Alerte Que Choisir sur les jouets connectés et nos données personnelles

	Alerte Que Choisir sur les jouets connectés et nos données personnelles

A l'approche de Noël et face à la multiplication des offres de jouets connectés pour enfants dans les rayons de magasins ou sur Internet, l'UFC-Que Choisir dénonce aujourd'hui, sur la base d'une analyse technique, des lacunes quant à la sécurité et la protection des données personnelles des enfants utilisateurs de la poupée connectée 'Mon amie Cayla' et du robot connecté 'i-Que' disponibles chez de nombreux vendeurs en France. Sur la base de ces inquiétants constats, l'association saisit la CNIL et la DGCCRF.

L'étude technique commanditée par notre homologue norvégien, Forbrukerradet, souligne que Cayla et i-Que, en apparence inoffensifs, ne garantissent pas le respect de la vie privée et de la sécurité des données personnelles de vos enfants.

Faille de sécurité du Bluetooth intégré

Ces jouets disposent d'un microphone intégré qui se connecte par Bluetooth à une application mobile, préalablement téléchargée par l'utilisateur sur son smartphone ou sa tablette. Le jouet peut alors comprendre ce que lui dit l'enfant et y répondre. Mais, les sociétés fabricantes, ont fait le choix d'implanter dans Cayla et i-Que, une technologie Bluetooth sujette à des risques de failles de sécurité élevées.

En effet, si les sociétés ont fait le choix d'une connexion simple et rapide, aucun code d'accès ou procédure d'association entre ces jouets et les téléphones/tablettes n'est exigé avant la connexion au jouet, ce qui garantirait pourtant que seul le propriétaire puisse s'y connecter. Résultat : 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 du Bluetooth, « Cayla » et « i-Que », permet très simplement d'identifier les poupées. 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.

Conditions contractuelles et utilisation des données personnelles

La protection des données personnelles des utilisateurs français est prévue par la loi Informatique et Libertés mais semble avoir été oubliée par les sociétés fabricantes.

Les conditions contractuelles les autorisent, sans consentement express, à collecter les données vocales enregistrées par Cayla et i-Que, et ce, pour des raisons étrangères au stricte fonctionnement du service. Ces données peuvent ensuite être transmises, notamment à des fins commerciales, à des tiers non identifiés. Les données sont aussi transférées hors de l'Union européenne, sans le consentement des parents: « aux Etats-Unis, ou vers les autres territoires concernés où les lois sur la protection de la vie privée ne sont peut-être pas aussi complètes que celles du pays où vous résidez et/ou dont vous êtes ressortissant»!

Matraquage publicitaire ciblé

Les sociétés fabricantes n'hésitent pas à faire de la publicité ciblée à destination de vos enfants. Les conditions contractuelles supposent que le simple fait de visualiser une publicité ciblée, constitue de votre part, un accord express à recevoir de telles publicités ciblées. L'étude a ainsi révélé que Cayla et i-Que prononcent régulièrement des phrases préprogrammées, faisant la promotion de certains produits – notamment des produits Disney ou des références aux dessins animés de Nickelodeon.

Loin d'être des cas isolés, Cayla et i-Que reflètent un problème général de sécurité et de données personnelles des jouets connectés. En effet, l'étude commanditée par nos homologues norvégiens souligne que la poupée Hello Barbie *(pas encore commercialisée en France)* est sujette aux mêmes griefs.

Au vu de ces éléments inquiétants, l'UFC-Que Choisir:

• appelle les parents à réfléchir à deux fois avant d'acheter la poupée Cayla et le robot i-Que ; rappelle qu'en cas de vente à distance, ils bénéficient d'un délai de rétractation de 14 jours. Pour ceux déjà équipés et qui souhaitent le conserver, l'association les invite à n'utiliser le jouet connecté qu'en leur présence, ou à défaut de l'éteindre.

