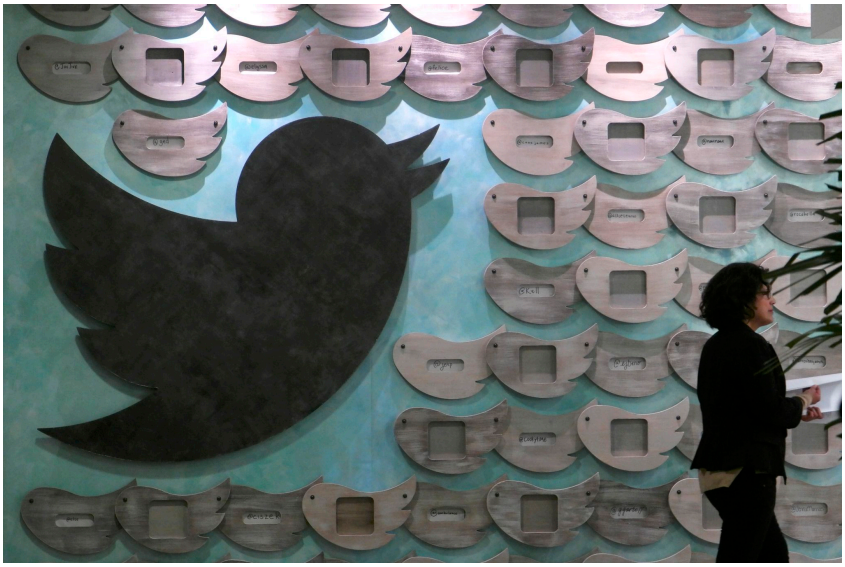
La lutte du cyberharcèlement sur Twitter grâce à l’intelligence artificielle



La lutte du cyberharcèlement sur Twitter grâce à l’intelligence artificielle

Le réseau social va s'aider d'outils d'apprentissage automatique pour repérer plus vite les messages allant à l'encontre de ses règles d'utilisation

Un concert d'excuses et quelques mesures concrètes. Après plusieurs années de silence et d'hésitation, Twitter promet que 2017 sera l'année de la lutte contre le harcèlement. Le réseau social présente trois nouveaux outils pour limiter l'influence des discours de haine et des attaques ciblés contre ses utilisateurs. Ils seront déployés à partir de mardi. D'autres fonctionnalités devraient être présentées dans le courant de l'année. «Nous avons entendu vos critiques. Nous n'avons pas progressé assez l'année dernière», avait déclaré Ed Ho, vice-président de Twitter, fin janvier. «Nous continuerons à être attentifs à vos retours, d'apprendre des critiques et de sortir des nouvelles fonctionnalités jusqu'à ce que tous nos utilisateurs ressentent ces changements.» Twitter va se reposer sur une nouvelle arme pour l'aider dans sa modération: l'intelligence artificielle.

Repérer plus rapidement les agressions

Le nouveau plan de Twitter comporte trois mesures phares. La première doit lutter contre la création abusive de nouveaux comptes par des utilisateurs déjà bannis du réseau social. Il est difficile de repérer ces internautes. Il changent généralement d'adresse mail, de numéro de téléphone et d'adresses IP pour s'inscrire à nouveau. Twitter va s'appuyer sur un programme d'apprentissage automatique afin de repérer les resquilleurs. Tout compte banni définitivement du réseau social sera analysé afin de repérer des signaux permettant d'identifier une personne, comme une manière de parler, des sujets ou des victimes de prédilection, des hashtags préférés, etc. Si un nouveau compte Twitter correspond à cette analyse, il pourra être rapidement supprimé.

Twitter crée également une nouvelle option pour masquer les images choquantes dans les recherches de tweets. Sont concernées les photos pornographiques ou violentes. Elles seront repérées automatiquement. Par exemple, une personne tapant «Bataclan» dans la barre de recherche de Twitter devrait en théorie ne pas voir de photos de la tuerie. Cet outil devrait aussi être utile pour les personnes faisant l'objet d'une campagne de dénigrement, afin de ne pas voir son pseudo associé à des images pornographiques ou violentes. L'option sera enclenchée par défaut, mais pourra être désactivée dans les réglages Twitter.

Dernier outil lancé par le réseau social: les réponses à un tweet seront bientôt classées par ordre d'intérêt. Les messages automatiquement détectés comme «peu intéressants» par Twitter seront relégués en bas. Parmi les critères examinés par le réseau social: si le compte est nouveau et ne suit aucune autre personne, s'il a déjà été signalé pour abus ou qu'il emploie des insultes.

