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

Un radar pour détecter les petits drones | Le Net Expert Informatique

Un radar pour détecter les petits drones

La détection de drones de moins d'un mètre d'envergure est un sérieux défi technologique. Tecknisolar, une société basée à Saint-Malo, a développé un radar portable et autonome, « parfaitement adapté à la surveillance des zones sensibles ».

Les récents survols de villes, de centrales nucléaires ou de terrains militaires comme l'Ile-Longue par des drones ont-ils dopé la vente de votre radar spécialisé dans la détection de petites cibles ?
Pascal Barguirdjian : Non, pas plus que cela. Les autorités militaires font la sourde oreille. Pourtant, notre radar fonctionne et a fait ses preuves auprès des gendarmes et douaniers d'Outremer (Cegom).

Quand l'avez-vous sorti et comment marche-t-il ?
Nous l'avons développé à la demande d'un général de gendarmerie alors patron du Cegom, en 2007. Nous avons livré quelques-uns de ces radars (100.000 euros pièce) capables de détecter des intrusions d'embarcations dans des zones maritimes sensibles. Ce système composé d'une antenne, d'un écran et de panneaux solaires pour une alimentation autonome est également adapté aux petits engins volants.

Quel est le rayon d'action de votre système ?
Il est capable de détecter des embarcations dans un rayon de 15 km comme des engins volants d'un peu plus d'un mètre d'envergure jusqu'à 2 km.

Et les plus petits, ceux que l'on soupçonne de survoler centrales nucléaires et zones militaires ?
Leur surface de réflexion est encore trop faible mais notre radar peut relever des échos dans un rayon de 500 m. Toute la difficulté réside dans la détection d'un engin de moins d'un mètre évoluant au ras du sol.

Les laboratoires militaires cherchent à détecter des engins de 50 cm d'envergure, qu'en pensez-vous ?
C'est très difficile, voire impossible.

Quelle est la parade après avoir détecté un drone ?
On peut le suivre à la trace ou notamment déterminer un cap de fuite pour tenter de le retrouver. Le plus efficace semble le brouillage de sa fréquence GPS pour le faire s'écraser au sol.

Quel est le risque d'un survol de drone de petite taille, à la charge utile forcément limitée ?
Ces drones peuvent être mis en oeuvre par des services secrets qui réalisent la collecte d'informations. L'acte terroriste avec une flotte de drones décollant sur une cible et transportant individuellement quelques centaines de grammes de puissant explosif est à craindre. La menace la plus sérieuse étant, selon moi, l'attaque bactériologique au-dessus d'une ville ou d'un stade de football plein à craquer.

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

Source : http://www.letelegramme.fr/economie/drones-un-radar-imagine-a-saint-malo-14-03-2015-10557015.php
www.tecknisolar.com

Piratage de ses comptes sociaux : prévenir, repérer et réagir ! | Le Net Expert Informatique

Piratage de ses comptes sociaux : prévenir, repérer et réagir !

Vos comptes sociaux abritent une somme considérable de données personnelles. Veillez à bien les sécuriser pour éviter les piratages d'individus malveillants.

I- Prévenir un piratage

Choisissez des mots de passe complexes, différents et non-signifiants !

Aucune personne ou ordinateur ne doit être en mesure de le deviner. La CNIL publie des conseils pour créer un mot de passe efficace, le retenir et le stocker dans une base.

Ne communiquez pas votre mot de passe

Il est vivement déconseillé de communiquer votre mot de passe à une tierce personne, de l'enregistrer dans un navigateur si vous n'avez pas défini de mot de passe maitre ou dans une application non sécurisée.

Activez un dispositif d'alerte en cas d'intrusion

La double authentification est une option activable sur la plupart des réseaux sociaux. Lorsque vous vous connectez depuis un poste informatique inconnu, le réseau social vous demandera de confirmer l'accès en entrant un code que vous aurez reçu par sms ou par mail. D'autres fonctions proposent simplement de vous alerter si une personne extérieure tente de se connecter à votre compte depuis un terminal inconnu (PC, smartphone, tablette, mac).

