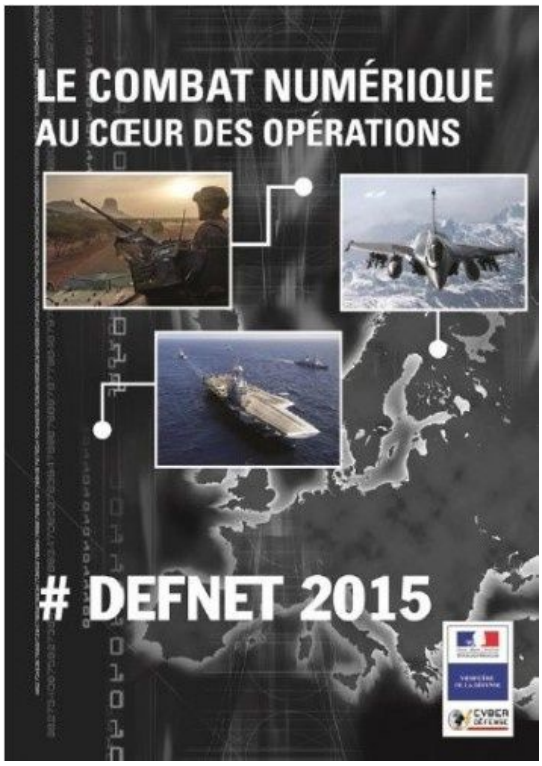
Deux bâtiments de notre marine nationale victime d’une cyberattaque sans précédent | Le Net Expert Informatique



Deux bâtiments de notre marine nationale victime d’une cyberattaque sans précédent

Vengeance de Vladimir Poutine ? Malveillance d'un hacker jihadiste ? On ne sait pas… Toujours est-il que deux bâtiments de notre marine nationale, le « Mistral » et son jumeau le «Tonnerre », actuellement en opérations en Méditerranée, viennent de faire de l'objet de cyberattaques simultanées. Leurs ordinateurs de bord ont été infectés par un virus informatique, générant un dysfonctionnement du SCADA, le système de contrôle automatisé qui permet gérer les principales fonctions de ces bateaux de guerre, à commencer par leurs radars et leurs systèmes d'armes. Un groupe d'intervention rapide composé de six membres de nos forces spéciales de cyberdéfense est en cours de déploiement sur les deux navires afin de résoudre la crise au plus vite.

Jusqu'au 27 mars, ce second exercice interarmées doit valider les choix de la chaîne de cyber-défense des armées françaises. Les administrations et opérateurs vitaux sont également concernés.

La cyberdéfense monte en puissance au sein des armées françaises avec la tenue jusqu'au 27 mars de DEFNET 2015, le second exercice interarmées grandeur nature consacré à ce thème.
« Il s'agit d'entraîner l'ensemble de la chaîne de cyber-défense » explique Le lieutenant-colonel Stéphane Dossé, le directeur de l'exercice, qui précise : « Il ne faut pas voir la cyber-défense comme un grand show hollywoodien. C'est un travail opérationnel du quotidien où il faut maintenir et renforcer une ligne de défense, comme dans l'armée de terre ».
Dans la forme, on risque donc d'être bien loin de la vidéo promotionnelle publiée par le Ministère de la Défense en février dernier sur la cyber-guerre : pas de terroristes encagoulés tapis dans l'ombre, pas de missiles expédiés en salve depuis un bâtiment de marine, pas de sergent chef Néo pour prendre à bras le corps la Matrice.
'La cyberdéfense : le combat numérique au coeur des opérations ', vidéo promotionnelle publiée en février 2015 par le Ministère de la Défense.