Accélérer le signalement

L'intelligence artificielle ne va pas remplacer les modérateurs de Twitter. Elle interviendra pour accélérer le signalement de contenus. Comme les autres réseaux sociaux, Twitter applique une modération *a posteriori*: les utilisateurs doivent lui signaler les contenus problématiques pour qu'ils soient contrôlés et éventuellement supprimés s'ils enfreignent les règles d'utilisation. Le réseau social collabore aussi avec les autorités qui peuvent lui signaler des contenus illégaux. En France, plus de 466 tweets ont fait l'objet d'une demande de retrait par la police ou le gouvernement entre janvier et juin 2016…[lire la suite]

Réagissez à cet article

Source : *Twitter s’appuie sur l’intelligence artificielle pour lutter contre le harcèlement*

Les dangers des jouets connectés | Denis JACOPINI

Les dangers des jouets connectés | Denis JACOPINI

La gamme Cloudpets de Spiral Toys a été piratée. Plus de 800000 comptes ont été piratés avec les informations qui y sont liées et plus de 2,2 millions de messages vocaux se retrouvent également sur la toile. Les peluches connectées de la marque permettait en effet aux parents et aux enfants de s'échanger des messages par le biais d'une application téléphonique, à travers l'ours en peluche.

Denis JACOPINI a été Interviewé par la revue Atlantico à ce sujet :

Atlantico : Une société d'ours en peluche connectés a été récemment piratée, les messages laissés par les parents à leurs enfants sont désormais hackable. Ce n'est pas la première fois que ce type de piratage arrive, pour protéger nos enfants, devrions-nous les éloigner de ce type de jouets connectés ?
Denis JACOPINI : En effet, au-delà du risque relatif à la protection des données personnelles des enfants et de leurs parents, la revue Que choisir avait déjà alerté les consommateurs en fin 2016 sur des risques inhérents au connexions non sécurisée de plusieurs jouets connectés.
Qui a tenu compte du résultat de cette étude pour revoir la liste des jouets qui seraient présents dans la hotte légendaire ?
La relation entre les enfants et les jouets va bien au-delà de la technologie et des risques qu'elle peut représente.
Les jouets bénéficie également de phénomènes de mode et l'engouement, sauf erreur, se fout bien de la qualité des produits et encore moins de leur sécurité.
Manque de connaissance, inconscience, crédulité ou trop de confiance de la part des parents ? Il est vrai qu'on peut facilement croire que si des jouets se trouvent sur nos rayons, c'est qu'ils ont forcément dû passer avec succès toute une batterie de tests rassurant pour le consommateur.
Pour la part des jouets à usage familial testés, même si les normes EN71 et EN62115 ont été récemment révisées pour répondre aux exigences de la nouvelle directive 2009/48/CE, les validations se reposeront sur des niveaux satisfaisants en terme de propriétés physiques et mécaniques, d'inflammabilité, de propriétés chimiques, électriques ou bien relatives à l'hygiène et à la radioactivité.
Vous l'aurez remarqué, aucun test n'est prévu pour répondre à des mesures ne serait-ce que préventive en terme de protection des données personnelles et encore moins en matière se sécurité numérique.
Alors finalement, pour répondre à votre question : « devrions-nous éloigner les enfants de ce type de jouets connectés ? »
A mon avis, en l'absence de normes protectrices existantes, la prudence devrait être de mise. Certes, il est impossible de se protéger de tout. Cependant, il serait à minima essentiel que les parents soient informés des risques existants et des conséquences possibles que pourraient provoquer des piratages par des personnes mal intentionnées pour prendre des mesures qu'ils jugent utiles.

Atlantico : Comment pouvons-nous restreindre la possibilité de piratage de données pour ce type d'objet ?
D.J. : La situation confortable serait que le consommateur soit vigilant pour ce qui concerne les mesures de sécurité couvertes par l'appareil et celles qui ne le sont pas. Malheureusement, ces gardes-fous ne sont qu'à l'état d'étude.
Sauf à vous retrouver dans un environnement ou le voisin le plus proche se trouve à plusieurs dizaines de mètres, être prudent dans l'usage de ces objets pourrait par exemple consister à :
– Si le jouet le permet, changer le mot de passe par défaut et mettre en place un mot de passe complexe pour accéder à sa configuration ;
– Si le jouet le permet, activer les connexions sécurisées par cryptage ;
– Si le jouet le permet, désactiver les connexions à partir d'une certaine heure ;
– N'utiliser les jouets connectés que dans des environnements protégés, en raison de la portée limitée des communications Bluetooth (par des distances suffisantes entre le jouet et des pirates éventuels) ;
– Pour les jouets utilisant le Wifi,
– Mettre en place des protections physiques contre les rayonnements électromagnétiques dans certaines directions ;
– Cacher les caméras si elles ne sont pas utilisées ;
– En fin d'utilisation du jouet, ne pas se satisfaire d'éteindre l'appareil qui ne sera peut-être seulement en veille, mais retirer les piles ou placer le jouet dans un espace protégé (fabriquez une cage de Faraday) ;
Enfin, compte tenu que le bon fonctionnement du jouet est lié à l'acceptation des conditions contractuelles d'utilisation des donnés personnelles ne respectent pas les règles européennes relative à la protection de ces données et de la vie privée car les fabricants sont généralement situés hors Europe, ne pas accepter ces conditions reviendrait à être privé de l'usage des fonctions du jouet.

