Voyagez aux Etats-Unis et laissez vos données être espionnées

Voyagez aux Etats-Unis et laissez vos données être espionnées

L'administration Trump envisage de demander aux voyageurs arrivant aux Etats-Unis l'accès aux données de leur smartphone et à leurs comptes Twitter, Facebook ou LinkedIn. Une sévère menace pour la cybersécurité des entreprises européennes.

Cette fois-ci, la côte d'alerte est clairement franchie. Dans ses colonnes, le *Wall Street Journal* évoque un projet de l'administration Trump qui pourrait forcer les visiteurs arrivant aux Etats-Unis à communiquer aux autorités les contacts et contenus présents sur leur téléphone mobile ainsi que les mots de passe de leurs comptes de réseaux sociaux, permettant d'accéder aux messages privés envoyés sur ces canaux. Un projet qui ne serait pas limité aux pays soumis aux règles de sécurité les plus strictes – et dont les ressortissants doivent obtenir un visa -, mais concernerait aussi les pays considérés comme des alliés des États-Unis, dont la France.
Rappelons que, pour se rendre de façon temporaire sur le sol américain, pour affaires ou en tant que touriste, les Français doivent déjà solliciter une autorisation électronique (Esta), valable 2 ans. En février, le ministre de l'Intérieur américain (Homeland Security) avait déjà évoqué, lors d'une audition devant le Sénat, le fait que les voyageurs étrangers (notamment issus des 6 pays blacklistés par un décret de l'administration Trump) venant aux États-Unis seraient tenus de fournir leurs mots de passe sur les médias sociaux aux autorités d'immigration avant de rentrer sur le territoire américain.

La peur de l'espionnage économique

Selon le *Wall Street Journal,* cette mesure serait donc étendue à d'autres pays et aussi aux contacts téléphoniques. « *S'il existe un doute sur les intentions d'une personne venant aux États-Unis, elle devrait avoir à prouver la légitimité de ses motivations, vraiment et véritablement jusqu'à ce que cela nous satisfasse* », a expliqué le conseiller principal du Homeland Security, Gene Hamilton, cité par le quotidien économique.
Si la question ne manquera pas de soulever de vifs débats sur le sol américain et entre les États-Unis et ses partenaires et si une procédure de la sorte pose également quelques questions pratiques assez épineuses, la perspective risque d'échauder de nombreuses entreprises européennes. Car, les activités des services de renseignement US associent sans vergogne antiterrorisme et espionnage économique au profit des entreprises américaines. Une porosité d'ailleurs assumée, comme l'ont montré de nombreux documents dévoilés par Edward Snowden ou *Wikileaks* et révélant les activités de la NSA en matière d'espionnage économique. Les activités de cette nature ne sont d'ailleurs pas limitées à la seule agence de Fort Meade, mais s'étendent à toute la communauté du renseignement aux Etats-Unis.
Au passage, les mesures envisagées par l'administration Trump signeraient probablement l'arrêt de mort du Privacy Shield, l'accord transatlantique sur les transferts de données qui succède au Safe Harbor. Pour mémoire, ce dernier érige comme credo le fait que les données des citoyens européens exportées aux Etats-Unis bénéficient de la même protection que celle que leur accorde le droit européen. En février, les CNIL européennes s'étaient déjà inquiétées des conséquences possibles du décret sur l'immigration du Président Trump sur cet accord…[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

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *L'entrée aux Etats-Unis conditionnée par les données des smartphones ?*

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.
À 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.

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

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DIRECCTE n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Source : *Comment immatriculer les drones de loisir*

Ce vibromasseur connecté muni d'une caméra est vraiment trop facile à hacker

Ce vibromasseur connecté muni d'une caméra est vraiment trop facile à hacker

Oui, évidemment on se demande bien qui voudrait hacker ce type d'objet, pour visionner ce type d'images. Mais ainsi va le monde : le Wi-fi de ce vibromasseur connecté se pirate en deux clics.

On ne le dira jamais assez, mais une connexion WiFi est une porte d'entrée royale pour n'importe quel hacker. Même fermée, elle est très simple à pirater. Ensuite, le pirate peut avoir accès à l'ensemble des données du trafic internet de l'objet connecté.

Photos, identifiants, mots de passe pour un téléphone, mais aussi flux *streaming* pour ce vibromasseur connecté. S'il vient à être piraté, c'est une tout autre intimité qui peut être violée.