Déconnectez à distance les terminaux encore liés à votre compte

Là encore, cette option disponible sur la plupart des réseaux sociaux vous permet d'identifier l'ensemble des terminaux avec lesquels vous vous êtes connectés à votre compte. Lorsque cela est possible, il est conseillé de désactiver le lien avec les terminaux dont vous ne vous servez plus. Une connexion identifiée depuis un navigateur inconnu ou une ville inconnue pourra vous mettre la puce à l'oreille.

Désactivez les applications tierces connectées à votre compte

Il arrive que les applications tierces connectées à votre compte soient vulnérables à une attaque extérieure. Il est conseillé de désactiver les applications tierces dont vous avez autorisés l'accès par le passé et qui ne vous servent plus.

Réglez vos paramètres de confidentialité

En devinant votre nom, votre fonction, votre liste d'amis, une personne mal intentionnée pourrait facilement déduire des informations qui servent à réinitialiser votre compte ou simplement à usurper votre identité afin de changer votre mot de passe par exemple.

II- Repérer un piratage

• votre mot de passe est invalide
• des tweets/posts imprévus sont envoyés depuis votre compte
• des messages privés sont envoyés de façon non volontaires
• des comportements inhabituels ont lieu sur votre compte sans consentement (comme suivre, se désabonner, ou bloquer)
• une notification de la part du réseau social vous informe que « Vous avez récemment changé l'adresse email associée à votre compte.

III- Réagir en cas de piratage

1. Signalez le compte piraté auprès du réseau social
2. Demandez une réinitialisation de votre mot de passe.

Si un site/réseau social n'apporte pas de réponse satisfaisante, contactez la CNIL

3. Une fois votre compte sécurisé, n'oubliez pas de parcourir les rubriques « sécurité » proposées par ces réseaux sociaux

---

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

Source : http://www.cnil.fr/documentation/fiches-pratiques/fiche/article/piratage-de-ses-comptes-sociaux-prevenir-reperer-et-reagir/

Les 10 règles du pilote de drone amateur pour voler en toute légalité | Le Net Expert Informatique

Survoler un troupeau de vaches, c’est à la fois pas très sympa pour elles et interdit par la loi. Photo : Lima Pix/Flickr.com

Les 10 règles du pilote de drone amateur pour voler en toute légalité

Alors que les vols de drones se multiplient au-dessus de la capitale, voici quelques conseils pour rester dans la légalité et ne mettre personne en danger.
PNJ, fabricant de drones, a réalisé un « petit guide d'utilisation de drone pour pilote amateur ». Voici Les 10 règles de base à connaître avant d'utiliser un drone en toute sécurité… et légalité. Vous pouvez télécharger le guide gratuit dans son intégralité en cliquant ici (PDF) ou en vous rendant sur le site PNJ-cam.com.

► 1. Ne volez pas en zone urbaine
On ne le dira jamais assez : non, il n'est pas permis de faire voler son drone dans une agglomération. Que ce soit Paris, une autre grande ville de France ou un minuscule village. La loi stipule clairement cela dans l'arrêté du 11 avril 2012, article 2. Si vous avez un doute, vous pouvez consulter une carte IGN. Les endroits marqués en orange et jaune sont interdits. En ligne, vous pouvez consulter le site AIP Drones ou Mach 7 Drones. Des applications mobiles sont également disponibles.

► 2. Ne survolez jamais des personnes ou des animaux
C'est amusant de filmer ses amis en faisant voler un drone au-dessus de leurs têtes. Ou encore des vaches dans un champ. Sauf que c'est interdit. Oubliez donc cette idée d'immortaliser le prochain concert de Violetta en survolant le Stade de France, de filmer un match de foot en vue aérienne ou ce troupeau de mouettes sur une plage. La loi vous l'interdit.

► 3. Ne dépassez pas les 150 mètres d'altitude
Même si votre drone est suffisamment puissant pour aller au-delà, 150 mètres, c'est la limite autorisée pour votre appareil volant. Au-dessus, c'est le territoire des avions… et des appareils militaires. Donc si votre drone est équipé d'un système de limitation de hauteur de vol, pensez à le régler à 150 mètres (ou à fixer un plafond moindre) pour plus de sécurité.