Atlantico : Concrètement, les objets connectés sont une porte ouverte à notre intimité, quels sont les dangers liés à ce type d'objets ?
A défaut d'information de la part des fabricants et d'alerte de la part des médias, il serait, à mon avis, adapté que le consommateur reconsidère les objets numériques et particulièrement les objets connectés comme étant des équipements dont les fonctions et conséquences induites risquent de se retourner contre son utilisateur.
L'année dernière, l'association de consommateurs UFC-Que choisir a mis en garde les consommateurs sur le stockage des données. Elle a d'ailleurs saisi sur le sujet la Commission nationale de l'informatique et des libertés et la Direction générale de la concurrence, de la consommation et de la répression des fraudes.
En effet, tout ce que disent les enfants à la poupée testée est enregistré et mystérieusement stocké sur des serveurs à l'étranger et géré par la société Nuance Communications. L'Association européenne de défense des consommateurs a déclaré : « Tout ce que l'enfant raconte à sa poupée est transmis à l'entreprise, basée aux États-Unis, Nuance Communications, spécialisée dans la technologie de reconnaissance vocale ».
Quelles sont les conséquences d'un tel usage de nos données ?
L'objectif évident est le matraquage publicitaire des enfants, car certains jouets ont une certaine tendance à faire souvent allusion à l'univers de Disney ou à Nickelodeon par exemple.
Enfin, des tests ont montré qu'un tiers situé à 20 mètres du jouet peut s'y connecter par Bluetooth et entendre ce que dit votre enfant à sa poupée ou à son robot, sans même que vous en soyez averti. La connexion peut même se faire à travers une fenêtre ou un mur en béton et le nom Bluetooth par défaut du jouet connecté, permet très simplement de les identifier.
Plus grave encore… Un tiers peut prendre le contrôle des jouets, et, en plus d'entendre votre enfant, communiquer avec lui à travers la voix du jouet.
Que ça soit en en terme d'écoute et d'espionnage à distance de l'environnement de l'enfant et de celui des parents, ou en terme de prise de contrôle à distance de l'appareil risquant de terroriser ou pire, traumatiser l'enfant, la prudence doit d'abord rester de mise.

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 : *Jouet connecté : après un piratage, les données de 800000 familles fuitent sur le web*

Le piratage informatique aussi risqué pour les animaux

Le piratage informatique aussi risqué pour les animaux

Pas évident d'y penser quand on n'est pas du milieu, mais au 21ème siècle, le braconnage se joue de plus en plus sur le terrain du numérique.

Le GPS, pour le meilleur comme pour le pire

Le balisage des animaux est une pratique qui date du début du XX^e^ siècle. **Après la pose de bagues sur les oiseaux au début du siècle, les scientifiques se sont tournés vers les transmetteurs radio dans les années 1950, avant de passer au système de suivi par satellite Argos dans les années 1970.** Aujourd'hui, c'est un autre système de suivi qu'utilisent les chercheurs : le GPS.

Cigogne équipée d'un GPS© Vasileios Karafillidis Shutterstock

Le GPS, tout le monde l'a dans son smartphone. Il nous facilite beaucoup la vie en nous aidant à nous retrouver dans une ville inconnue, en nous permettant d'appeler un taxi ou encore en nous rassurant lorsque nos enfants, rentrant seuls de l'école, utilisent leur smartphone pour partager avec nous leur localisation.

Mais au-delà de ces usages pratiques, s'en cache un plus obscur. Les balises GPS que les chercheurs placent sur les animaux ne sont pas des smartphones sophistiqués, il est donc assez facile de les pirater pour recevoir de manière indue ces données. Une faille que les braconniers exploitent à volonté, en mettant en danger la vie des animaux.

*Lire aussi : **la lutte contre le commerce en ligne de faune sauvage est engagée***

Le cyber-braconnage, un problème qui ne sera pas résolu du jour au lendemain

Le phénomène est encore trop peu connu et réservé au milieu des chercheurs…[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 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 : *Le piratage informatique, un risque pour les animaux*

Vous offrez aux hackers des données invisibles sans le savoir

Vous offrez aux hackers des données invisibles sans le savoir

Empreintes digitales, données GPS des photos, réponses aux questions prétendues «secrètes»…: des données sensibles se cachent sur ce que vous publiez sur les réseaux sociaux, même si l'essentiel du risque se concentre sur des informations livrées plus directement encore…