• saisit d'une part la CNIL pour qu'elle diligente sans délai un contrôle du respect de la protection des données personnelles des utilisateurs de la poupée Cayla et du robot i-Que, et d'autre part, la DGCCRF afin que ses services enquêtent sur le niveau de sécurité des jouets connectés et sanctionnent tout manquement aux dispositions légales et réglementaires.

Réagissez à cet article

Original de l’article mis en page : Jouets connectés et données personnelles – UFC-Que Choisir

---

900 000 routeurs de Deutsche Telekom infectés par un malware

Deutsche Telekom a confirmé la thèse d'un malware ayant infecté plus de 900.000 de ses routeurs. Selon Flashpoint, environ 5 millions de routeurs à travers le monde seraient vulnérables à la faille exploitée par cette variante de Mirai.

Le Cert-FR alerte les utilisateurs français sur cette attaque. L'équipe rappelle ainsi que « plusieurs version du binaire malveillant sont en circulation ». Le Cert-FR recommande de changer les mots de passe par défaut, de restreindre l'accès aux outils d'administration et de désactiver « les services inutilement lancés sur les équipements exposés sur le réseau. »
Mirai se tourne vers de nouvelles cibles et la nouvelle version du ver informatique s'attaque maintenant aux routeurs. On avait déjà constaté par le passé des variantes de ce malware modifiées afin de s'attaquer à de nouveaux appareils. Mais l'attaque ayant visé Deutsche Telekom montre que les opérateurs de cette nouvelle variante entendent maintenant changer de cible et délaisser les objets connectés pour s'attaquer aux routeurs.

Comme l'explique Flashpoint dans une note de blog, la mise à disposition du code source de Mirai par son créateur a entraîné une guerre entre les cybercriminels, alors que plusieurs groupes tentaient d'utiliser Mirai pour prendre le contrôle du maximum d'objets connectés vulnérables. « L'évolution logique pour ce malware était de découpler le mécanisme d'infection de la charge utile du malware, en exploitant un nouveau vecteur d'attaque » précise ainsi Flashpoint sur son blog.
La dernière déclinaison de Mirai n'exploite donc plus simplement Telnet pour tenter de se connecter à des objets connectés en utilisant les identifiants par défaut. Selon Flashpoint, celle-ci exploite des vulnérabilités connues au sein des protocoles TR-064 et TR-069, des protocoles de maintenance utilisés par les opérateurs. C'est grâce à cette faille que les opérateurs du réseau botnet sont parvenus à infecter plus de 900.000 routeurs livrés par Deutsche Telekom à ses clients. Mais selon Flashpoint, l'opérateur allemand n'est pas le seul à devoir s'inquiéter de ce type d'attaques. Flashpoint évoque ainsi le fait que des appareils infectés ont également été détectés au Brésil et en Grande-Bretagne. Selon Flashpoint, environ 5 millions de routeurs à travers le monde sont vulnérables à cette nouvelle variante.
Reste à déterminer l'origine de l'attaque contre l'opérateur. Flashpoint précise que les administrateurs de cette variante semblent être des habitués de Mirai, puisque le nouveau malware présente plusieurs points communs (notamment des serveurs de command and control) avec des Botnets déjà identifiés lors d'attaques précédentes effectuées grâce à Mirai.
Selon le journal allemand Tagesspiegel, les soupçons se tournent vers la Russie. Dans une prise de parole, la chancelière Angela Merkel s'est refusée à confirmer cette thèse, mais précise néanmoins que de nombreuses cyberattaques ont été constatées en Europe et appelle ses citoyens à s'habituer à ce type d'attaques. Cité par la presse locale, le directeur de l'équivalent allemand de l'Anssi, le BSI, évoque de son côté « le crime organisé » à l'origine de l'attaque, mais rappelle que l'attaque n'a pas fonctionné. Le malware a bien déconnecté les routeurs des abonnés, mais celui-ci n'est pas parvenu à s'installer correctement. Plus de peur que de mal donc…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : Deutsche Telekom : 5 millions de routeurs vulnérables au malware – ZDNet

---

14 millions de Français victimes des pirates Informatiques en 2016

	14 millions de Français victimes des pirates Informatiques en 2016

La prolifération des cyberattaques a un corollaire : aucune classe d'âge et aucune profession ne sont aujourd'hui épargnées. Explications.