Un premier exercice avait eu lieu en octobre dernier, avec « un thème simple, sur un seul lieu ». DEFNET 2015 s'articule lui sur une dimension multi-sites. Sept sites militaires sont concernés, ainsi que deux bâtiments de la Marine nationale.
Le scenario de DEFNET 2015 simule, dans un contexte international fictif, des menaces et des attaques cyber multiples contre plusieurs sites sur des thèmes très différents, mentionne le communiqué de presse du Ministère de la Défense. Il associe les spécialistes de cyberdéfense des unités interarmées et des trois armées.
SI militaire, opérateurs vitaux et administrations
Le Ministère de la défense définit la cyberdéfence comme « l'ensemble des actions défensives et offensives conduites dans le cyberespace pour garantir le bon fonctionnement du ministère de la Défense et l'efficacité de l'action des forces armées en préparation ou dans la planification et la conduite des opérations ».
Mais dans le cadre de cet exercice, le périmètre de protection couvre en plus des systèmes d'information militaires, les opérateurs d'importance vitale et les administrations, raison pour laquelle l'Anssi est associée au projet.
A noter que cet exercice est l'occasion de tester le nouveau modèle de réserve cyber. Il s'agit d'accueillir des équipes de volontaires sur des sites militaires, simulant des sites d'intervention. Des équipes d'expérimentation sont constituées d'un réserviste des armées, d'un ou deux enseignants et de 10 à 12 étudiants en informatique et télécommunication d'un niveau bac+ à bac+5 (CentraleSupélec, Telecom Paris Tech ou encore l'Epita sont partenaires).
Elles devront effectuer un travail d'éradication de code malveillant et de réinstallation de système. L'exercice rassemble en tout un effectif de 580 personnes.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source :
http://www.zdnet.fr/actualites/defnet-2015-un-exercice-de-cyberdefense-multi-sites-est-en-cours-39816640.htm
Par Guillaume Serries

Projet de loi relatif au renseignement | Le Net Expert Informatique

Projet de loi relatif au renseignement

Le Conseil d'État a été saisi le 20 février 2015 et le 5 mars 2015 du projet de loi relatif au renseignement.

Ce projet de loi définit la **mission des services spécialisés de renseignement** et les **conditions dans lesquelles ces services peuvent être autorisés, pour le recueil de renseignements** relatifs à des intérêts publics limitativement énumérés, à recourir à des techniques portant sur l'accès administratif aux données de connexion, les interceptions de sécurité, la localisation, la sonorisation de certains lieux et véhicules, la captation d'images et de données informatiques, enfin à des mesures de surveillance internationale.
Il instaure pour l'ensemble de ces techniques, à l'exception des mesures de surveillance internationale, un régime d'autorisation préalable du Premier ministre après avis et sous le contrôle d'une autorité administrative indépendante dénommée « Commission nationale de contrôle des techniques de renseignement », qui pourra recevoir des réclamations de toute personne y ayant un intérêt direct et personnel. Il fixe les durées de conservation des données collectées.
Il prévoit un régime spécifique d'autorisation et de contrôle pour les mesures de surveillance et de contrôle des transmissions émises ou reçues à l'étranger.
Il institue un recours juridictionnel devant le Conseil d'État ouvert à toute personne y ayant un intérêt direct et personnel, ainsi qu'à la Commission nationale de contrôle des techniques de renseignement, tout en prévoyant des règles procédurales dérogatoires destinées à préserver le secret de la défense nationale.
Le Conseil d'État a veillé à ce que soient conciliées les nécessités propres aux objectifs poursuivis, notamment celui de la protection de la sécurité nationale, et le respect de la vie privée protégé par l'article 2 de la Déclaration des droits de l'homme et du citoyen et l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales. Il s'est attaché à préciser et renforcer les garanties nécessaires à la mise en œuvre des techniques de renseignement, tenant en particulier à l'existence, d'une part, d'un contrôle administratif s'exerçant au moment de l'autorisation et en cours d'exécution, d'autre part, s'agissant d'une procédure administrative spéciale, d'un contrôle juridictionnel approfondi du Conseil d'État statuant au contentieux.

Lire la suite….

