Sécurité informatique des collectivités : Toujours plus avec moins…

	Sécurité informatique des collectivités : Toujours plus avec moins…

Les collectivités et leurs groupements, notamment les communautés de communes, peinent encore à prendre en compte tous les aspects de la sécurité des systèmes d'information, à en croire le rapport 2016 du Club de la sécurité de l'information Français (Clusif). Alors qu'elles se numérisent de plus en plus, les collectivités vont devoir maintenir voire accentuer leurs efforts dans un contexte budgétairement contraint.

Dans l'édition 2016 de son rapport sur les « Menaces informatiques et pratiques de sécurité en France » (Mips), le Club de la sécurité de l'information Français (Clusif) se penche de nouveau sur les collectivités (1). De plus en plus nombreuses à recourir à des services dématérialisés, celles-ci auront à charge de « maintenir » leurs « efforts » pour « assurer la sécurité de leur système d'information et des informations qui leur sont confiées », selon les auteurs de ce document de plus de cent pages. Le tout dans un contexte budgétaire restreint. Globalement, alors que le sentiment de dépendance à l'égard du numérique s'enracine, la sécurité des systèmes d'information est « efficiente dès lors que les moyens organisationnels, humains et financiers sont clairement attribués » et que la direction est fortement impliquée, indique le rapport. Cependant, sur la base des 203 collectivités interrogées, il est fait état de grandes disparités entre les échelons territoriaux, où les communautés de communes sont à la peine.

Stagnation des budgets malgré la numérisation en cours

Publié tous les deux ans, le « Mips » délivre un bilan approfondi des usages en matière de sécurité de l'information ; et inclut dans son édition 2016 (comme tous les 4 ans) les collectivités territoriales de grande taille. Autrement dit les communes de plus de 30.000 habitants, les intercommunalités (communautés de communes, d'agglomération, communautés urbaines ou encore les métropoles) et enfin les régions et les départements (regroupés par le rapport sous le terme de conseils territoriaux).

Côté résultats, si une grande partie des collectivités interrogées a confié un sentiment toujours croissant de « dépendance » vis-à-vis de l'informatique (75% contre 68% en 2012), les budgets qui y sont liés tendent pourtant à baisser et restent très disparates (avec un rapport de 1 à 100 entre les plus petits et les plus importants). Ainsi, près de 54% des collectivités ont un budget informatique inférieur à 100.000 euros en 2016, contre 45% en 2012. En moyenne, les conseils territoriaux sont les mieux dotés avec 5,8 millions d'euros, pour un million d'euros dans les intercommunalités et 800.000 euros dans les villes.

Dans ce total, la part de la sécurité est difficilement évaluable et demeure au mieux constante (67% des cas) ou diminue (28% des collectivités contre 14% en 2012 y consacrent moins de 1% de leur budget informatique). Enfin, si augmentations il y a, elles servent avant tout à mettre en place des solutions de sécurité (25%), même si des efforts importants sont effectués en matière organisationnelle (11%) et en sensibilisation (9%).

Pas de politique de sécurité sans personnels qualifiés

Bien que majeur, l'aspect financier n'occupe que la deuxième place des principaux freins pour les collectivités (à 45%), pour qui l'absence de personnels qualifiés semble être le véritable problème (à 47%), accru par un manque avoué de connaissance (38%). En conséquence, les contraintes organisationnelles (29%) et les réticences de la direction générale, des métiers ou des utilisateurs (24%) ferment la marche.

Malgré tout, l'étude montre que les collectivités sont de plus en plus nombreuses à formaliser leur politique de sécurité (PSI), en particulier les villes (54% contre 43% en 2012) et les conseils territoriaux (52% contre 35%). A l'inverse, les communautés de communes sont à la peine (un peu plus de 2 sur 10).