Vibromasseur avec hot spot WiFi

Le vibromasseur Svakom Siime Eye (disponible au prix de 249 dollars) dispose du WiFi et d'une caméra intégrée pour procéder à des *livestreams*. Les chercheurs en sécurité de Pen Test Partners ont découvert que l'interface de l'objet connecté était très simple à hacker pour toute personne se trouvant à portée de la connexion WiFi (et pourvu d'un minimum de connaissance en la matière, cela s'entend).
Un piratage d'autant plus facilité que le mot de passe par défaut de ce point d'accès WiFi est « 88888888 », soit 8 fois le chiffre 8.

Un piratage enfantin

N'importe quelle personne à proximité du signal peut accéder au flux vidéo. Pire, en poussant leur investigation un peu plus loin, ces chercheurs sont parvenus à accéder au serveur web et à la racine de l'appareil pour configurer une connexion à distance.

Les utilisatrices qui voudraient partager ces instants intimes avec leur partenaire, pourraient se retrouver à faire de même avec leur voisin de palier. Une perspective peu réjouissante.
Le fondateur de Pen Test, Ken Munro, explique qu'il a tenté de contacter la compagnie pendant des mois avant de rendre publique ces informations.
Ce n'est pas la première fois que ce type d'objet connecté est mis au ban : le mois dernier, la société canadienne Standard Innovation a été condamnée à verser 3 millions de dollars à ses clientes pour avoir omis de mentionner qu'elle collectait leurs données personnelles via leur vibromasseur connecté et l'application dédiée.
Auteur : Elodie

Réagissez à cet article

Source : *Ce vibromasseur connecté muni d'une caméra est vraiment trop facile à hacker*

Alerte : Sérieuse faille WiFi. Mettez à jour vos iPhones avec la IOS 10.3.1

Alerte : Sérieuse faille WiFi. Mettez à jour vos iPhones avec la IOS 10.3.1

La mise à jour 10.3.1 du système d'exploitation mobile iOS corrige une vulnérabilité permettant d'exécuter du code à distance sur les puces WiFi de Broadcom dans les iPhone, iPad et iPod. Le fabricant de puces a pu obtenir une grâce d'une dizaine de jours avant divulgation de l'exploit par l'équipe sécurité de Google, Project Zero.

L'iPhone 7 est concerné par la faille WiFi et éligible pour la mise à jour iOS 10.3.1. (crédit : Susie Ochs)

Si vous n'avez pas mis à jour iOS pour vos terminaux mobiles Apple depuis longtemps, voici une bonne occasion de le faire. Apple a en effet lancé la version 10.3.1 de son système d'exploitation pour iPhone, iPad et iPod pour corriger une vulnérabilité permettant à un attaquant d'exécuter du code malveillant distant sur les puces WiFi Broadcom de ces terminaux. Cette vulnérabilité touche la fonction d'authentification dans le protocole 802.11r permettant aux terminaux de se connecter de façon sécurisée entre plusieurs stations de base sans fil d'un même domaine. Les hackers peuvent exploiter cette faille pour exécuter du code au sein même du firmware de la puce WiFi s'ils se trouvent à portée du réseau sans fil des terminaux visés.
Il s'agit là d'une vulnérabilité parmi d'autres trouvées par le chercheur Gal Benjamini de l'équipe de sécurité de Google, Project Zero, dans le firmware des puces Broadcom WiFi. Certaines d'entre elles concernent également les terminaux Android et ont été patchées dans le cadre du bulletin de sécurité Android d'avril. La mise à jour iOS 10.3.1, lancée lundi, est quelque peu inhabituelle car elle vient une semaine à peine après la 10.3 qui apportait pourtant un lot de correctifs touchant différents composants. L'explication pour ce court intervalle entre ces deux mises à jour est à voir du côté du délai pratiqué par Google Project Zero pour dévoiler au public les exploits de failles…[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

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

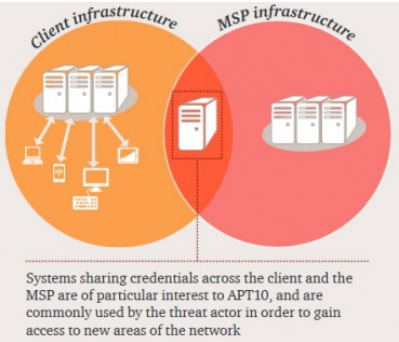
Source : *Apple colmate une sérieuse faille WiFi dans iOS – Le Monde Informatique*

Les services Cloud au centre d’attaques d’entreprises par APT10

Les services Cloud au centre d’attaques d’entreprises par APT10

Le groupe de pirates chinois APT10 a infiltré des services Cloud managés pour remonter aux serveurs des entreprises qui les utilisent.