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.legifrance.gouv.fr/Droit-francais/Les-avis-du-Conseil-d-Etat-rendus-sur-les-projets-de-loi/Projet-de-loi-relatif-au-renseignement-PRMX1504410L-19-03-2015

Apologie du terrorisme : un premier site bloqué en France | Le Net Expert Informatique

Crédit capture d'écran ministère de l'Intérieur

Apologie du terrorisme : un premier site bloqué en France

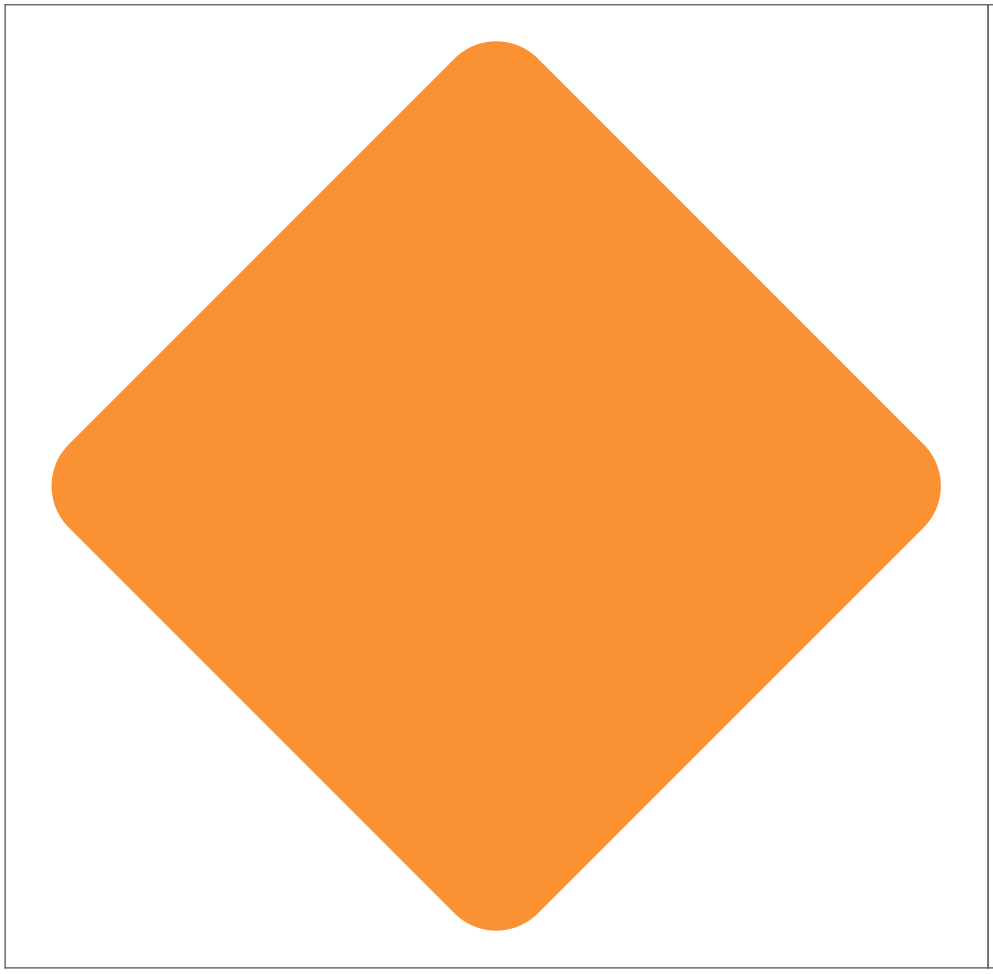
En audition au Sénat, l'Office central de lutte contre la cybercriminalité avait affirmé qu'une cinquantaine de sites internet pourraient être concernés par ces mesures de blocage.