Concrètement, les DSI (directions des systèmes d'information) gèrent les politiques de sécurité dans 65% des cas, alors que les directions générales des services tendent à se désengager (impliquées dans 54% des cas, contre 80% en 2012). Dans 21% des cas, des élus y ont contribué. Enfin, on notera que la présence d'un responsable de la sécurité des systèmes d'information (RSSI) « serait une condition sine qua none pour disposer d'une PSI ». Par ailleurs de plus en plus nombreux (+3 points, à 35%), les RSSI voient cependant leur fonction se diluer, avec 39% de personnel dédié en 2016 contre 62% en 2012 dans les villes, pour ne citer qu'elles. Enfin, ils sont bien souvent rattachés à la DGS (dans les communautés de communes notamment) ou à la DSI (dans les régions ou les départements par exemple) – selon une règle qui veut que « plus la collectivité est petite et plus les fonctions sont cumulées par le comité de direction »…[lire la suite]

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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

Original de l’article mis en page : Sécurité informatique : les collectivités encouragées à maintenir leurs efforts – Localtis.info – Caisse des Dépôts

---

Le DSI traditionnel dans les collectivités locales est voué à disparaître

Le DSI traditionnel dans les collectivités locales est voué à disparaître

---

Le DSI traditionnel des collectivités locales est voué à disparaître avec l'arrivée des nouvelles générations et la disponibilité de solutions en mode Saas. C'est l'avis de David Larose, directeur de l'aménagement numérique de la ville de Drancy, et jusqu'au début 2016, DSI emblématique de la communauté de communes de l'aéroport du Bourget.

Il s'est exprimé à l'occasion de l'événement Cloud Week 2016 le 6 Juillet. Il est intervenu également sur la table ronde **Choisir ses prestataires et conserver la maîtrise du Cloud**, créée et animée par La Revue du Digital.

Le DSI n'est pas fait pour monter des Data Center ni surveiller des clignotants
– David Larose
'L'ancien DSI ne mâche pas ses mots. "*Le DSI dans les collectivités locales, c'est un dinosaure, il est voué à disparaître. Pourquoi ? Parce que le DSI n'est pas fait pour monter des Data Centers et regarder si la lumière clignote verte ou rouge, mais pour s'occuper des vrais métiers et aider les citoyens*," débute David Larose.

Les nouvelles générations se débrouillent seules
Si le DSI n'existe plus qui va faire son métier ? "*Cela va être un modèle réparti. Les nouvelles générations qui arrivent chez nous, elles savent elles-mêmes trouver leurs ressources dans le Cloud, en mode Saas. Et finalement, on ne sert plus à rien nous DSI car ce sont les services eux-mêmes qui vont être moteurs dans leurs choix d'applicatifs, et dans le choix de l'évolution du logiciel. C'est pour cela que je dis que le DSI est fini*," tranche-t-il.
Qu'en est-il des logiciels pour le secteur des collectivités locales qui est un marché très spécifique ? "*Les logiciels pour les collectivités locales sont une honte pour le métier*," répond David Larose.

Les logiciels pour les collectivités locales sont une honte
– David Larose
"*Elles ont des interfaces d'il y a trente ans, ou des socles de développement inadaptés. C'est pour cela, que s'il y a une offre Saas, on plonge vers l'offre Saas. Sinon, nous faisons nous mêmes nos développements, ou nous les externalisons, comme cela on sait que la technologie est récente, et n'a pas plus de vingt ans et parfaitement adaptée à ce que l'on veut*," poursuit-il.

Nouvel appel d'offres
La communauté de communes de l'aéroport du Bourget a externalisé l'ensemble de son système d'information dans le Cloud, il y a déjà trois ans chez OVH. "*Nous allons de nouveau lancer un appel d'offres cette année. A mon avis, Orange va être comme d'habitude plus cher que tout le monde. OVH devrait répondre et on va voir s'il y a un nouveau challenger français qui va se présenter, SFR étant mort et enterré*," conclut-il.
Source : larevuedudigital.com

Denis Jacopini anime des **conférences et des formations** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique, découvrir et comprendre les arnaques et les piratages informatiques pour mieux s'en protéger et se mettre en conformité avec la CNIL en matière de Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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