La maturité des attaques ciblées contre les entreprises est montée d'un cran. *« Un groupe de piratage a mené l'une des campagnes d'espionnage les plus prolifiques depuis l'APT1 en 2013, employant de nouvelles tactiques pour atteindre une large audience »*, a alerté PwC (Pricewaterhouse Coopers) lundi 3 avril. En collaboration avec BAE Systems et le National Cyber Security Centre (NCSC) britannique, la branche réseau du cabinet d'audit a découvert ce qu'il considère comme *« l'une des plus importantes campagnes mondiales de cyber-espionnage jamais organisées »*. Pas moins.



De quoi s'agit-il ? Du piratage des infrastructures de fournisseurs de services managés à partir desquelles les cyber-attaquants remontent aux serveurs des organisations qui y ont recours. Une opération que PwC a baptisé 'Cloud Hopper'. Les cyber-criminels derrière ces agissements seraient le groupe de hackers chinois APT10. *« PwC et BAE Systems croient que le groupe de piratage largement connu sous le nom 'APT10' a mené la campagne d'espionnage en ciblant les fournisseurs de services informatiques externalisés comme une façon d'accéder aux organisations de leurs clients à travers le monde, leur conférant un accès sans précédent à la propriété intellectuelle et aux données sensibles »*, indique PwC dans son communiqué. APT10 est le nom donné par FireEye à un groupe de pirates chinois également référencé sous les appellations Red Apollo (par PwC UK), CVNX (par BAE), Stone Panda (par CrowdStrike), et menuPass Team (plus globalement).

Un grand volume de données exfiltrées

Les méthodes d'infection restent relativement classiques et s'appuient sur le spear-phishing, ou harponnage. Cette méthode de phishing ciblé fait appel à des techniques d'ingénierie sociale qui visent à tromper le destinataire d'un e-mail pour l'inciter à installer, à son insu, un malware ou visiter une page infectieuse, à partir desquels les pirates ouvrent une porte d'entrée sur le réseau. Objectif ici : prendre le contrôle des accès d'employés de prestataires Cloud, afin d'exploiter les canaux de communication existant entre les services managés de ces derniers et les serveurs des entreprises clientes. De la grande distribution aux technologies en passant par l'énergie, l'industrie manufacturière, le secteur public ou l'industrie pharmaceutique, tous les grands secteurs sont touchés par cette campagne…[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

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

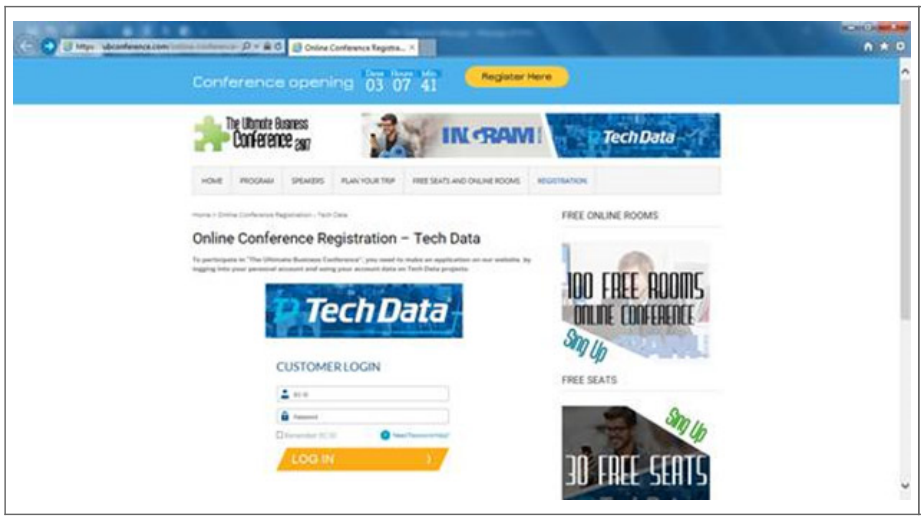
Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Les services Cloud au centre d'attaques d'entreprises par APT10*

Alerte : Les revendeurs informatiques de Tech Data France ciblés par un site Internet Frauduleux



Alerte : Les revendeurs informatiques de Tech Data France ciblés par un site Internet Frauduleux

---

Chers revendeurs informatiques, attention à la nouvelle arnaque. Les intentions des pirates ne sont pas encore connues, mais les intentions sont forcément malveillantes.