Le blocage du site www.islamic-news.info a été demandé par l'Office central de lutte contre la cybercriminalité.
Pour la première fois en France, un site internet a été bloqué administrativement pour apologie du terrorisme, a révélé le site spécialisé Next INpact. Consécutivement à l'adoption au mois de décembre de la loi de « lutte contre le terrorisme », le site www.islamic-news.info n'est plus accessible depuis le lundi 16 mars.
Sa page d'accueille redirige les internautes vers le site su ministère de l'intérieur et affiche le message suivant : « Vous avez été redirigé vers ce site officiel car votre ordinateur allait se connecter à une page dont le contenu provoque à des actes de terrorisme [sic] ou fait publiquement l'apologie d'actes de terrorisme ».
Un décret de la loi de « lutte contre le terrorisme » permet à l'Office central de lutte contre la cybercriminalité (OCLCTIC) d'exiger aux fournisseurs d'accès à internet le blocage sous 24 heures des sites désignés comme faisant « l'apologie du terrorisme ». Et ce sans consultation d'un juge.
En audition au Sénat, l'Office central de lutte contre la cybercriminalité avait affirmé qu'une cinquantaine de sites internet jihadistes pourraient être concernés par ces mesures de blocage.
D'après David Thomson, le journaliste de RFI qui a découvert ce blocage, le site » islamic-news.info » est « un site pro-jihad assez peu influent ». Celui-ci se définit comme « un site d'information musulman qui se concentre en particulier sur les territoires dits islamiques » et dit vouloir « fournir une information détaillée de l'actualité du monde musulman ainsi que des explications d'ordre politique et historique ».
Les auteurs du site précisent : « Ce site d'information n'est en aucun cas partisan d'un quelconque groupe, organisation ou mouvement politique, religieux, civil ou armé. Ceci étant, nous considérons qu'il est de notre droit de dénoncer la manipulation, même lorsqu'elle concerne des organisations classées comme 'terroristes' à l'image d'Al-Qaïda, de l'Etat islamique ou des Frères musulmans. Le fait de réfuter des affirmations s'attaquant à ces organisations ne peut en aucune manière signifier une adhésion de notre part à celles-ci ni même faire la promotion de leurs idées et actes. »

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.atlantico.fr/pepites/apologie-terrorisme-premier-site-bloque-en-france-2042029.html

La sécurité selon Yahoo : chiffrement et mot de passe jetable | Le Net Expert Informatique



La sécurité selon Yahoo : chiffrement et mot de passe jetable

Yahoo a soumis sur GitHub le code d'un plugin permettant de chiffrer de bout-en-bout les courriels envoyés depuis son service de messagerie. La firme veut aussi faire disparaître le mot de passe et implémente un système OTP, un mot de passe à usage unique.

Depuis les révélations autour d'Edward Snowden concernant l'espionnage américain, la sécurité et la confidentialité des communications préoccupent nettement plus les fournisseurs de services en ligne, dont Yahoo et Google.
La firme de Marissa Mayer a ainsi notamment choisi d'adopter le chiffrement des échanges. Et dans ce cadre, Yahoo travaille à une solution de chiffrement de bout-en-bout de la messagerie par l'intermédiaire d'un plugin.

Stamos répond à la NSA avec un plugin
Afin de s'assurer de la robustesse de cette technologie, le directeur de la sécurité de Yahoo, Alex Stamos, fait appel à l'expertise de la communauté. Le code du plugin a été publié sur GitHub et disponible pour être audité et les vulnérabilités identifiées.
Yahoo a collaboré avec Google pour que leurs systèmes de messagerie soient compatibles avec le plugin de chiffrement, qui devrait être finalisé d'ici la fin de l'année et est basé sur le standard OpenPGP.
A noter que Yahoo, comme d'autres services Web, planche également sur la sécurisation de la phase d'authentification. Comment ? En proposant des méthodes alternatives au mot de passe classique, dont la vulnérabilité est établie.
Ainsi, Yahoo a implémenté un système OTP ou One Time Password. Après avoir activé la fonction et communiqué un numéro de téléphone mobile Yahoo, l'utilisateur n'a plus à mémoriser son mot de passe habituel.
Lors de la connexion, l'internaute n'a qu'à cliquer sur le bouton déclenchant l'envoi du mot de passe. Celui-ci parvient sous la forme d'un SMS comportant un code de 4 caractères. Il ne reste plus qu'à le saisir pour se connecter.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source :
http://www.zdnet.fr/actualites/la-securite-selon-yahoo-chiffrement-et-mot-de-passe-jetable-39816374.htm

---

Skype sur écoute : un

amendement de la loi Macron relance le débat | Le Net Expert Informatique

	Skype sur écoute : un amendement de la loi Macron relance le débat

Le débat sur la qualification de Skype et de certains autres services de VoIP en tant qu'opérateurs de téléphonie devrait repartir. Un amendement contenu dans la loi Macron souhaiterait que ce type d'outil dispose des mêmes obligations que les opérateurs classiques.