Dans un rapport publié mercredi 16 novembre, l'éditeur d'antivirus Symantec-Norton pointe l'ampleur que le phénomène « cybercriminel » a prise en 2016. Selon cette étude, 13,7 millions de Français auront été victimes d'attaques informatiques cette année. Le fait d'avoir baigné dans l'univers numérique depuis sa naissance ne change rien à la donne. Les « digital natives » (comme les experts désignent les jeunes qui manipulent des ordinateurs depuis le berceau) sont aussi démunis face à cette menace que leurs aînés.
La génération Y, celle des 18-34 ans, fait ainsi partie des plus touchées par le problème. Il faut dire que cette catégorie de population se comporte sur le Web de manière particulièrement risquée. Or, pour les professionnels de la cybersécurité, la négligence des internautes serait en cause dans la plupart des attaques informatiques dont ils sont victimes.

Des internautes imprudents

Bien que 77 % des Français sachent qu'ils doivent protéger leurs données en ligne, les utilisateurs gardent de mauvaises habitudes sur le Web. Les réflexes d'élémentaire prudence sont de peu de poids face à l'attrait de certains liens… même d'origine douteuse. Ainsi, 65 % des Français reconnaissent avoir déjà ouvert une pièce jointe postée d'un expéditeur inconnu. Et quasiment un internaute sur cinq partage ses mots de passe avec d'autres utilisateurs. Faut-il, dès lors, s'étonner qu'un Français sur deux se résigne à l'idée qu'il est désormais plus probable qu'une personne accède frauduleusement à ses appareils domestiques connectés qu'à son logement ?
D'après Laurent Heslault, directeur des stratégies numériques chez Symantec, les internautes ont bien conscience des dangers mais « n'ont pas envie de prendre les précautions adéquates pour assurer leur sécurité ». Alors que les cybercriminels, eux, disposent de techniques de plus en plus recherchées pour arriver à leurs fins.
Il ne s'agit pas seulement de paresse chez les internautes. 31 % d'entre eux sont dépassés par la quantité d'informations qu'ils ont à protéger. La plupart considèrent d'ailleurs que la question de la gestion sécurisée des données ne les concerne pas et qu'il appartient aux fournisseurs d'accès à Internet et aux entreprises du secteur des nouvelles technologies de résoudre ces problèmes.

Un problème mondial

Une étude réalisée en octobre, par le Ponemon Institute pour le compte de l'éditeur de logiciels professionnels Varonis Systems, démontre qu'il ne s'agit pas d'un problème strictement hexagonal. Si 37 % (seulement !) des internautes français indiquent qu'ils prennent toutes les mesures appropriées pour protéger les données auxquelles ils accèdent et qu'ils utilisent, la même réponse est donnée par 50 % chez les collaborateurs allemands, 39 % des employés britanniques et 35 % des employés américains.
Le nombre d'entreprises ayant fait l'expérience des ransomwares l'an dernier est en hausse constante. Ces logiciels rançonneurs, dont le FBI a révélé qu'ils avaient généré, au premier semestre 2016, plus de 209 millions de dollars de butin, ont infecté les serveurs de 12 % des entreprises allemandes, contre 17 % aux États-Unis, 16 % en France et 13 % au Royaume-Uni. Le nombre de cas de perte ou de vol de données au cours des deux dernières années a, lui aussi, explosé… Et l'on ne compte plus les cyberbraquages signalés chaque semaine à travers la planète.
De quoi inciter les États à renforcer leur arsenal pour lutter plus efficacement contre les gangs à l'oeuvre sur la Toile. Les 68 pays signataires de la convention de Budapest, le premier traité international abordant la question de la lutte contre la cybercriminalité adopté en 2001, se sont d'ailleurs réunis les 14 et 15 novembre derniers pour renforcer leur coopération en la matière. Un protocole additionnel à la convention sera adopté courant 2017 pour mettre en place un nouvel outil juridique permettant de collecter des preuves électroniques sur le « cloud », quelle que soit la localisation du serveur qui l'héberge… Preuve, s'il en était besoin, que les gouvernements du monde entier ont pris la mesure de la menace.