En tant que revendeur informatique, il est fort probable que vous commandiez votre matériel destiné à la revente ou non chez les principaux et parmis les plus anciens grossistes et importateurs Français : Ingram ou Techdata.
Une récente communication de Techdata, qui nous a été remontée par un précieux partenaire Parisien, nous informe que Techdata vient de lancer l'alerte suivante auprès de ses clients :

Cher client,
Il a été porté à notre connaissance que certains Clients de TECH DATA ont reçu des emails comportant un lien internet vers un site web frauduleux leur demandant :
– de s'inscrire à une conférence dans laquelle TECH DATA et d'autres distributeurs participeraient,
– de fournir des informations type login et mot de passe de TECH DATA ainsi que d'autres informations sensibles.
Le site Web apparaît comme indiqué ci-dessous :

Veuillez noter que ce site web n'est d'aucune façon associé à TECH DATA. La sécurité de nos partenaires est une priorité pour TECH DATA et nous n'autorisons aucun tiers à collecter les identifiants de connexion de nos clients.
Aussi, actuellement nous œuvrons avec les autorités compétentes pour la fermeture de ce site frauduleux.
A ce jour, à notre connaissance les clients européens ne semblent pas affectés, ce site frauduleux visant les clients américains principalement.
Cependant, nous comptons sur votre vigilance et vous remercions de nous informer dans le cas où vous recevriez des emails contenant des liens vers ce site internet ou similaires en vous adressant à l'adresse suivante : itsecurity@techdata.com
Nous attirons votre attention sur la sophistication et l'augmentation de la cybercriminalité (phishing), dès lors restez vigilants.
Nous vous remercions de votre attention et collaboration.
Tech Data Europe

Comme vous pouvez le remarquer, à l'instar de KPMG pourtant spécialisé en audit et conseil dans de nombreux domaines dont la sécurité informatique, pourtant victime d'une arnaque au Président leur ayant coûté plusieurs millions d'Euros (7,6) en 2014, les professionnels de l'informatique sont aussi la cible des pirates.
Nous espérons que, même si la plupart n'ont pas assisté à nos conférences de sensibilisation à la Cybercriminalité, ils sauront à quoi ressemble le loup pour ne pas le laisser rentrer dans la bergerie.

Denis JACOPINI

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

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DIRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *E-mailing Tech Data France*

Secret des correspondances : Ce que change la Loi Lemaire

à partir de 2017

	**Secret des correspondances : Ce que change la Loi Lemaire à partir de 2017**

Le 30 mars 2017 a été publié au Journal Officiel un décret d'application de la loi pour une République numérique relatif au secret des correspondances (article 68 de la loi). A cette occasion, la CNIL en profite pour faire le point sur cette notion et sur ce qui change pour les utilisateurs de services de messagerie électronique.

Le 30 mars 2017 a été publié au Journal Officiel un décret d'application de la loi pour une République numérique relatif au secret des correspondances (article 68 de la loi). A cette occasion, la CNIL en profite pour faire le point sur cette notion et sur ce qui change pour les utilisateurs de services de messagerie électronique.
La correspondance privée se définie comme tout message exclusivement destiné à une ou plusieurs personnes physiques ou morales, déterminées et individualisées. L'exemple le plus concret est le courriel échangé entre deux ou plusieurs correspondants, depuis un service de messagerie.
Ainsi, toute correspondance entre deux personnes doit être protégée au titre du secret, par les opérateurs dont l'activité consiste à acheminer, transmettre ou transférer le contenu de ces correspondances. Tout comme un facteur n'a pas le droit d'ouvrir un courrier postal, le fournisseur de messagerie électronique ou le fournisseur d'accès à internet sont tenus de respecter le secret des courriers électroniques.
Ce principe de confidentialité était d'ailleurs déjà garanti par l'article L32-3 du Code des postes et des communications électroniques qui prévoyait, dans sa version antérieure à la publication de la loi pour une République numérique que « *les opérateurs, ainsi que les membres de leur personnel, sont tenus de respecter le secret des correspondances* ».
La directive européenne 2002/58 modifiée relative à la vie privée dans les communications électroniques (l'article 5.1) interdit « *à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs* ».
Le contenu des communications, c'est-à-dire des correspondances entre deux individus, est par principe confidentiel et l'obligation de garantir le secret repose sur les opérateurs de télécommunication.
Il est en revanche possible de lever le secret des correspondances, en demandant aux personnes concernées leur consentement.