► 4. Gardez votre drone à l'œil
Il faut toujours avoir une vue directe sur son appareil. Et l'arrêté du 11 avril interdit l'usage de jumelles pour ce faire. Il existe toutefois une exception : les vols en immersion. Nous en parlerons dans la règle 9.

► 5. Pas de vols depuis un véhicule en mouvement
Pendant un vol de drone, il est interdit de se trouver dans une voiture en mouvement, sur un bateau qui se déplace, un quad, une moto, etc. Et ce, même si vous ne conduisez pas le véhicule en question. La meilleure position pour piloter un drone ? Debout, sur un sol fixe et les yeux fixés sur l'appareil volant, en vue directe.

► 6. Respectez la vie privée des personnes environnantes
A priori en respectant la règle 1 (interdiction de voler en zone urbaine) et la règle 2 (ne pas survoler des personnes ou des animaux), cela ne devrait pas se produire. Cependant, il est toujours bon de rappeler l'article 226-1 du Code pénal : il est interdit de filmer ni diffuser des images de quelqu'un dans un endroit privé sans son accord. Et si jamais vous avez décidé de survoler une maison isolée en pleine pampa afin de voir de plus près à quoi ressemble ce mystérieux jardin entouré de hauts murs, oubliez aussi. Et puis, de toute façon, il y a Google Earth/Maps pour ça…

► 7. Ne faites pas un usage commercial des photos et vidéos
A moins d'avoir obtenu une autorisation spéciale pour un usage professionnel, la Direction générale de l'aviation civile (DGAC) interdit que les photos et vidéos filmées avec un drone soient utilisées dans un cadre commercial. En revanche, il est autorisé de les partager entre amis et de les mettre sur les réseaux sociaux à titre privé.

► 8. Restez dans les fréquences autorisées
Pour piloter un drone, des émissions radio sont nécessaires entre l'appareil volant et sa télécommande (votre smartphone, une manette, etc.). Les plages de fréquences et la puissance d'émission autorisées sont réglementées. Il faut utiliser la plage 2,4 GHz avec une puissance de 100 MW maxi ou la plage 5,8 GHz (avec des fréquences comprises entre 5 725 et 5 875 MHz) et une puissance maxi de 25 MW.

► 9. L'exception des vols en immersion
Les FPV (First Person View) sont des vols en immersion ou, au lieu de piloter le drone en vue directe, on utilise soit des lunettes ou un casque avec écran LCD. On peut aussi utiliser l'écran d'une tablette par exemple. On voit alors ce que « voit » le drone. Ces vols sont autorisés mais il faut néanmoins que la vue directe soit toujours possible. Il faut donc deux pilotes dans ce cas : une personne qui regarde dans l'écran LCD et une autre qui surveille visuellement le drone. Les deux doivent avoir une commande pour prendre la main sur l'appareil à tout moment. >> Voir une démonstration vidéo de FPV

► 10. Respectez les règles de l'insertion dans l'espace aérien
Restez à bonne distance des aéroports, aérodromes et des zones déclarées comme interdites par le gouvernement français. Là encore, si vous avez un doute, il faut consulter des cartes, en l'occurrence les cartes aéronautiques (cf. liens proposés en règle 1).

Et si je ne respecte pas une (ou plusieurs) de ces règles, je risque quoi ?
Si vous ne respectez pas les règles 1 à 9, cela relève de l'article L6232-4 du Code des transports. A savoir que vous encourez des peines maximales de 75 000 euros d'amende et un an de prison. En outre, le manquement de la règle 7 est sanctionné par 45 000 euros d'amende et un an de prison (article 226-1 du Code pénal. Vous ne respectez pas la règle 10 ? Le Code des postes et télécommunication électroniques prévoit dans l'article L39-1 des peines maximales de 30 000 euros d'amende et 6 mois de prison. Et toutes ces peines sont cumulables. Ça fait réfléchir, non ?