Quels sont les cyberdélits les plus fréquents en France ?

• Le vol de mot de passe (14 %)
• le piratage électronique (11 %)
• le piratage des réseaux sociaux (10 %)
• la fraude à la carte de crédit (9 %)
• le ransomware ne représente que 4 % des actes de cybercriminalité contre les particuliers (mais 12 % des entreprises), soit environ 548 000 cas en 2015. 30 % des victimes de ransomware ont payé la rançon demandée et 41 % d'entre eux n'ont pas pu, malgré tout, récupérer leurs fichiers. [Article Original du Point]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l'article mis en page : Cybersécurité : un

Français sur cinq victime de hackers en 2016

Contrôles biométriques en entreprise : vos obligations changent !

	Contrôles biométriques en entreprise : vos obligations changent !

Le cadre légal régissant la mise en place de dispositifs biométriques en entreprise évolue. En effet, la Cnil a adopté le 30 juin 2016, suite aux exigences fixées par le règlement européen sur la protection des données personnelles (2), 2 autorisations uniques, publiées au journal officiel le 27 septembre 2016.

Ces autorisations uniques fixent un nouveau cadre légal afin d'encadrer le recours aux dispositifs biométriques et protéger au mieux les libertés individuelles des personnes concernées par de tels systèmes d'identification.
Ainsi, les entreprises ayant recours à la mise en place de dispositifs biométriques ne seront plus soumises à une autorisation préalable de la Cnil. Elles devront simplement réaliser une demande d'autorisation unique et se conformer aux obligations prévues par l'autorisation.

La Cnil distingue désormais 2 types de dispositifs :
1/ l'autorisation unique 052 (3) pour les dispositifs garantissant la maîtrise par la personne concernée sur son gabarit biométrique. Ce peut être soit :
– un système recourant au stockage des données biométriques sur un support individuel détenu par les personnes concernées ;
– si la détention d'un support dédié au seul stockage du gabarit n'est pas adaptée à l'architecture et au contexte d'exploitation du dispositif, le responsable du traitement peut, de manière alternative, assurer le verrouillage des données biométriques stockées en base, par un secret détenu uniquement par la personne concernée ;
Dans ces deux hypothèses, l'utilisation du gabarit biométrique est conditionnée à une action de la personne concernée en tant que détentrice du gabarit ou du secret permettant de le déverrouiller.

2/ l'autorisation unique 053 (4) pour les dispositifs reposant sur une conservation des gabarits en base par le responsable du traitement.
Un « gabarit » biométrique désigne les mesures qui sont mémorisées lors de l'enregistrement des caractéristiques morphologiques, biologiques ou comportementales de la personne concernée.

Ainsi, à chaque demande d'autorisation unique visant à mettre en place un dispositif biométrique dans leur entreprise, les dirigeants doivent se conformer à certaines exigences :
• justifier de la nécessité et de la pertinence d'avoir recours à un dispositif biométrique. Le recours à ce dernier ne doit pas avoir pour effet de se substituer à des dispositifs non biométriques ;
privilégier les dispositifs biométriques qui garantissent aux personnes concernées la maîtrise de leur gabarit ;
justifier et garantir la protection et la conservation des gabarits en base ;
• prendre toute mesure permettant de limiter les risques d'atteinte à la vie privée.
Si vous avez mis en place un dispositif biométrique sous couvert de l'ancien cadre légal, vous devez vérifier s'il répond à ces nouvelles exigences :
si c'est le cas : un engagement de conformité à l'une de ces nouvelles autorisations peut être réalisé ;
si ce n'est pas le cas : vous avez 2 ans pour vous mettre en conformité.

