit, par conséquent, contenir des informations sur les clés de chiffrement utilisées sur la machine en question. Mais selon les chercheurs de Kaspersky, il s'avère que cet identifiant est totalement aléatoire. *« Les attaquants ne peuvent extraire une quelconque information de déchiffrement d'une telle suite de caractères aléatoire »*, soulignent-t-ils dans une note de blog.

Kaspersky – L'identifiant unique affiché est totalement aléatoire

De son côté, le chercheur en sécurité Matt Suiche a découvert que les données de la zone d'amorçage ne sont sauvegardées nulle part, mais simplement remplacées par autre chose. Le système de fichier du disque serait donc de toute façon irrécupérable. *« La version actuelle de Petya a été réécrite pour être un wiper, et non un ransomware »*, souligne l'expert….[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *Non, NotPetya n'est pas un ransomware… mais un logiciel de sabotage*

Voilà la prochaine cyberattaque

	Voilà la prochaine cyberattaque

Après WannaCry et ses 200.000 demandes de rançon, une nouvelle cyberarme cible les réseaux électriques. Où sont les failles? Nos industries sont-elles parées? Enquête exclusive.

À lui seul, son nom file déjà des frissons. Baptisé “Industroyer” (contraction des termes anglais “industrial” et “destroyer”), un nouveau virus vient d’être identifié par des chercheurs en sécurité informatique. Il s’agit d’un puissant logiciel malveillant, voire une cyberarme de destruction massive. Ce virus industriel cible en effet le secteur de l’énergie. “C’est même la menace la plus puissante pour les systèmes de contrôle industriels depuis Stuxnet!”, enchérit le spécialiste slovaque en cybersécurité ESET, codécouvreur de cette nouvelle menace avec l’américain Dragos.
Pour rappel, le ver informatique Stuxnet, attribué aux services secrets américains et israéliens, a saboté une centrale nucléaire iranienne en 2010, provoquant même des explosions. Une première mondiale dans l’histoire du piratage informatique, qui aurait pu se solder selon les experts russes par un accident pire que celui de Tchernobyl. Le potentiel de cette super-mine numérique? D’après ces chercheurs européens et américains, Industroyer serait déjà responsable du piratage du réseau ukrainien en décembre 2016, qui avait privé une partie de Kiev d’électricité pendant plus d’une heure. “Ce nouveau virus peut être immédiatement adapté pour attaquer des réseaux en Europe et dans une partie du Moyen-Orient et de l’Asie”, avertit encore l’expert US. Cette cyberarme peut-elle dès lors frapper la Belgique, pays fortement nucléarisé et très densément électrifié? Se couvrant derrière le secret-défense, aucun opérateur belge ne se risque à y répondre…[lire la suite]

Bref commentaire de Denis JACOPINI :
Les années nous ont donné raison, nous les lanceurs d’alertes qui sensibilisons les décideurs et les élus depuis des années en tirant la sonnette d’alarme pour anticiper les risques. Chaque jour qui passe nous donne raison nous comptons les victimes de la cybercriminalité par milliers.
Le cybercrime peut prendre de nombreuses apparences, mais les décideurs et les élus, pénalement responsables aussi bien des fuites de données que de la perte des données doivent prendre les devants. Fort de nos années d’expérience dans ce domaine, nous organisons, en collaboration avec les CCI, les clubs d’entreprises et les centres de formations des sessions de sensibilisation aux risques informatiques et à la mise en conformité de vos données personnelles.
Contactez-nous

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d’expertises, d’audits, de formations et de sensibilisation dans toute la France et à l’étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d’un Correspondant Informatique et Libertés (CIL) ou d’un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l’Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d’informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *Voilà la prochaine cyberattaque | Moustique.be*

Les entreprises du CAC 40 sont la cible de cyberattaques

Les entreprises du CAC 40 sont la cible de cyberattaques

Renault n’est pas la seule entreprise dans le viseur des cyberterroristes. Les champions de la défense et les géants de la Bourse peaufinent leur bouclier.
par Guerric PONCET