Le « V » de la victoire pourrait être celui des hackers. Un chercheur japonais avertissait début janvier contre le danger contenu dans ce signe parfois associé aux selfies: en montrant vos doigts, vous courez le risque de vous faire voler vos empreintes digitales, prévient Isao Echizu.
Alors que les «données sont le pétrole du 21ème siècle », comme on l'entend à l'envi, nous avons une fâcheuse tendance à livrer les nôtres, intentionnellement, sur les réseaux sociaux, en négligeant bien souvent les règles de confidentialité ou l'utilisation commerciale qui est leur est destinée. Mais la vigilance se complique quand on n'a même pas conscience qu'une donnée en est une…

Attention aux données invisibles…

Permettez-moi d'emprunter vos empreintes

Avec la haute résolution des photos prises par les smartphones, une opération – assez complexe, toutefois, et loin d'être à la portée de tout le monde – peut permettre de récupérer les empreintes. « Or à l'inverse des mots de passe, les empreintes, une fois volées, ne pourront jamais être changées», rappelle à *20 Minutes* Gérôme Billois, expert cybersécurité au cabinet Wavestone.
Il note que si l'avertissement du professeur japonais a fait le tour du monde, « on connaissait le risque depuis 2014 »: un hacker avait montré lors d'une conférence qu'il était parvenu à cloner les empreintes digitales de la ministre allemande de la Défense. Depuis, les empreintes digitales sont de plus en plus utilisées, pour déverrouiller smartphones, objets connectés ou pour réaliser certains paiements.

Des photos très bavardes

Autre donnée invisible, la géolocalisation associée aux photos, la grande majorité étant prise aujourd'hui par des smartphones équipés d'une puce GPS (qui ne sert pas qu'à vous guider sur la route jusqu'à Palavas-Les-Flots). Aux images numériques sont associées tout un ensemble de métadonnées, qui «peuvent renseigner la date, l'heure, voire les données GPS de l'image, la marque, le numéro de série de l'appareil ainsi qu'une image en taille réduite de l'image originale», comme le précise We Fight Censorship, qui indique la marche à suivre pour nettoyer ces métadonnées.«Internet abonde de ces images floutées dont le fichier EXIF contient toujours le document avant floutage», lit-on encore.
En septembre dernier, deux étudiants de Harvard ont pu démasquer 229 dealers grâce aux coordonnées géographiques contenues dans les métadonnées associées à des photos qu'ils avaient prises et postées en ligne.

En huit tweets, tout est dit

Sur Twitter, si la géolocalisation des tweets est désactivée par défaut, beaucoup l'activent. En mai dernier, des experts du MIT et d'Oxford démontraient que huit tweets (d'utilisateurs pour lesquels la géolocalisation est activée) suffisaient à localiser quelqu'un de façon très précise. « Il est extrêmement simple pour des personnes avec très peu de connaissance technique de trouver où vous travaillez ou vivez », expliquaient-ils, à l'issue d'une expérience concluante.

Le secret imaginaire des questions secrètes

Il y a enfin ces infos que nous livrons publiquement sur les réseaux sociaux alors qu'elles contiennent parfois les réponses aux questions censées être «secrètes». «Les questions secrètes sont le talon d'Achille des réseaux sociaux, souligne Gérôme Billois. Elles vous permettent d'accéder à vos comptes en cas d'oubli de mot de passe et ce sont toujours les mêmes: Quel est le prénom de votre mère? Quel est votre plat préféré? Or toutes ces infos peuvent être retrouvées facilement sur les réseaux sociaux.»

… et surtout aux données plus évidentes, qui permettent de personnaliser le phishing

Pour les scénarios ci-dessus, qui peuvent avoir le mérite d'attirer l'attention, la probabilité d'utilisation malveillante est pourtant « faible », assure Gérôme Billois. Parallèlement, «nous passons notre temps à livrer des informations hypersensibles», et de façon bien plus directe. Or l'occupation principale des cybercriminels reste les mails de phishing, et ces données les aident à les personnaliser.
«Si le mail est pointu, que c'est votre « bonne » banque qui vous dit qu'elle a remarqué votre passage à telle heure la veille, et que toutes ces infos sont correctes parce que vous avez partagé ces données sur les réseaux sociaux, il y a toutes les chances pour que vous cliquiez sur le lien malveillant.»…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous accompagner dans vos démarches de mise en conformité avec la réglement Européen relatif à la protection des données à caractère personnel (RGPD).
Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.
Par des actions de formation, de sensibilisation ou d'audits 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

Original de l’article mis en page : Sans le savoir, vous offrez aux hackers des données invisibles

---

Ressources pour la collecte et la vérification d’informations à destination des journalistes

Ressources pour la collecte et la vérification d’informations à destination des journalistes

---

Votre guide pour le traitement des contenus mis en ligne par des tiers, de la découverte à la vérification

Présentation de Samuel Laurent, éditeur délégué du Monde, partenaire de First Draft
L'éditeur délégué du Monde présente à First Draft ses travaux en matière de lutte contre la désinformation en ligne et ses projets…[Lire la suite]