2ans pour être en conformité
Si vous ne vous êtes pas mis en conformité d'ici la fin de ce délai, sachez néanmoins que la Cnil pourra à tout moment contrôler que le dispositif de biométrie mis en place dans votre entreprise répond aux obligations imposées par les nouvelles autorisations uniques.

Références :
(1) Article 25 de la Loi n°78-17 du 6 janvier 1978 modifiée, modifié par la Loi n°2016-1321 du 7 octobre 2016 pour une République numérique
(2) Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (Texte présentant de l'intérêt pour l'EEE)
(3) Délibération n°2016-186 du 30 juin 2016 portant autorisation unique de mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail et garantissant la maîtrise par la personne concernée sur son gabarit biométrique (AU-052)
(4) Délibération n°2016-187 du 30 juin 2016 portant autorisation unique de mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail, reposant sur une conservation des gabarits en base par le responsable du traitement (AU-053)…[Article source et complet]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l'article mis en page : Contrôles biométriques en entreprise : vos obligations changent !

Comment pirater des codes PIN

en sniffant le WiFi des smartphones ?

Comment pirater des codes PIN en sniffant le WiFi des smartphones ?

Des chercheurs peuvent récupérer des données sensibles en se basant sur les perturbations du signal WiFi lors des frappes sur l'écran.

Quand un utilisateur déplace ses doigts sur l'écran tactile de son téléphone, il perturbe le signal WiFi émis par son terminal. Ces interruptions peuvent être interceptées par un pirate, analysées et en appliquant de la rétro-ingénierie deviner quelle sont les frappes saisies sur le téléphone ou dans les champs de saisie de mot de passe.
Ce type d'attaque est nommé WindTalker (messager du vent), par des chercheurs chinois et elle n'est possible que si le pirate contrôle le point d'accès WiFi (un hotspot par exemple dans un rayon de 1,5 mètre) afin de collecter les perturbations du signal WiFi. Un contrôle impératif pour analyser le trafic et savoir quand l'utilisateur accède à des pages nécessitant une authentification.

Le CSI en ligne de mire

Si l'attaque semble issue du domaine de la science-fiction, cette menace se sert du CSI (Channel State Information), un composant du protocole WiFi chargé de fournir les informations générales sur l'état du signal WiFi. Quand l'utilisateur tape du texte sur l'écran, sa main modifie les propriétés de CSI du signal WiFi sortant et la modification peut être captée par un point d'accès malveillant.
Dans une démonstration exposée lors de la ACM Conference on Computer and Communications Security à Vienne, les chercheurs ont montré qu'en réalisant une analyse et un traitement basique du signal, un pirate peut avoir accès aux signaux CSI perturbés et deviner avec une précision moyenne de 68,3% les caractères qu'un utilisateur a tapé. La précision de WindTalker est différente selon les modèles de smartphones et elle peut être améliorée avec le niveau de données collectées…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : WindTalker : pirater des codes PIN en sniffant le WiFi des smartphones

---

Un système de chauffage d’immeubles victime d’attaque informatique

Un système de chauffage d’immeubles victime d’attaque informatique

---

Les systèmes de chauffage de deux immeubles ont été paralysés par une attaque par déni de service.
Avec des températures tournant autour de 0 degré Celsius au mois de novembre, les problèmes de chauffage sont loin d'être anecdotiques pour les habitants de la ville de Lappeenranta, dans l'est de la Finlande. Au début de novembre, certains d'entre eux ont été confrontés à une coupure de chauffage un peu particulière. Deux immeubles ont en effet vu le système de contrôle de leur chauffage paralysé par une attaque informatique, ce qui les a privés de chauffage et d'eau chaude.
Selon l'Agence de régulation des communications finlandaise (Ficora), citée par la radio-télévision publique Yleisradio Oy mardi 8 novembre, il s'agirait d'une attaque par déni de service (DDOS), qui consiste à surcharger un serveur de requêtes afin de le saturer. Néamoins, l'agence précise que ces systèmes de chauffage *« n'étaient pas la cible de cette attaque, ils ont été compromis dans une cyberattaque visant des entités européennes »*, a déclaré son responsable cybersécurité, Jarkko Saarimäki. *« Cette attaque a été réalisée de façon à faire passer son trafic à travers différents systèmes vulnérables »*, parmi lesquels ces systèmes de chauffage, explique-t-il, évoquant l'acte d'un *« groupe criminel »*…[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l'article mis en page : Une attaque informatique prive de chauffage des immeubles finlandais