Qu'est-ce qui change avec la loi pour une République numérique et son décret d'application relatif à la confidentialité des correspondances ?

L'article 68 de loi pour une République numérique précise ce que couvre le secret des correspondances. Ce secret s'applique ainsi à l'identité des correspondants, au contenu, à l'intitulé et aux pièces jointes des correspondances.

Quels sont les professionnels concernés ?

Sont désormais soumis au respect du secret des correspondances, à la fois les « *opérateurs* », c'est-à-dire les opérateurs de télécommunications essentiellement, et les « *fournisseurs de services de communication au public en ligne* », en d'autres termes, tout acteur permettant à deux personnes de correspondre en ligne. Seront notamment concernés les fournisseurs de services de messagerie électronique, de réseaux sociaux, de communication synchrone (VoIP), etc.

A quelles conditions peuvent-ils exploiter la correspondance privée ?

La loi Lemaire leur permet toutefois d'exploiter la correspondance privée, **sous réserve d'obtenir le consentement des utilisateurs et pour les seules finalités suivantes** :
• l'amélioration du service de communication au public en ligne,
• la réalisation de statistiques,
• l'utilisation des données à des fins publicitaires.

Quels sont les effets en pratique pour les opérateurs de communication électronique ou fournisseurs de service ?

La CNIL rappelle que, pour être valable, ce consentement doit être libre, spécifique et informé. Il doit en outre résulter d'un acte positif et être préalable à la collecte des données, c'est-à-dire à la réalisation du traitement.

Un consentement informé

Les opérateurs souhaitant utiliser la correspondance de leurs utilisateurs à des fins statistiques, publicitaires ou encore pour améliorer leur service devront recueillir leur consentement spécifique après les avoir informés de ce qu'ils souhaitent faire (en rappelant les mentions requises par l'article 32 de la loi Informatique et libertés).

Un consentement spécifique

La CNIL rappelle que le consentement doit être spécifique et qu'à ce titre, un consentement global pour plusieurs finalités différentes, de même que l'acceptation globale des Conditions générales d'utilisation (ou CGU) du service, **ne peuvent être considérés comme un consentement valable**.

Un consentement libre

Le consentement ne doit pas être contraint, c'est-à-dire que le refus de consentir ne doit pas empêcher la personne d'accéder au service de messagerie. Le consentement doit prendre la forme d'un acte positif des utilisateurs et ne peut donc être déduit du silence ou de l'inaction des utilisateurs. Le consentement devant être recueilli avec une périodicité d'un an, la CNIL recommande que les responsables de traitement alerte les personnes dans un délai raisonnable avant l'échéance de ce délai, pour que le renouvellement ne soit pas automatique.