Lancement de CrossCheck : à l'approche des élections françaises, les rédactions s'associent pour lutter contre la désinformation
CrossCheck réunit les compétences des secteurs des médias et des technologies pour s'assurer que fausses déclarations soient rapidement détectées et corrigées…[Lire la suite]

Outils pour renforcer la confiance envers les journalistes
Fort de son expérience dans le paysage journalistique américain, Josh Stearns nous présente des outils pour que journalistes et rédactions regagnent la confiance de leur audience…[Lire la suite]
Outils et ressources : Hearken, Engaging News Project, Coral ProjectNews Voices Engaged Newsroom Toolkit

Guide pour la vérification visuelle des vidéos
Il s'agit d'un guide de référence rapide pour vous aider à identifier le qui, quoi, où, quand et pourquoi des vidéos des internautes…[Lire la suite]

Guide pour la vérification visuelle des photos
Il s'agit d'un guide de référence rapide pour vous aider à identifier le qui, quoi, où, quand et pourquoi des photos mises en ligne par des tiers…[Lire la suite]

Utiliser Google Earth pour vérifier des images comme un pro
Google Earth offre bien plus que des images satellites…[Lire la suite]

Réseaux sociaux et contenus viraux : comment les développeurs des rédactions peuvent-ils faciliter la démystification ?
Les nouveaux projets de vérification doivent tenir compte des leçons clés tirées des procédés de « fact-checking » (vérification par les faits) ayant faits leurs preuves, tout en les adaptant aux écosystèmes des réseaux sociaux…[Lire la suite]
Savoir où chercher : sources d'image pour la géolocalisation
Trouver d'autres photos ou vidéos d'un lieu peut être un des meilleurs moyens de vérifier le lieu où a été capturé un contenu. Voici où chercher…[Lire la suite]
10 façons de mieux couvrir le terrain pour les journalistes locaux
Combiner le reportage traditionnel sur le terrain et les possibilités offertes par les services numériques modernes peut faire la différence entre un bon et un très bon journaliste…[Lire la suite]
Respecter la source : l'importance du témoin dans la couverture de l'actualité en temps réel
Les témoins sont des personnages clés dans de nombreux événements majeurs se produisant aux quatre coins du monde…[Lire la suite]
Comment se protéger face aux contenus traumatisants ?
Sam Dubberley, cofondateur de Eyewitness Media Hub, détaille certains des résultats principaux d'une étude récente portant sur les traumatismes indirects dans les rédactions…[Lire la suite]

Réagissez à cet article

Original de l’article mis en page : First Draft News FR – Votre guide pour le traitement des contenus mis en ligne par des tiers, de la découverte à la vérification

---

Le FBI pourra t-il accéder aux mails de Gmail ?

Le FBI pourra t-il accéder aux mails de Gmail ?

Le juge fédéral Thomas Rueter de la cour de Philadelphie a donné son verdict et a statué concernant la saisie de mails depuis des serveurs étrangers, par les autorités américaines. Ce dernier a affirmé : «Même si la récupération de données électroniques par Google à partir de ses multiples centres de données à l'étranger peut en soi représenter un risque d'atteinte à la vie privée, la véritable atteinte intervient au moment de la divulgation aux Etats-Unis».

En gros, le juge fédéral a estimé que le fait d'ordonner à Google de remettre aux autorités les courriers électroniques de sa messagerie Gmail, stockés à l'étranger, n'était pas contraire à la loi. La firme de Mountain View devra se conformer aux mandats et perquisitions du FBI. Google a évidemment déclaré qu'il faisait appel de la décision, en se référant à la jurisprudence Microsoft, car une affaire similaire avait donné raison à Microsoft il y a quelques semaines à New York.

Google devra fournir au FBI les mails hébergés à l'étranger

Google ne souhaite pas livrer au FBI les e-mails stockés hors des Etats-Unis, afin de garantir la vie privée de ses usagers aux quatre coins du monde. Sont concernés par la décision du juge fédéral Thomas Rueter, les six serveurs de l'entreprise présents en Belgique, en Finlande, en Irlande, à Taïwan, Singapour et aux Pays-Bas.
Le juge a estimé qu' « *aucune ingérence significative* » avec les droits de propriété du titulaire du compte ne pouvait être invoquée concernant les données ciblées, car comme l'a fait remarquer le juge, Google procède déjà régulièrement au transfert de ces données vers ses serveurs aux Etats-Unis, pour ses propres business et sans que les clients en soient forcément informés. Thomas Rueter de la cour de Philadelphie a souligné : *« Ces transferts n'interfèrent pas avec l'accès du client ou les droits de propriété des données utilisateur. Même si le transfert interfère avec le contrôle du propriétaire du compte sur ses informations, cette interférence est minime et temporaire ».*
Il semble donc que le juge ait retourné les méthodes de Google contre lui-même pour justifier la légalité des saisies des e-mails stockés hors des Etats-Unis au FBI. Du côté de l'entreprise, on s'est contenté de déclarer : *« Nous continuerons à repousser les mandats excessifs ».*