---

Disney va lancer des spectacles de drones dans ses parcs d'attractions

Disney va lancer des spectacles de drones dans ses parcs d'attractions

Après deux ans d’attente, la compagnie de divertissement a reçu l’autorisation d’utiliser des drones dans ses parcs d’attractions pour enrichir ses shows nocturnes.…[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** en Cybercriminalité et est régulièrement invité à des **tables rondes en France et à l’étranger** pour sensibiliser les décideurs et les utilisateurs aux **Dangers liés à la Cybercriminalité (Arnaques, Piratages…) pour mieux s’en protéger** (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.

Réagissez à cet article

Internet : il n’y a plus d’adresses IPv4 disponibles

Internet : il n'y a plus d'adresses IPv4 disponibles

Cette fois, on touche le fond. Pas seulement à cause du résultat de l'élection du 45e président des Etats-Unis mais parce qu'il n'y a plus une seule adresse IPv4 disponible. C'est l'IAB (Internet Architecture Board) qui le dit.…[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** en Cybercriminalité et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **Dangers liés à la Cybercriminalité (Arnaques, Piratages…) pour mieux s'en protéger** (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.

Réagissez à cet article

L’industrie de l’IoT fait route vers un standard commun

Serions-nous à l’aube de l’initiative qui va standardiser l’industrie de l’Internet des objets (IoT) ? L’Industrial Internet Consortium (IIC), une organisation mondiale qui se donne pour mission de favoriser la croissance de l’Internet des objets industriels, et l’IoT Acceleration…[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** en Cybercriminalité et est régulièrement invité à des **tables rondes en France et à l’étranger** pour sensibiliser les décideurs et les utilisateurs aux **Dangers liés à la Cybercriminalité (Arnaques, Piratages…) pour mieux s’en protéger** (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.

Réagissez à cet article

Denis JACOPINI intervient au Conseil de l’Europe lors de la conférence Octopus 2016

	Denis JACOPINI intervient au Conseil de l’Europe lors de la conférence Octopus 2016

A l'occasion de sa conférence annuelle consacrée à la lutte de la Cybercriminalité à travers le monde du 16 au 18 Novembre prochain au Conseil de l'Europe, Denis JACOPINI intervient au Workshop n°7

Au programme :

• La Convention de Budapest: 15e anniversaire
• Criminalité et compétence dans le cyberespace : la voie à suivre
Ateliers
• Coopération entre les fournisseurs de service et les services répressifs en matière de cybercriminalité et de preuve électronique
• L'accès de la justice pénale aux preuves dans le Cloud: les résultats du groupe sur les preuves dans le Cloud (Cloud Evidence Group)
• Renforcement des capacités en cybercriminalité: les enseignements tirés
• L'état de la législation en matière de cybercriminalité en Afrique, en Asie/Pacifique et en Amérique latine/aux Caraïbes
• Le terrorisme et les technologies de l'information : la perspective de la justice pénale
• Coopération internationale: amélioration du rôle des points de contact 24/7
• A la recherche des synergies: politiques et initiatives en cybercriminalité des organisations internationales et du secteur privé

Participation

La conférence sera l'occasion, pour les experts en cybercriminalité des secteurs public et privé ainsi que les organisations internationales et non gouvernementales du monde entier, d'échanger.

La conférence Octopus fait partie du projet **Cybercrime@Octopus** financé par les contributions volontaires de l'Estonie, du Japon, de Monaco, de la Roumanie, du Royaume-Uni, des Etats-Unis d'Amérique et de Microsoft ainsi que du budget du Conseil de l'Europe.
Agenda Octopus 2016

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l'article mis en page : Octopus 2016