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

Source : http://www.metronews.fr/high-tech/les-10-regles-du-pilote-de-drone-amateur-pour-voler-en-toute-legalite/mocd!pR40pDYEwywIg/
Par Florence SANTROT

Toulouse attaqué par le virus «Rançongiciel» | Le Net Expert Informatique

Toulouse attaqué par le virus «Rançongiciel»

Ce mardi 10 mars, le système informatique de la ville de Toulouse a été attaqué par le virus «Rançongiciel», a confirmé hier une source municipale à La Dépêche du Midi3.

Vendredi 6 mars, les services informatiques municipaux avaient été mis en garde sur une éventuelle attaque par une autre collectivité de l'agglomération, qui avait elle-même été la cible de ce virus. «Rançongiciel» se propage par l'ouverture de pièces jointes dans les courriels, le téléchargement de fichiers infectés, la navigation sur internet. Il s'installe silencieusement dans l'ordinateur contaminé dont il crypte certains types de documents qui deviennent alors illisibles. Les pirates adressent alors un message dans lequel ils demandent une rançon en échange de la clé de déchiffrement des données. Généralement, cette clé n'est jamais fournie, même en cas de paiement.

Ce mardi 10 mars, un «Rançongiciel» a été détecté dans le système informatique de la ville de Toulouse qui avait été placé sous surveillance. Des mesures de précaution, comme l'interruption du travail en réseau, ont été prises immédiatement pour éviter sa propagation. De source interne, aucun fichier n'a été endommagé. Le réseau a été rétabli ce jeudi à 15 heures.

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…

Source : http://www.ladepeche.fr/article/2015/03/13/2065766-le-reseau-de-la-ville-attaque-par-le-virus-rancongiciel.html

---

L'externalisation, pourquoi et comment ? | Le Net Expert Informatique

L'externalisation, pourquoi et comment ?

L'externalisation (ou sous traitance) se développe de plus en plus en France, quels sont les avantages pour les professionnels du droit à avoir recours à ce type de service, et dans quelles conditions peut-elle être mise en place ?

L'externalisation c'est l'Action pour une entreprise de confier une partie de ses activités à des partenaires extérieurs.(Larousse). Aujourd'hui sous traiter se développe de plus en plus en France. Mais comment en tant que professionnel pouvez-vous inclure cette prestation extérieure dans la gestion quotidienne de votre activité ? Quelles taches peuvent être sous traitées ? Par qui ? Quid de la confidentialité des données transmises ? Quels sont les bénéfices et avantages ?

Des bénéfices et des avantages pour les professionnels
Le fait de confier des taches récurrentes et chronophages à une entreprise extérieure permet de réduire automatiquement vos frais de gestion, et vos charges liées au personnel. Des économies vous permettant une meilleure gestion de votre activité (réinvestissement, augmentation du budget communication ou publicitaire…).
De plus, comme un assistant, votre prestataire extérieur connait vos besoins et s'adapte. Il est possible de lui dicter vos conditions, et de travailler avec lui suivant votre fonctionnement.

Quelles taches peuvent être sous traitées ?
Autant de questions que les professionnels se posent avant de « sauter le pas ». Il existe des agences ou des cabinets spécialisés en expertise comptable, pour la gestion de la paie et des ressources humaines. Il est également possible d'externaliser une partie de son secrétariat, ou de sa permanence téléphonique.
Il suffit de déterminer au préalable un besoin : Aujourd'hui je ne peux plus répondre à mon standard téléphonique, ou je n'ai pas le temps de saisir mes courriers ou mes actes, j'aimerai trouver un expert comptable pour la gestion de ma comptabilité…

Comment inclure la prestation dans ma gestion quotidienne, et par qui sera t-elle réalisée ?
Votre prestataire est là pour vous aider à mettre en place la prestation et sa gestion au quotidien. Il est un professionnel qualifié et diplômé. N'hésitez pas à demander la qualification de la personne effectuant les tâches à l'entreprise. La prise en charge de la permanence téléphonique ou l'envoi par email d'un courrier à taper ou d'un fichier à retranscrire par email, autant de solutions qui peuvent être trouvées pour vous décharger de certaines taches.