« En 2016, de gros industriels ont été touchés et des géants du CAC 40 ont pris conscience qu’ils pouvaient disparaître du jour au lendemain à cause d’une cyberattaque », nous confie Guillaume Poupard, directeur général de l’Agence nationale de la sécurité des systèmes d’information (Anssi). « Je veux dire que, si leur piratage était dévoilé, ils étaient *OPAbles* le lendemain », précise-t-il. En effet, la révélation d’une telle attaque ferait immédiatement chuter le cours de la Bourse…
Nos champions de la cybersécurité, Airbus, Thales, Capgemini et Orange en tête, sont sollicités de toutes parts par les comités exécutifs. Mais leurs tarifs sont souvent hors de portée des PME : dans le cyber, la défense coûte cent fois le prix de l’attaque. Et, quand bien même, le budget ne fait pas tout : JP Morgan, Yahoo !, Adobe, Visa ou encore Sony ont beau avoir alloué des centaines de millions de dollars à leur sécurité informatique, ils ont tous vécu des intrusions gravissimes. « Il est impossible de créer un cyberbouclier infaillible », tranche Guillaume Poupard, pour qui il faut avoir « une bonne gouvernance avant même de parler technique ». « Jusqu’à présent, nous avons stoppé les attaques majeures qui nous visaient, mais, si l’une d’elles réussissait, ce serait une catastrophe, avec des conséquences sur la souveraineté économique de la France et, très rapidement, sur la sécurité des populations », nous glisse, sous le couvert de l’anonymat, le responsable de la sécurité informatique d’une entreprise classée « opérateur d’importance vitale » (OIV).
Des exercices de crise sont régulièrement menés pour anticiper et limiter les dégâts que créerait assurément une cyberattaque chez un OIV – panne générale dans la production électrique, paralysie des transports, implosion des télécoms… Des agents de l’Anssi jouent aux hackers, tentent de déjouer les systèmes de sécurité… et y parviennent : « La dernière fois, ils ont pris le contrôle d’une partie de notre système assez facilement, ils auraient pu créer des accidents graves », reconnaît, lui aussi en toute discrétion, le responsable informatique d’un autre OIV. Nous voilà rassurés…[lire la suite]

Réagissez à cet article

Source : *Cyberguerre : le CAC 40 dans le viseur – Le Point*

La Police pourrait prochainement consulter vos données personnelles sur Facebook sans autorisation

	La Police pourrait prochainement consulter vos données personnelles sur Facebook sans autorisation

Face à la vague d'attentats qui frappe l'Europe, la Commission européenne discute actuellement de quelques changements dans les réglementations afin de permettre aux forces de Police d'accéder aux données des utilisateurs des services de Google et Facebook, sans autorisation préalable d'un Juge.

Les vagues d'attentat et la peur ambiante sont bien souvent l'occasion pour les gouvernements de voter des lois liberticides, et ce pourrait à nouveau être le cas dans toute l'Europe. La Commission européenne réfléchit actuellement à changer les réglementations afin de permettre aux forces de police d'aller piocher des informations dans les comptes des réseaux sociaux des utilisateurs, sans accord préalable de qui que ce soit.

Concrètement, le projet évoque même la possibilité pour les policiers d'origine étrangère de consulter les données privées des profils de ces réseaux sociaux, afin notamment d'enquêter sur un touriste ou une personne d'un autre pays de l'Union européenne. Exemple : vous partez en Italie pour quelques jours et vous faites arrêter par la police locale, ces derniers pourraient alors éplucher vos profils sociaux pour tenter d'obtenir plus d'informations sur vous, et ce, sans rien demander à la France.