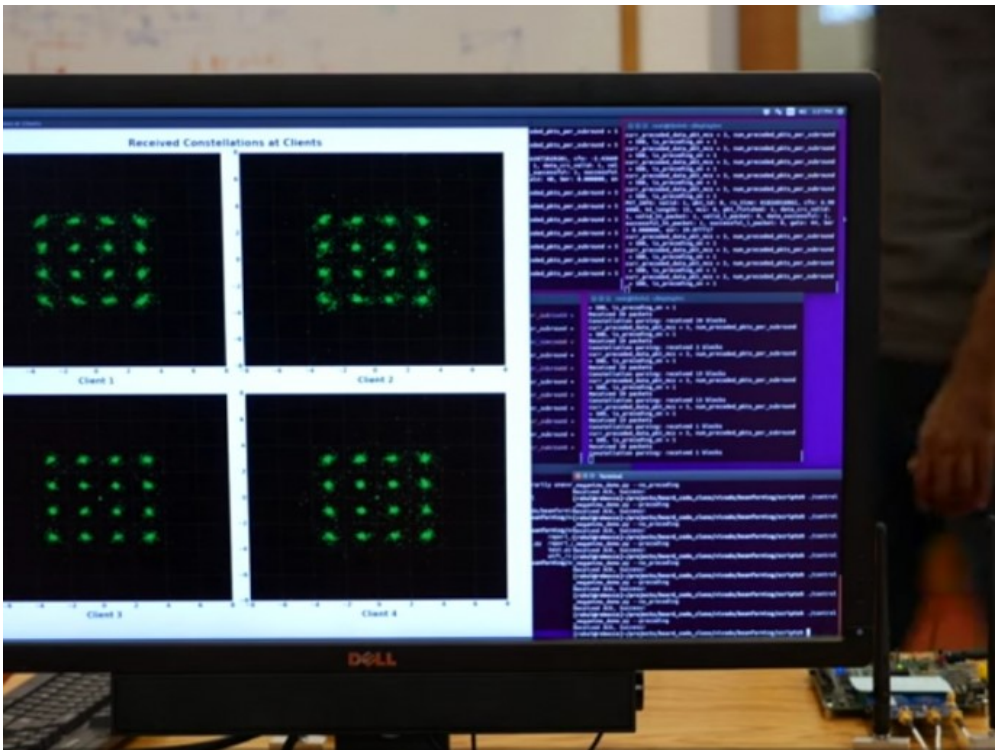
Contactez-nous

Réagissez à cet article

Original de l’article mis en page : “Le DSI dans les collectivités locales, c’est fini” | La Revue du Digital

---

La vitesse de votre Wi-Fi sera bientôt multipliée par 3



La vitesse de votre Wi-Fi sera bientôt multipliée par 3

Des chercheurs du MIT ont mis au point un système qui coordonne différents points d'accès Wifi environnants pour palier la congestion du trafic.

Des chercheurs du CSAIL (Computer Science and Artificial Intelligence Lab au Massachussetts Institute of Technology) ont développé une technique qui améliore grandement les performances du Wifi et des communications sans fil plus généralement.

Ezzeldin Hamed, Hariharan Rahul, Mohammed Abdelghany et Dina Katabi présentent leurs travaux dans le cadre du ACM SIGCOMM 16 (Association for Computing Machinery's Special Interest Group on Data Communications), qui se tient au Brésil (à Florianópolis) jusqu'au 26 août. Ils entendent palier les risques de congestion qui peuvent survenir dans un réseau sans fil traditionnel quand deux points d'accès rapprochés émettant à la même fréquence risquent de causer des interférences.

Aujourd'hui, la solution pour éviter ces interférences consiste à traiter les requêtes les unes après les autres, ce qui restreint inévitablement l'envoi des données (même si, à haute fréquence de traitement, cela ne se perçoit pas tant que le point d'accès n'est pas saturé de connexions). Un peu comme si les supermarchés n'étaient équipés que d'une seule caisse obligeant les consommateurs à d'interminables queues pour payer leurs achats (même si la caissière est super rapide…). Les scientifiques du MIT ont donc envisagé une autre approche visant à coordonner de multiples points d'accès sans fil à la même fréquence sans créer d'interférences.