Et la confidentalité des données ?
Votre prestataire, tenu au secret professionnel se doit de vous garantir la confidentialité des données en n'effectuant aucune sauvegarde de fichiers transmis. N'hésitez pas à faire ajouter cette mention lors du devis signé entre les deux parties.
L'externalisation ou sous traitance ne doit pas être vue comme une contrainte, mais plutôt comme une solution de « facilitateur » du quotidien. Elle peut être utilisée ponctuellement ou pour répondre à un besoin régulier. Un bon moyen de recentrer le travail de vous et/ou collaborateurs sur l'essentiel de leurs taches et missions quotidien et de se concentrer sur l'essentiel de l'activité.

ATTENTION :
Ce n'est pas parce que vous bénéficiez des services d'un prestataire que ceci vous exempt de déclaration à la CNIL des traitements de données à caractères personnel qui seront manipulées.
Comme tout professionnel de l'informatique et de l'Internet, il est de mon devoir de vous informer que vous devez mettre en conformité et déclarer à la CNIL tous vos traitement de données à caractère personnel (factures, contacts, emails…).
Vous trouverez plus d'information sur le site de la cnil (www.cnil.fr) ou, étant correspondant CNIL local, dans notre rubrique Protection des données personnelles.

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…

Source : http://www.village-justice.com/articles/externalisation-pourquoi-comment,19173.html
Par Mme Pollet, responsable de l'entreprise APSAEE, spécialisée dans la sous traitance du Secrétariat Juridique : Permanence téléphonique et Retranscription audio.

Alerte ! Des escrocs se font passer pour des techniciens en informatique | Le Net Expert Informatique

Alerte ! Des escrocs se font passer pour des techniciens en informatique

Mercredi, une habitante de Saint-Pal-de-Mons a subi une tentative d'escroquerie par des cybercriminels. Elle a reçu un appel téléphonique d'une personne parlant anglais se présentant comme employée d'une célèbre entreprise d'informatique. Selon les dires de son interlocuteur, son ordinateur serait infecté d'un virus. L'appel a été transmis à un second présumé technicien qui, toujours en anglais, a proposé à la San-palouse de prendre la main sur la machine.

La femme a alors eu la puce à l'oreille lorsqu'on a lui a demandé ses coordonnées bancaires. Elle a raccroché et s'est rendue dans une entreprise spécialisée. Des fichiers de son ordinateur ont été endommagés.
Elle a ensuité déposée plainte auprès des gendarmes de la communauté de brigades de Saint-Didier-en-Velay.
Selon nos informations, les premiers éléments tendraient vers une escroquerie depuis l'étranger, l'indicatif « 00221 » au moment de l'appel étant celui du Sénégal.

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…

Source : http://www.leprogres.fr/faits-divers/2015/03/13/cybercriminalite-ils-se-font-passer-pour-des-techniciens-en-informatique

---

Limelight lance un service de détection de limitation de l'impact des attaques DDoS – Global Security Mag Online | Le Net Expert Informatique

Un service de détection de limitation de l'impact des attaques DDoS

Les menaces à la cyber sécurité connaissent une évolution croissante en termes de complexité, de rythme et d'échelle. Selon un enquête récente mondiale, menée en collaboration avec TechValidate, les clients sont le plus préoccupés par l'impact des cyberattaques de type DDoS sur la diffusion de contenu numérique [TVID : 957-39D-E29]. En outre, la majorité des clients interrogés croient que leur fournisseur de CDN est le mieux placés pour les aider à détecter et à limiter l'impact des attaques DDoS [TVID : 0B3-2FC-2FD].

Limelight Networks, Inc. annonce la disponibilité de sa solution DDoS Attack Interceptor, basée sur la plateforme Limelight OrchestrateTM (« Orchestrate »). Composante centrale du service Limelight Orchestrate Security, DDoS Attack Interceptor offre plusieurs lignes de défense pour la protection des clients : notification proactive en cas d'attaque, nettoyage du trafic et protection contre les coûts imprévus en raison des pics de trafic.