Original de l'article mis en page : Le FBI pourra bien accéder aux mails de Gmail situés à l'étranger

---

A Lire aussi :
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Le RGPD, règlement européen de protection des données. Comment devenir DPO ?
Comprendre le Règlement Européen sur les données personnelles en 6 dessins
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

Notre métier : Vous accompagner dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits 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

Original de l'article mis en page : Le FBI pourra bien accéder aux mails de Gmail situés à l'étranger

---

Apprenez à vous protéger contre le piratage de vos objets connectés du quotidien

Apprenez à vous protéger contre le piratage de vos objets connectés du quotidien

Souhaitant mettre rapidement sur le marché leurs produits, les fabricants d'objets connectés ont eu tendance à négliger l'aspect sécurité, contribuant ainsi à la vulnérabilité de leurs utilisateurs face à de possibles attaques.

Atlantico : En septembre et octobre 2016, deux attaques DDOS ont été particulièrement marquantes : la première sur l'entreprise OVH et la deuxième sur DYN. Dans les deux cas, ces attaques ont été rendues possibles par les objets connectés. Malgré l'ampleur de ces attaques, celles-ci sont à relativiser. Dans une récente étude réalisée pour le compte de l'entreprise HSB, on note que seulement 10% des utilisateurs ont été touchés par des problèmes de piratage. Quels sont les risques du piratage des objets connectés ?

Quel peut être le préjudice porté aux particuliers et aux entreprises ?

Yvon Moysan : Une attaque DDoS ou attaque par déni de service massive vise à **rendre un serveur, un service ou une infrastructure indisponibles en surchargeant la bande passante du serveur, ou en accaparant ses ressources jusqu'à épuisement.** Lors d'une attaque DDoS, une multitude de requêtes sont envoyées simultanément et depuis de multiples endroits. L'intensité de ce « tir croisé » rend le service instable, voire indisponible. **Le risque d'être confronté à ce type d'attaque est important et surtout les tentatives sont nombreuses**. Dans le cas de la société américaine Dyn que vous évoquez, celle-ci a été victime d'une attaque de plus d'un Téra-octet par seconde, ce qui pourrait concerner environ 10 millions d'objets connectés piratés. Ce niveau d'intensité est toutefois très rare.

Le préjudice subi dépend du type d'objets connectés piratés et du caractère sensible des données des particuliers. Si la majorité des objets connectés contiennent rarement des informations aussi sensibles que celles qui sont stockées sur un ordinateur, **il en existe des sensibles comme les voitures connectées ou les fusils intelligents qui, piratés à distance, peuvent représenter un véritable danger, potentiellement mortel pour l'utilisateur.** Et **ce risque s'est d'ores et déjà avéré.** Des experts en sécurité informatique ont ainsi réussi à prendre le contrôle à distance d'une Jeep Cherokee. Ils ont pu agir sur la vitesse, freinant et accélérant à leur guise, envoyant même la voiture dans le fossé alors que pour le fusil intelligent, d'autres experts ont réussi a bloqué le déclenchement du tir.

Le risque existe également pour des objets plus communs comme les applications de smart home. Des hackers ont ainsi réussi à bloquer la température de thermostats connectés à une température polaire ou saharienne. Plus préjudiciable, des hackers ont pris le contrôle de caméras de surveillance, récupéré les vidéos enregistrées, et au final les ont diffusées sur le Web. Un baby phone a également été la cible d'un hacker terrorisant un bébé et ses parents. En prenant le contrôle de l'appareil équipé d'une caméra, d'un micro et d'un haut-parleur, celui-ci s'est mis à hurler des insanités sur le nourrisson. **Le risque peut surtout être généralisé si des hackers réussissent à prendre le contrôle des réseaux d'électricité ou de gaz sur un quartier par exemple.** Il devient en effet possible de plonger toute une zone dans le noir ou, en fonction des données récoltées sur la consommation, de savoir quelles habitations sont occupées ou pas, en vue d'éventuels cambriolages.

Cela peut ensuite être contraignant pour la société qui a fabriqué et vendu les objets piratés car cela révèle **la faiblesse du niveau de sécurité**. Dans le cas de l'attaque de la société Dyn, une partie des objets connectés étaient ceux de la société chinoise Xiongmai, qui a dû les rappeler en urgence pour leur appliquer un correctif de sécurité. Cela peut aussi être problématique pour les clients de la société victimes de l'attaque. Dans le cas de Dyn, cela a eu pour conséquence de rendre inaccessible pendant une dizaine d'heures des sites comme Twitter, Ebay, Netflix, GitHub ou encore PayPal.