Un amendement contenu dans le projet de loi Macron pourrait bien relancer le débat autour de la classification de Skype en tant qu'opérateur de téléphonie. Il ne s'agit pas ici d'un simple conflit pour tenter de mettre le service de VoIP dans une case, mais d'obliger le logiciel, propriété de Microsoft, à respecter certaines obligations qui découlent de ce statut.
Parmi ces obligations figurent par exemple le fait de devoir **autoriser les appels d'urgence**, de **financer le service universel** ou encore de **permettre les écoutes téléphoniques**. Dans ce dernier cas, cela supposerait que les services de renseignement français pourraient accéder au logiciel dans le cadre d'enquêtes.
Selon Les Echos, un amendement parlementaire, soutenu par le gouvernement et d'ores et déjà adopté le 7 février à l'Assemblée nationale, confère le droit à l'Arcep de déclarer un tel programme comme un opérateur de télécommunications. Le texte n'est pas encore définitivement adopté puisqu'il doit d'abord être voté par le Sénat.
Si le Parlement vote en sa faveur, l'Arcep pourrait à terme obliger certains programmes de VoIP à respecter leurs obligations sans que le régulateur ne soit obligé de les attaquer en justice au préalable.

Le sujet traîne depuis 2007
Si l'amendement semble récent, le sujet traîne auprès des autorités concernées depuis quelques années. Depuis 2007, l'Arcep souhaite en effet que Skype soit déclaré en tant qu'opérateur de téléphonie en France. Pour l'autorité, le fait que la plateforme propose d'appeler des numéros de téléphonie, fixes ou mobiles via un ordinateur ou un smartphone est une condition permettant de la faire entrer dans cette catégorie.
Une enquête préliminaire aurait même été diligentée sur la question, les investigations étant a priori dirigées par la brigade de répression de la délinquance aux personnes. L'enjeu était alors identique à savoir l'obligation de se plier à des impératifs comme le fait d'autoriser les appels d'urgence, financer le service universel ou encore permettre les écoutes téléphoniques.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source :
http://pro.clubic.com/legislation-loi-internet/actualite-758733-skype-macron-ecoute.html

Comment se passe un contrôle de la CNIL et comment s’y préparer ?

17

Aucun organisme public ou privé n'est à l'abri d'un contrôle de la CNIL. Il est donc important de se tenir prêt. Pour ce faire, la préparation et la sensibilisation des différents acteurs sont essentielles. Le CIL a bien évidemment une place prépondérante dans ce processus, que ce soit en amont, pendant ou après. Thierry Ramard, Président d'Ageris Group, rappelle les bonnes pratiques pour se mettre en conformité avec la législation et se préparer au mieux à un éventuel contrôle, à l'occasion de 9ème Université des CIL de l'AFCDP.

Les missions de contrôle de la CNIL s'inscrivent dans le cadre d'un programme annuel adopté en séance plénière. Ce programme est élaboré en fonction des thèmes d'actualité et des grandes problématiques dont la CNIL est saisie. Cela représente près de 2/3 des contrôles. Ceux-ci peuvent également être décidés en réponse à des besoins ponctuels, dans le cadre de l'instruction de plaintes, ou de demandes de conseil (environ 1/3 des contrôles).