Actuellement, trois projets de ce type ont été proposés et soumis à étude, l'un d'entre eux pouvant être adopté d'ici la fin de l'année 2018. Une des propositions évoque la possibilité de copier les données directement depuis le Cloud de la plateforme sociale afin d'en faire une sauvegarde et éviter la disparition des données en cas d'enquête…[lire la suite]

Commentaire de Denis JACOPINI

Entre Facebook qui analyse et espionne ses membres et les OPJ (Officiers de Police Judiciaire) qui peuvent consulter les données collectées par Facebook, il n'y a qu'un pas pour que ce même type de démarche soit aussi engagée auprès de Google pour qu'on nous mette des radars automatiques sur Internet qui nous flashent dès que quelqu'un en train picoler publie une photo.
Sans plaisanter, ces projets de loi consistent à permettre à des OPJ d'accéder aux zones privées de Facebook, car vous savez que lorsque vous publiez quelque chose sur Facebook, cet ajout peut être public (tout le monde peut le consulter et le voir) ou privé et il n'y a qu'un juge qui peut forcer Facebook à communiquer le contenu privé d'un compte. Ce projet ne changera rien pour ceux qui n'ont rien à se reprocher, et pas grand chose pour ceux qui ont quelques chose à se reprocher. Les OPJ pourrons disposer plus rapidement des contenus privés pour alimenter leurs enquêtes.
Il est fort probable à l'avenir qu'un autre réseau social soit utilisé par les malfrats l'histoire de faire courrier le chat…

Réagissez à cet article

Source : *Europe : la Police pourrait prochainement consulter vos données personnelles sur Facebook sans autorisation*

Limiter les risques venant des drones en les immatriculant. Une bonne idée ?

Limiter les risques venant des drones en les immatriculant. Une bonne idée ?

Hostile à une surveillance en réseau, le fabricant DJI propose une immatriculation électronique que seules les forces de l'ordre pourraient exploiter.
Jean-Michel Normand

L'idée trotte dans la tête de nombre de législateurs. Installer à bord des drones de loisir un système de reconnaissance électronique fait déjà partie de l'arsenal législatif adopté l'an passé par les parlementaires français, sans pour autant que des précisions techniques aient été définies. L'Italie et le Danemark ou la FAA, l'Aviation civile américaine, l'ont également inscrit à leur programme. Dans une proposition qu'il vient de rendre publique, le fabricant de drones chinois DJI préconise une identification électronique *« simple, qui maintient un équilibre entre le respect de la vie privée de l'opérateur du drone et les légitimes préoccupations des autorités relatives à l'utilisation »* de ces appareils.

1.
Plusieurs pays, dont la France, envisagent d'imposer une signature électronique. NIR ELIAS / REUTERS

« Comparable à une plaque d'immatriculation automobile »
DJI est favorable à ce que tous les drones commercialisés soient capables d'émettre un signal qui indique leur localisation, mais aussi un code d'identification *« comparable à une plaque d'immatriculation automobile »* en mode électronique. Ce code serait émis sur les bandes de fréquence (2,4 GHz et 5,8 GHz) utilisées pour la liaison entre le drone et la radiocommande du pilote et pour la liaison vidéo. Il suffirait de réaliser une mise à jour des protocoles de contrôles radio existants. L'information pourrait être captée par la police ou un particulier furieux de voir un quadricoptère évoluer au-dessus de sa propriété, à condition qu'il soit équipé d'un récepteur adapté. Il lui faudra alors se tourner vers les forces de l'ordre, seules autorisées (avec les autorités aéroportuaires, notamment) à remonter jusqu'au titulaire de l'immatriculation électronique…[lire la suite]

Commentaire de Denis JACOPINI :
Je trouve personnellement l'idée intéressante, encore faut-il que :
1. L'émission de cette information ne puisse pas être perturbée (j'en doute) ;
2. L'émission du code du drone ne puisse pas être modifiée (plus facile) ;
3. Cette procédure soit légiférée et suivie par tous les constructeurs mondiaux.

Ceci n'empêchera pas les groupes les plus obscurs d'utiliser des drones volés non pourvus de cette signature.
A mon avis, la mise en place de ces précautions ne concernent que l'utilisateur lambda, pas ceux que l'on craint actuellement le plus sur le territoire.

Réagissez à cet article

Source : *Comment immatriculer les drones de loisir*