On peut aussi s'interroger sur certaines pratiques des constructeurs. Le fait de mettre un mot de passe commun à tous les appareils avant une première connexion a déjà été pointé du doigt. Quels autres dysfonctionnements peut-on mettre en avant ? Face à l'augmentation du nombre d'objets connectés, comment s'adaptent précisément les constructeurs en termes de sécurité ?

Tout d'abord il est important de préciser que ce type d'attaques par déni de service n'a rien de nouveau : les cybercriminels utilisent depuis des années des armées d'ordinateurs piratés pour inonder de requêtes les sites ciblés et les rendre inaccessibles.

La nouveauté réside ici dans le nombre croissant des objets connectés qui accroit de manière exponentielle les possibilités d'attaques. Or **la puissance d'une attaque dépend essentiellement du nombre de périphériques piratés, d'où l'intérêt de passer par les objets connectés**. Il existe en effet **plusieurs milliards d'objets connectés dans le monde contre quelques centaines de millions d'ordinateurs.** Pour y faire face, il existe des solutions proposées par les hébergeurs pour protéger leurs serveurs des attaques. Ces solutions permettent, par exemple, d'analyser en temps réel et à haute vitesse tous les paquets, et si besoin d'aspirer le trafic entrant, voire de mitiger, c'est-à-dire repérer tous les paquets IP non légitimes, tout en laissant passer les paquets IP légitimes.

Du côté des constructeurs d'objets connectés, tous les thermostats, toutes les webcams ou les imprimantes ne présentent pas de faille de sécurité, mais il s'agit d'un point préoccupant car **pour la plupart des fabricants, la sécurité n'a pas été la priorité dès le départ**, **ayant souvent été donnée à la rapidité de la mise à disposition du produit sur le marché pour répondre à un nouveau besoin**. Il faudrait que des normes minimales de sécurité puissent être définies comme le cryptage des données échangées sur le réseau ou l'exigence de mot de passe sécurisé mêlant caractères spéciaux et chiffres pour l'accès à distance et l'interdiction de mots de passe comme « 123456 » particulièrement vulnérables. Dans cet esprit, la Online Trust Alliance, qui regroupe des éditeurs comme Microsoft, Symantec (Norton) et AVG, a rédigé un guide des bonnes pratiques pour minimiser les risques de piratage. Les constructeurs d'objets connectés peuvent, par ailleurs, faire évaluer leurs systèmes de cryptage par des sociétés spécialisées, pour identifier les éventuelles vulnérabilités.

Comment se prémunir du piratage d'objets connectés ? Quels sont les bons comportements à adopter ? Que faire en cas de doute ?

Du côté des particuliers, il apparait préférable de privilégier les produits de sociétés à la pointe des questions de sécurité informatique, comme Google ou Apple. Il faut également installer régulièrement **les mises à jour de sécurité et les mises à jour logicielles**, pour limiter le nombre de vulnérabilités connues qui pourraient être exploitées. Après, il faut **changer le nom et le mot de passe par défaut de chaque objet connecté, car c'est la première chose qu'un hacker tentera d'attaquer pour en prendre le contrôle.** Pour finir, il faut **limiter l'accès d'un objet connecté aux autres objets connectés dans la maison.** Par exemple, si vous avez une Smart TV, vous devrez restreindre l'accès à cette TV et autoriser seulement son accès à des ressources particulières du réseau. Par exemple, il n'est pas vraiment nécessaire que l'imprimante soit connectée à la télévision.

Réagissez à cet article

Original de l’article mis en page : Attention danger : apprenez à vous protéger contre le piratage de vos objets connectés du quotidien | Atlantico.fr

---

Privacy Shield et donnés personnelles : un décret de Trump inquiète

Un décret adopté par Donald Trump menace potentiellement le Privacy Shield, l’accord censé veiller à la protection des données personnelles des citoyens européens exportées aux États-Unis par des entreprises comme Google et Facebook. La Commission européenne se veut rassurante mais affirme sa vigilance.

Privacy Shield et donnés personnelles : un décret de Trump inquiète

---

Un décret adopté par Donald Trump menace potentiellement le Privacy Shield, l'accord censé veiller à la protection des données personnelles des citoyens européens exportées aux États-Unis par des entreprises comme Google et Facebook. La Commission européenne se veut rassurante mais affirme sa vigilance.

L'accord Privacy Shield, qui présume que les données personnelles des Européens exportées aux États-Unis par des entreprises bénéficient du même degré de protection qu'en droit européen, aura nécessité de longs mois de négociation entre les États-Unis et l'Union européenne avant d'être adopté en juillet dernier.
Si de grands noms du milieu, comme Microsoft, Google et Facebook n'ont pas tardé à s'engager à le respecter – alors que de nombreuses critiques perdurent à son sujet – son application est désormais directement menacée par Donald Trump.