Utiliser efficacement le spectre disponible

« Dans le monde sans fil d'aujourd'hui, vous ne pouvez pas résoudre le problème de la contraction du spectre en multipliant les émetteurs, car ils continueront d'interférer les uns avec les autres, explique Ezzeldin Hamed, selon des propos repris par le site de news du MIT. *La réponse tient dans une coordination de tous les points d'accès afin d'utiliser efficacement le spectre disponible. »* Et cette réponse se traduit par la mise au point du **dispositif MegaMIMO 2.0**, un boîtier de la taille d'un routeur traditionnel qui embarque processeur, système de traitement radio temps réel, émetteur-récepteur et, surtout, algorithmes maison.

Ces derniers génèrent un signal qui permet à de multiples émetteurs indépendants de transmettre des données sur la même ressource hertzienne à plusieurs points d'accès indépendants sans interférer les uns avec les autres grâce à une synchronisation de leur phase d'ondes. Autrement dit, une sorte de réseau MIMO distribué que nombre d'ingénieurs tenaient jusqu'à présent pour difficile à mettre au point. Mais l'équipe du CSAIL a fait une démonstration de l'efficacité du MegaMIMO 2.0, via une simulation de quatre ordinateurs portables en mouvement dans une salle de réunion. Il en ressort une augmentation des débits de 330 % par rapport à un système Wifi traditionnel (et même par rapport à leurs premiers travaux, MegaMIMO, présentés en 2012 et dans lesquels l'utilisateur devait fournir manuellement les informations sur les différentes fréquences). Sans oublier un doublement de la portée du signal. MegaMIMO permet même d'adapter le signal en fonction des obstacles environnants (par exemple lorsque quelqu'un se positionne entre l'émetteur et le récepteur).

Applicable aux réseaux mobiles

Les chercheurs entendent poursuivre leurs travaux pour parvenir à coordonner des dizaines de routeurs sans fil afin de gérer toutes ces ressources comme une seule, ce qui devrait encore démultiplier les performances. Mais le système vise avant tout à palier les risques de congestion du réseau alors que ses usages progressent beaucoup plus vite que la disponibilité des ressources hertziennes.

Dans l'absolu, le MegaMIMO pourrait en effet parfaitement s'appliquer aux réseaux cellulaires. Et permettrait d'assurer des services mobiles de qualité dans les endroits particulièrement fréquentés, comme les stades lors des événements sportifs, les gares les jours de grève ou lors d'incidents de circulation des transports, etc. En attendant, les campus et grandes entreprises pourraient être les premiers à adopter le MegaMIMO pour fournir des accès Wifi efficaces… si le système est commercialisé un jour.

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

Original de l'article mis en page : MegaMIMO 2.0, le système qui multiplie par 3 les performances du Wi-Fi

Eleanor, nouvelle menace sur la planète Mac

Eleanor, nouvelle menace sur la planète Mac

Alors que beaucoup d'utilisateurs de Mac se montrent parfois négligents en matière de sécurité, les équipes de BitDefender ont détecté un nouveau backdoor baptisé Eleanor qui ciblent les Mac et qui peut causer d'importants dégâts sur les machines. En effet, il offre la possibilité aux pirates de prendre le contrôle d'une machine à distance.

Le backdoor Eleanor à l'assaut des Mac

Comme souvent, c'est l'éditeur BitDefender qui a identifié la nouvelle menace qui pèse sur les Mac. Eh oui, même si les dangers sont généralement moindres sur Mac que sur PC, voilà que ceux qui ont choisi les ordinateurs d'Apple doivent se montrer vigilants.

En effet, dès lors que ce backdoor silencieux est parvenu à infecter une machine, il a la capacité de permettre à un attaquant de prendre le contrôle du Mac à distance. Ainsi, les hackers peuvent s'en servir pour voler des données présentes sur la machine piratée, télécharger des applis frauduleuses ou même pour détourner la webcam, une pratique de plus en plus courante.

Reste que l'infection du Mac ne se produit pas toute seule et qu'elle est l'une des conséquences du téléchargement de l'application malveillante Easy Doc Converter. En effet, lors du démarrage d'OS X, cette appli va installer sur le Mac trois composantes : un service Tor, un service web capable de faire tourner PHP et un logiciel dédié. Autrement dit le matériel indispensable pour que s'installe, sur Mac, un backdoor silencieux comme Eleanor.

L'intégralité des Mac concernée par Eleanor ?