En accord avec cette préférence des clients, DDoS Attack Interceptor est directement intégrée dans le réseau CDN mondial de Limelight. Contrairement aux offres concurrentes, qui fonctionnent au niveau du routeur, la solution de Limelight place la détection directement dans le PoP du réseau CDN, offrant la seule détection en fonction de la situation accompagnée de technologies d'atténuation dans le Cloud. Le système de détection perfectionné de Limelight surveille en permanence le réseau pour détecter tout trafic malveillant. Allant au-delà des simples techniques de vérification des signatures, le moteur de détection utilise des techniques brevetées sur les comportements qui comparent la base de référence à partir du volume et des schémas et qui différencie de manière intelligente un bon trafic d'un trafic douteux.
Lorsqu'une attaque est détectée, le système détermine le centre de nettoyage distribué optimal dans le monde et y dirige le trafic, qui y sera alors filtré avant d'être retransmis à l'origine. Le service est entièrement fourni dans le Cloud via la plateforme Limelight Orchestrate, ce qui offre des performances élevées et une haute disponibilité, surtout en temps de sérénité, tout en offrant simultanément une détection continue. Les clients n'ont pas besoin d'acheter un matériel quelconque et aucune dépense d'investissement n'est nécessaire pour bénéficier de la totalité des fonctionnalités de cette offre.
Avec une capacité Egress de plus de 11 Tbit/s, la plateforme Orchestrate de Limelight gère plus de sept milliards de demandes utilisateurs par heure, garantissant la capacité de DDoS Attack Interceptor à gérer les plus grandes cyberattaques connues aujourd'hui. La solution offre un délai d'atténuation à la pointe de l'industrie, basculant rapidement en mode atténuation et offrant une base de référence coordonnée, une détection active et une atténuation rapide qui assurent le démarrage rapide du nettoyage, avec une très courte durée d'accélération, même pour les attaques plus difficiles à détecter.
Aujourd'hui, Limelight a également annoncé la disponibilité de Orchestrate 3.0, une plateforme complète conçue spécialement pour la diffusion de contenu numérique avec une qualité d'expérience (QoE) exceptionnelle. La plateforme Orchestrate 3.0 comprend le plus grand nombre d'améliorations jamais apportées par la société, que ce soit au niveau de l'infrastructure, de la suite logicielle ou de l'offre de services. Elle améliore ainsi pratiquement tous les aspects de l'expérience client et élargit l'offre de la société en incluant de nouveaux services axés sur la sécurité.

Réseau privé mondial Limelight
Le réseau mondial Limelight est l'un des réseaux privés de diffusion de contenu numérique les plus vastes au monde. Avec plus de 80 PoPs et 11 Tbps de capacité Egress, ce réseau a permis la diffusion sur Internet de quelques-uns des évènements les plus importants au monde. Le réseau Limelight assure la diffusion du contenu numérique tout en offrant une expérience d'une qualité irréprochable, quels que soient les pics de trafic et indépendamment des caprices de l'Internet public. Les autres améliorations que la version V3.0 apporte au réseau Limelight comprennent des mises à niveau des disques à circuits intégrés, une capacité supplémentaire de traitement, une bande passante plus large et une connectivité accrue, et de nouveaux points de présence dans le monde.

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

Source : http://www.globalsecuritymag.fr/Limelight-lance-un-service-de,20150312,51490.html

---

Trend Micro dresse le bilan de l'année écoulée dans son rapport annuel de sécurité | Le Net Expert Informatique

Trend Micro dresse le bilan de l'année écoulée dans son rapport annuel de sécurité

Les cyber-attaques réussies contre Sony, avec environ 100 Téraoctets de données piratées et des dommages estimés à près de 100 millions de dollars, sont venues couronner une année mémorable en termes de cyber-sécurité. Le rapport de sécurité annuel de Trend Micro, intitulé « The High Cost of Complacency » (Le coût élevé de la négligence), revient sur ce piratage ainsi que sur les événements de sécurité majeurs qui ont de nouveau illustré l'obstination des cybercriminels et la sophistication de leurs attaques en 2014.