Selon le rapport d'activité 2013 de la CNIL :
Elle a reçu 5 638 plaintes au cours de l'année 2013 : dans 99% des cas, l'intervention de la CNIL s'est traduite par une suite favorable pour le demandeur ;
414 contrôles ont été réalisés, dont 33% étaient issus de plaintes. 280 contrôles ont concerné des traitements relevant directement de la Loi Informatique et Libertés, et 134 des dispositifs de vidéoprotection/vidéosurveillance. La majorité des contrôles ont été effectués dans le domaine du commerce (117), de la santé et du social (73). 89% des organismes contrôlés se sont mis en conformité après échanges de courriers ;
57 mises en demeure ont été adoptées : 88% d'entre elles font suite à un contrôle, 12% sont directement issues de plaintes sans contrôle sur place. 86% de ces organismes mis en demeure en 2013 se sont mis en conformité ;
14 dossiers ont fait l'objet d'une procédure de sanction.

Contrôle de la CNIL : avant, pendant, après

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.globalsecuritymag.fr/AFCDP-Comment-se-preparer-a-un,20150130,50435.html

Colloque « Innovation et cybercriminalité : l'Europe face aux défis de la transformation numérique » | Le Net Expert Informatique

Colloque à Montpellier « Innovation et cybercriminalité : l'Europe face aux défis de la transformation numérique »

Programme du Mercredi 8 avril 2015

13:30-14h Accueil des participants

14h:00 Ouverture du colloque :
Philippe Augé, Président de l'Université de Montpellier
Marie-Elisabeth André, Doyen de la Faculté de Droit et Science politique de Montpellier
Adel Jomni, Enseignant-chercheur, Université de Montpellier
Michal Choras, Représentant du projet européen CAMINO
Akhgar Babak, Représentant du projet européen COURAGE

14h30 Session 1: Innovations numériques, Cybercriminalité et Cyber-terrorisme : Enjeux et défis : quelles stratégies ? :
Lord Carlile of Berriew, Membre du Parlement du Royaume-Uni,
Général Marc Watin-Augouard, Directeur du centre de recherche de l'Ecole des Officiers de la Gendarmerie Nationale (EOGN)
Andy Archibald, Directeur adjoint de l'unité nationale cybercriminalité de l'Agence Nationale de la Criminalité du Royaume-Uni
Marco Lozano, Représentant INCIBE (Instituto Nacional de Ciberseguridad de España)

16h:00 Pause

16h:15 Session 2: Les menaces cybernétiques : Analyse des risques et des stratégies? :
Président de session : Cormac Callanan, Expert auprès du Conseil de l'Europe, CEO, Aconite, Irlande
– Etat des lieux des cyber menaces – Jean-Dominique Nollet, Directeur de l'unité d'investigation et recherche (European Cybercrime Centre (EC3-Europol)
– L'investigation et la coopération entre les organisations internationales (Interpol, Europol,..) – Valérie Maldonado, Directrice de l'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC)
– Analyse des réseaux sociaux et sécurité nationale – Thomas Delavallade, THALES
– Comment améliorer la résilience face à la cybercriminalité et au cyber-terrorisme (Projet Européen CAMINO – FP7) – Michal Choras,Professeur, Coordinator du projet FP7-CAMINO, ITTI, Pologne

---

Programme du Jeudi 9 avril 2015

9h:00 Session 3: Enjeux et risques liés au développement des monnaies virtuelles
Président de session : Daniel Guinier, Expert en cybercriminalité, Cour Pénale Internationale de La Haye
– Flux illicites et monnaies virtuelles – Myriam Quéméner, Magistrate, Cour d'appel de Versailles
– Monnaie virtuelle et crypto monnaie : quels enjeux et réponses réglementaires? Quelles préconisations pour les utilisateurs et les entreprises? – Cathie-Rosalie Joly, Avocate
– Paiements 2.0: nouveaux défis de sécurité et rôle de l'Autorité Bancaire Européenne – Geoffroy Goffinet, European Banking Authority (EBA)- Bruxelles