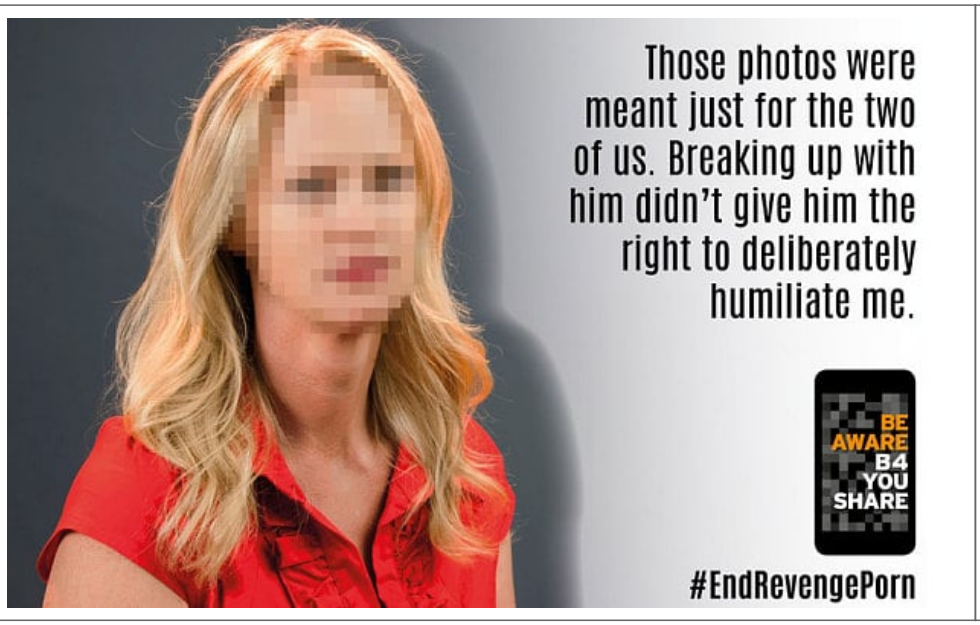
Un consentement renouvelé tous les ans

La loi pour une République numérique prévoit que le consentement doit être renouvelé périodiquement, c'est-à-dire recueilli tous les ans par les opérateurs exploitant les correspondances.
Par ailleurs, la CNIL rappelle que les traitements réalisés sur les correspondances doivent se limiter aux données collectées de manière loyale et licite. En conséquence, les traitements ne doivent produire des effets qu'à l'égard des personnes qui ont valablement consenti à la collecte de leurs données à caractère personnel issues du contenu de leurs correspondances. À titre d'exemple, les traitements opérés à des fins publicitaires et basés sur le contenu des correspondances ne doivent pas permettre à l'opérateur de cibler d'éventuelles personnes tierces dont les données personnelles apparaitraient dans la correspondance.
Enfin, la CNIL rappelle qu'une fois le règlement européen relatif à la protection des données, adopté, les responsables de traitement devront être en mesure de prouver que les personnes ont effectivement consenti au traitement et seront tenus de les informer de la possibilité de retirer leur consentement.

Réagissez à cet article

Source : *Secret des correspondances : un consentement renforcé des utilisateurs de services de communication électronique | CNIL*

Le « revenge porn » dans la loi pour une République numérique



Le « revenge porn » dans la loi pour une République numérique

---

Nous nous penchons ici sur une des nouvelles conquêtes de la loi du 7 octobre 2016 pour une République numérique.Nous avons déjà examiné certaines facettes de cette loi sur les questions d'e-réputation, notamment celle du droit à l'effacement pour les mineurs (notre actualité du 26 janvier 2017) et celle de la mort numérique (celle du 3 février). Voici à présent la prévention pénale du revenge porn, qui du reste vient de connaître une illustration judiciaire intéressante.

Par Didier FROCHOTN

Notion de *revenge porn*

On nomme sous cette élégante expression franglaise l'action qui consiste à se venger d'une personne en rendant publique des contenus pornographiques, réalisés avec ou sans accord de l'intéressé(e) mais qui n'a jamais donné son accord pour leur publication, dans le but évident de l'humilier. Il s'agit fréquemment de « retombées collatérales » d'une séparation de couple qui se passe mal. Il n'est pas nécessaire d'être footballeur professionnel pour se trouver au cœur d'une tourmente médiatique très traumatisante pour la victime, comme en témoigne certain(e)s de nos client(e)s qui en 'ont vécu une.

Le *revenge porn* face au droit

La Cour de cassation s'était déjà prononcée sur cette question le 16 mars 2016 (actualité du 18 mars) dans une affaire où elle avait alors écarté le délit pénal de publication d'image. Dans ce cas précis, la personne avait été consentante à la réalisation d'une vidéo d'ébats sexuels avec son conjoint, mais pas de sa mise en ligne après séparation.

Nous nous sommes montré quelque peu critique sur cette décision qui certes se bornait à appliquer l'interprétation stricte de la loi pénale. Nous montrions alors quelles autres voies la Cour aurait pu suivre. Et nous avions annoncé le futur renforcement de l'arsenal pénal en cas de vengeance par publication de contenus à caractère sexuel par la loi pour une République numérique alors en gestation.