« L'essentiel d'une stratégie de cyber-sécurité repose sur l'identification de ce qui est le plus important, le déploiement de technologies adéquates et la sensibilisation des utilisateurs », explique Raimund Genes, CTO de Trend Micro. « C'est le rôle de tout un chacun, pas seulement des informaticiens, que de préserver les données sensibles de l'entreprise. »
Les informations rassemblées au sein de ce rapport confirment notamment la prédiction formulée par Trend Micro fin 2013, selon laquelle un piratage majeur de données se produirait en moyenne une fois par mois. Pour les entreprises, le besoin de déployer des dispositifs de protection des réseaux et de détection des intrusions se fait d'autant plus sentir.
« A l'image du piratage de Sony, l'envergure et la portée des attaques perpétrées l'année dernière se sont avérées dramatiques », commente Tom Kellermann, Chief Cybersecurity Officer de Trend Micro. « Malheureusement, il ne s'agit sans doute que d'un aperçu de ce que l'avenir nous réserve. »

Parmi les principaux éléments traités dans ce rapport de sécurité 2014 :
Il ne faut négliger aucune menace, aussi minime soit-elle. Les pirates utilisent des méthodes simples pour déjouer la sécurité des entreprises et causer d'importants dégâts.
Les RAM scrapers, ces malware installés sur les terminaux de points de vente, sont presque devenus monnaie courante en 2014. Plusieurs cibles notables ont perdu des millions de données clients au profit des malfaiteurs tout au long de l'année.
De nouvelles attaques ont démontré qu'aucune application n'était invulnérable face à des pirates qui se diversifient.
La banque en ligne et mobile a connu ses plus importants défis de sécurité en 2014, notamment une sérieuse remise en question de l'authentification à deux facteurs comme garant de la sécurité des opérations sensibles.
Les ransomware ont gagné en puissance et en sophistication. Ils se sont étendus à de nouvelles régions du monde et à de nouvelles cibles. Ils vont désormais jusqu'à chiffrer les fichiers sur les systèmes infectés pour s'assurer du paiement de la rançon.

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

Source : http://www.globalsecuritymag.fr/Trend-Micro-dresse-le-bilan-de-l,20150309,51375.html

L’État veut réglementer l’utilisation de drones | Le Net Expert Informatique

	L’État veut réglementer l’utilisation de drones

Le gouvernement prépare des règlements pour contrôler l'utilisation des drones pour la photographie ou pour faire des vidéos. C'est ce qu'a annoncé le Premier ministre, sir Anerood Jugnauth, hier au Parlement, suite à une question d'Alan Ganoo, du Mouvement militant mauricien (MMM).

En effet, les appareils volant sans pilote pesant entre 7 et 20 kg sont contrôlés par les Civil Aviation Regulations de 2007. Les drones de moins de 7 kg sont considérés comme des «model aircraft» à but récréatif, et ne sont sujets à aucun règlement.

«Leur utilisation, pour la reconnaissance également, représente de nouveaux défis pour la sécurité, notamment pour les avions et pour le respect de la vie privée. Elle nécessite donc des règlements», a ajouté le Premier ministre. Ces règlements sont prêts, a-t-il dit. Il y aura des consultations avec les autorités concernées pour les calquer sur les modèles européens.

Les drones interdits de vol ?
Alan Ganoo a ajouté que sa question concerne uniquement la sécurité et le respect de la vie privée. En même temps, il a voulu savoir si le gouvernement compte introduire une loi. Sir Anerood Jugnauth a répondu que pour le moment, il s'agira de règlements. Toutefois, si cela s'avère nécessaire, le gouvernement pourrait légiférer, a précisé le PM.

Le leader du MMM, Paul Bérenger, a ajouté que l'Inde a banni les drones en attendant l'introduction d'une loi. «Je ne dis pas qu'il faille en faire autant, mais est-ce que le gouvernement fera quelque chose en attendant l'introduction des nouveaux règlements ?», a-t-il demandé.
Le Premier ministre a répondu en boutade : «Je me prépare à tout bannir.» Shakeel Mohamed a demandé au gouvernement de ne pas être trop dramatique non plus.

Cet article concerne l'île Maurice.

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

Source : http://www.lexpress.mu/article/259731/letat-veut-reglementer-lutilisation-drones