---

10h:15 Pause

10h:30 Session 4: Big data, Internet des objets, Cybersécurité et protection de la vie privée
Président de session : Christian Aghroum, Membre CDSE, Expert en Cybersécurité
– Big Data et sécurité : le pouvoir de l'anticipation au service de la cybersécurité – Adel Jomni, Enseignant-chercheur, Université de Montpellier
– Le droit est-il un frein pour le développement du Big Data ? – Francesca Bosco, Chef de projet UNICRI (United Nations Interregional Crime and Justice Research Institute); Giuseppe Vaciago, Cybercrime Institute, Germany
– Objets connectés et santé : l'innovation au service ou au détriment du citoyen? – Corinne Thierache, Avocate
– Le Big Data : un déclencheur de changement des règles juridiques – Fraser Sampson, Responsable de l'office des crimes – West Yorkshire Police

---

13h:00 Pause déjeuner

14h:00 Session 5: Projets européens, coopération internationale, recherche et formation dans le domaine de la lutte contre la Cybercriminalité et le Cyberterrorisme
Président de session : – Nigel Jones,Directeur du Centre for Cybercrime Forensics, Université de Canterbury
– Défis majeurs de la recherche dans le domaine de la cybercriminalité et le cyber terrorisme – Akhgar Babak, Projet Européen COURAGE
– Nouvelles approches de la protection des données et Cryptographie -Projet ENISA (European Union Agency for Network and Information Security) – María Pilar Torres Bruna,Responsable Cybersécurité chez Everis, Espagne
– Nouvelles méthodes d'investigation et de formation forensique dans un environnement virtuel (cloud) (projet D-FET) – Adrian Smalesn Researcher, Université Napier d'Edimbourg
– La coopération internationale pour renforcer les capacités de protection des infrastructures d'information critiques 2015-2020 (CIIP) – Jean-Christophe Letoquin, Expert auprès du Conseil de l'Europe, Président de SOCOGI
– Coopération internationale en matière de formation cyber (enjeux et rôles des partenaires) ? – Yves Vandermeer, Federal Computer Crime Unit, Belgique E.C.T.E.G Chair (Europol)

16h:00 Fin du colloque

Emportez le programme avec vous ! Téléchargez le PDF

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.
Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

La justice néerlandaise annule une loi sur les données personnelles | Le Net Expert Informatique

La justice néerlandaise annule une loi sur les données personnelles

La justice néerlandaise a annulé mercredi une loi exigeant le stockage de données personnelles, assurant que bien qu'utile à la lutte contre le crime, le texte violait la vie privée des utilisateurs des réseaux téléphoniques et d'internet.

« Les juges ont estimé que le stockage de données était nécessaire et efficace pour combattre le crime, mais la législation néerlandaise est contraire aux droits des personnes à une vie privée et à la protection de leurs données personnelles », a indiqué le tribunal de La Haye dans un communiqué.
« La loi est donc contraire à la Charte des droits fondamentaux de l'Union européenne », a ajouté le tribunal.
Sept organisations, dont l'organisation de défense de la vie privée Privacy First et l'Association néerlandaise des Journalistes, avaient entamé une action contre l?État le mois dernier.
Cette décision des juges intervient environ un an après une décision de la justice européenne, qui avait imposé en avril 2014 une révision de la législation sur la conservation des données personnelles, la jugeant « disproportionnée » malgré son utilité dans la lutte contre le terrorisme.
La directive en question datait de 2006 et exigeait des opérateurs de télécoms et des fournisseurs d'accès internet de stocker les données des communications téléphoniques ou de courriels pendant six mois à deux ans.
Étaient donc conservées les métadonnées desdites communications, comme l'heure, la date, la durée et la destination, mais pas leur teneur.
Ces données pouvaient ensuite être consultées par les services de renseignement ou la police.
« Les droits à une vie privée des citoyens néerlandais ont été violés en masse par cette surveillance », a affirmé Vincent Boehre, le directeur des opérations de Privacy First, cité dans un communiqué publié sur le site internet de l'organisation.
Privacy First « lutte pour une société dans laquelle des civils innocents ne doivent pas se sentir comme s'ils étaient constamment surveillés », a-t-il ajouté, soulignant que ce jugement est « une étape importante dans cette direction ».