Un renforcement de l'arsenal juridique pénal

L'article 67 de la loi du 7 mars 2016 est donc venu renforcer le code pénal en créant, sous les articles 226-1 et 226-2 (délit d'atteinte volontaire à l'intimité de la vie privée par transmission de propos tenus en privé ou par captation et diffusion d'image, puni d'un an de prison et de 45 000 € d'amende), un nouvel article 226-2-1 qui renforce les sanctions pénales dans les cas spécifiques de contenus à caractère sexuel…[lire la suite]

Réagissez à cet article

Source : *Le « revenge porn » dans la loi pour une République*

numérique

Samsung Galaxy S8 ou S8+ : Une première faille de sécurité dénichée



Samsung Galaxy S8 ou S8+ : Une première faille de sécurité dénichée

La semaine dernière, le géant Sud-Coréen Samsung dévoilait ses nouveaux Smartphones Galaxy S8 et S8+. Un enjeu important pour le constructeur qui souhaite retrouver une image de marque suite à ses déboires avec les batteries explosives de son Note 7. Mais alors que les nouveaux modèles S8 et S8+ ne sont pas encore commercialisés, une première faille vient d'être décelée, le système de reconnaissance faciale peut être en effet trompé par une simple photo.

Galaxy S8 : Le système de reconnaissance faciale déjoué par une simple photo

Quelques jours seulement après sa présentation officielle, le Samsung Galaxy S8 est déjà sous le feu des critiques. En effet, une vidéo mise en ligne le 29 mars par la chaîne iDeviceHelp montre un utilisateur déverrouiller un **Samsung Galaxy S8** à l'aide d'une simple photo. Le système de **reconnaissance faciale** censé être un procédé sécurisé montre donc déjà sa première faille !

Avec ses deux nouveaux modèles, le constructeur Samsung avait pourtant misé sur la sécurité avec la présence **d'un système de reconnaissance d'iris**, un lecteur d'empreintes digitales situé désormais au dos de l'appareil ainsi que la reconnaissance faciale, une manière rapide et aisée de déverrouiller le Galaxy S8 ou S8+…[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

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Samsung Galaxy S8 ou S8+ : Une première faille de*

Bug Butter : la plateforme collaborative de mise en relation entre pirates et forces de l’ordre

Bug Butter : la plateforme collaborative de mise en relation entre pirates et forces de l’ordre

La plateforme Bug Butter met en relation pirates et membres des forces de l'ordre autour d'une place de marché d'informations sensibles.

Après les plates-formes de Bug Bounty, qui visent à mettre en relation des experts en cybersécurité avec des entreprises, une nouvelle étape vient d'être franchie dans la « *plateformisation* » des relations humaines : en partenariat avec l'ANSSI, la société OPFOR Intelligence ouvre aujourd'hui Bug Butter, la première plateforme de mise en relation entre pirates et membres des forces de l'ordre.
Bug Butter a pour ambition de fluidifier le processus d'enquête tout en permettant aux pirates de mieux gérer leur capital informationnel et leur image. La plateforme a également pour objectif de pallier le manque de moyen des services d'enquêtes, en offrant à ces derniers un outil simple et transparent capable d'optimiser le taux de résolution des affaires pour un budget donné.
La plateforme se compose de trois parties essentielles : des profils de cybercriminels, des profils de cyber-enquêteurs et, au centre, une place de marché unique en son genre.
Concrètement, Bug Butter permet aux cybercriminels de s'enregistrer sur une plateforme conçue à l'image de LinkedIn : compétences techniques, exploits réalisés, mentors, affiliations récentes avec des groupes de cybercriminels en vue, ils peuvent créer un profil complet et moderne afin d'offrir une vision complète de leurs activités.
Toutefois, et contrairement aux plateformes sociales que l'on connaît actuellement, ce profil reste pour l'essentiel privé : seul le pseudo du pirate est visible par défaut. C'est ensuite au criminel de décider quelles informations il souhaite rendre visibles, à quel prix, et -surtout- à qui.
Car outre les pirates, la plateforme est ouverte aux membres des forces de l'ordre. Ces derniers peuvent eux aussi créer leur profil de manière similaire. Nationalité, unité de rattachement, centres d'intérêt (fraude aux outils de paiement, recel, harcèlement, moeurs, renseignement…), outils maîtrisés (EnCase, i2 Analyze, Palantir…) là aussi tout est fait pour que chaque investigateur puisse donner une vision à 360° de son activité et valoriser son image…[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

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Bug Butter : la plateforme collaborative de mise en*

relation entre pirates et forces de l’ordre