EXCLUSION DES « NON-CITOYENS AMÉRICAINS »

La quatorzième clause du décret « *d'amélioration de la sécurité publique au sein des États-Unis* » – le fameux texte anti-immigration de Trump – signé cette semaine par le 45ème président affirme en effet : « *Les agences* [comme la NSA et le FBI] *devront, dans la mesure permise par la loi en vigueur, s'assurer que leurs politiques de protection des données personnelles excluent les non-citoyens américains et les non-résidents permanents autorisés, des protections offertes par le Privacy Act au regard des informations personnelles identifiables.* »
Le rapporteur du Parlement européen en matière de protection de données, Jan Philipp Albrecht, n'a pas caché son inquiétude sur Twitter : « *Si cela est confirmé, la Commission européenne doit immédiatement suspendre le Privacy Shield et sanctionner les États-Unis d'avoir violé l'accord* ».
Suivre

Jan Philipp Albrecht
✔@JanAlbrecht
If this is true @EU_Commission has to immediately suspend #PrivacyShield & sanction the US for breaking EU-US umbrella agreement. #CPDP2017 https://twitter.com/cobun/status/824398742275104768 …
10:45 – 26 Janv 2017

LA COMMISSION EUROPÉENNE SE VEUT RASSURANTE

La Commission européenne, elle, a tenu à se montrer rassurante en indiquant que le Privacy Shield ne dépendait pas du Privacy Act, le texte de 1974 qui encadre l'usage des données personnelles de citoyens américains par les agences fédérales : « *Nous sommes au courant du décret qui a été adopté. Le Privacy Act américain n'a jamais garanti la protection des données personnelles des Européens.* » Cette affirmation contredit pourtant une déclaration antérieure de l'Union européenne à propos du Privacy Act.

Dans une explication de septembre 2015 sur le contenu du Privacy Shield, elle le présentait en effet comme une « *extension du cœur des garanties juridiques* » fournies par le Privacy Act. L'adoption du Privacy Shield a été permise par le Judicial Redress Act adopté par Barack Obama en 2014, une extension directe des garanties du Privacy Act aux citoyens non-Américains.
L'Union européenne affirme tout de même sa vigilance : « *Nous continuerons à suivre de près […] le moindre changement aux États-Unis qui pourrait avoir un impact sur les droits des Européens en matière de protection de leurs données personnelles* »…[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 de formation, de sensibilisation ou d'audits 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

Forum International de la

Cybersécurité 24 et 25 janvier 2017 à LILLE

Forum International de la Cybersécurité 24 et 25 janvier 2017 à LILLE

Lille grand palais accueille à partir de ce mardi 24 janvier à 09:30 la 9ième édition du Forum International de la Cybersécurité.

Favoriser l'innovation

Résolument tournée vers l'innovation, les écoles Epitech ont développé au sein de chaque campus des Innovation, des espaces dédiés aux expérimentations, au prototypage et au développement de projet innovants. Ces Hub reposent sur une méthodologie collaborative et transversale, reposant sur 5 domaines de compétences permettant de balayer le champ des innovations dont celui de la sécurité.

Ainsi, situé au sein de l'Espace Carrières, réunissant des écoles spécialisées, des étudiants d'Epitech et des encadrants pédagogiques proposeront des démonstrations d'attaques/défense lors des Hacking Trucks du Forum.

Les démonstrations proposées par l'Epitech :

• Démonstration de la facilité d'interception et d'altération des communications sur le(s) réseau(x) GSM et/ou Wi-Fi, par l'interception de SMS, de conversations vocales (pour le GSM) et autres communications quelconques (pour le Wi-Fi),

• Démonstration Ransomware : Démonstration du mode opératoire et des conséquences d'une campagne d'attaque par rançongiciel,

• Hacking Live : Démonstration d'une attaque en live d'une plateforme CMS Web, de la découverte de la faille Web jusqu'à la prise de contrôle du serveur l'hébergeant,

• Poisontap : À l'aide d'un matériel peu coûteux, il suffira de quelques minutes à nos étudiants démonstrateurs pour siphonner les communications d'un ordinateur, même verrouillé.

Ces démonstrations ont pour but de sensibiliser tout visiteur sur la protection des données, notamment avec le développement des usages et des nouvelles technologies afin que les consommateurs soient de plus en plus soucieux de leur sécurité tout en gardant un confort d'utilisation. Le FIC est un événement gratuit dont l'inscription est soumise à la validation des organisateurs…[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 de formation, de sensibilisation ou d'audits 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

Original de l’article mis en page : Lille FIC 2017

La CIA donne accès à des millions de pages sur son histoire et ses opérations secrètes

La CIA propose un moteur de recherche pour explorer sa base de données, composée de 930 000 documents confidentiels qui ont été déclassifiés. L’agence lève ainsi le voile sur une partie de son histoire, bien souvent méconnue.…[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 de formation, de sensibilisation ou d’audits

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 sur cette page.

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

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

Contactez-nous

Réagissez à cet article