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.leparisien.fr/high-tech/la-justice-neerlandaise-annule-une-loi-sur-les-donnees-personnelles-11-03-2015-4595081.php

---

Accord pour faciliter les plaintes transfrontalières | Le Net Expert Informatique

Accord pour faciliter les plaintes transfrontalières

Les Etats membres de l'Union européenne se sont accordés ce vendredi à Bruxelles sur le principe de permettre aux entreprises et aux citoyens le dépôt, au sein de leur Etat national, d'une plainte en matière de protection de la vie privée contre une entreprise du web établie dans un autre Etat.

Ce guichet unique («one-stop-shop») serait compétent pour veiller à l'application des règles pour les transferts transfrontaliers de données personnelles collectées dans plusieurs pays de l'UE par des entrepri1ses ou des plate-formes internet comme Amazon, Google, Facebook.
Les plaignants auront la possibilité de saisir leurs autorités nationales, comme la Commission de la protection de la vie privée en Belgique, en cas de litige.
Le but est d'obtenir une procédure plus rapide, des coûts et une charge administrative moindres ainsi qu'une sécurité juridique accrue.
Le secrétaire d'Etat belge en charge de la protection de la vie privée, Bart Tommelein, ne voit que des avantages au principe du guichet unique, mais reconnaît sa complexité. «Nous devrons activer ce système avant de voir par la suite comment l'améliorer et le simplifier», a-t-il commenté.
Un accord global sur la législation sur la protection des données personnelles est toutefois encore loin d'être définitif.
Les ministres européens de la Justice ont donc décidé de se réunir en «conclave» le 15 juin à Luxembourg afin de conclure un accord.
Les discussions sont engagées depuis février 2012, mais elles ont longtemps piétiné. Onze chapitres sont ouverts, et six ont fait l'objet d'un accord de principe, dont celui portant sur la création d'un «guichet unique».
Sur les cinq restant en discussion, on relève celui concernant les droits des personnes, avec le droit d'accès aux données collectées, le droit de les faire rectifier et le droit à l'oubli avec la possibilité «de faire effacer les informations mises en ligne avec insouciance par les mineurs».

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lavenir.net/cnt/dmf20150313_00616117

Interpellation d’un pilote de drone à Paris | Le Net Expert Informatique

Interpellation d’un pilote de drone à Paris

Un homme a été interpellé et placé en garde à vue pour avoir piloté samedi un drone au-dessus de Paris, où les mystérieux vols de drones se multiplient malgré l’interdiction de survol de la capitale, a-t-on appris de source policière.

Le pilote présumé, un des responsables de la Commission nationale de l’informatique et des libertés (CNIL), chargé des technologies et de l’innovation, a été interpellé à la suite d’un signalement d’un particulier, a-t-on précisé de source policière.
L’homme était « en possession d’un drone de 400 grammes à quatre hélices, équipé d’une caméra à l’avant », selon cette source.
Depuis le 5 octobre, au moins 60 survols de drones ont été constatés au-dessus de sites sensibles, comme des centrales nucléaires, ou de la ville de Paris, selon le ministre de l’Intérieur, Bernard Cazeneuve.
Particuliers souhaitant tester leur nouveau jouet, amateurs de photos s’amusant à narguer les autorités ou repérages à des fins criminelles: les motivations et le profil de ces pilotes demeurent inconnus.
Début mars, une dizaine de vols de drones au-dessus de Paris avaient mobilisé la police. Quatre journalistes allemands avaient alors été brièvement interpellés alors qu’ils étaient en possession d’un drone.
Le 25 février, trois journalistes de la chaîne qatarie Al-Jazeera avaient été placés en garde à vue après avoir fait voler un drone à Paris pour un reportage, lui-même consacré aux mystérieux survols nocturnes de la capitale ces dernières semaines.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lorientlejour.com/article/915809/un-homme-interpelle-apres-avoir-fait-voler-un-drone-a-paris.html