Si BitDefender a tenu à alerter sur sa découverte, il semblerait tout de même que tous les Mac ne soient pas tous concernés par cette menace.

En effet, parce que le logiciel Easy Doc Converter n'est pas signé numériquement avec un certificat approuvé par Apple, les risques d'infection sont réduits. D'ailleurs, la marque à la pomme a tenu à le préciser en rappelant que tous les Mac dotés de la protection Gatekeeper n'avaient rien à craindre.

Article original de Jérôme DAJOUX

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

Original de l’article mis en page : Eleanor, nouvelle menace sur la planète Mac

---

Peut-on vraiment forcer les collectivités locales d’utiliser un « cloud souverain » ?

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'intérieur
Direction générale des collectivités locales
Sous-direction des compétences et des institutions locales

Ministère de la culture et de la communication
Direction générale des patrimoines
Service interministériel des Archives de France

Note d'information du 5 avril 2016 relative à l'informatique en nuage (*cloud computing*)

Références : DGP/SIAF/2016/006
~~DGCL~~
NOR: MCCA6143540

Ministère de la Culture et de la Communication
05 AVR. 2016 – 2016/004
SAFIG/SDAIG/MPDOC

Le directeur général des collectivités locales et le directeur chargé des archives de France

à

Mesdames et Messieurs les préfets de région
et Mesdames et Messieurs les préfets de département

Peut-on vraiment forcer les collectivités locales d’utiliser un « cloud souverain » ?

---

par Emilien Ercolani
Une circulaire d'avril dernier, qui sert à rappeler le cadre légal applicable, écrit noir sur blanc qu'il est illégal d'utiliser « un cloud non souverain » pour les documents créés et gérés par les collectivités territoriales. Au-delà d'être illusoire, la mesure est en plus ubuesque.

C'est une circulaire du 5 avril 2016 qui a remis le sujet sur le tapis. Relative à l'informatique en nuage, elle explique tout d'abord que les documents et données numériques produits par les collectivités territoriales « *relèvent du régime juridique des archives publiques dès leur création* ». Les archives publiques sont considérées comme « *des trésors nationaux* », et les données numériques ne font pas exception.
Le raisonnement est donc le suivant : pour protéger les « *trésors nationaux* », il convient de les conserver sur le territoire national pour ainsi dire garantir leur préservation. « *Un trésor national ne peut pas sortir du territoire douanier français sinon à titre temporaire* », souligne encore le texte. Pour les données numériques, il faut donc qu'elles soit traitées et stockées en France. Raisonnement logique… pour qui ne connaît pas vraiment le monde de l'informatique.


Ministère de l'intérieur
Direction générale des collectivités locales
Sous-direction des compétences et des institutions locales

Ministère de la culture et de la communication
Direction générale des patrimoines
Service interministériel des Archives de France

Note d'information du 5 avril 2016 relative à l'informatique en nuage (*cloud computing*)

Référence : DGCL/SIAF/2016/006

Le directeur général des collectivités locales et le directeur chargé des archives de France

à

Mesdames et Messieurs les préfets de région et Mesdames et Messieurs les préfets de département

Ministère de la Culture et de la Communication
05 AVR. 2016 - 2016/004
SAFIG/SDAIG/MPDOC

Les conséquences de la loi appliquée à la lettre

Concrètement, cela voudrait dire qu'une collectivité territoriale doit donc traiter et stocker ses données, anciennes et futures, sur le territoire. Et donc, dans des data centers installés sur le sol français. Ce qui implique que toutes les suites d'outils logiciels et bureautiques en mode cloud sont désormais interdites : Office 365 et les Google Apps (pour ne citer que les plus connues) sont désormais bannies puisque ni l'une ni l'autre ne sont en mesure de garantir un stockage sur le territoire national.
« *L'utilisation d'un cloud non souverain (…) est donc illégale pour toute institution produisant des archives publiques* », poursuit la circulaire. A savoir que la définition d'un cloud souverain pour la direction générale des collectivités locales (DGCL), qui dépend du ministère de l'Intérieur, est la suivante :
Modèle de déploiement dans lequel l'hébergement et l'ensemble des traitements effectués sur des données par un service de cloud sont physiquement réalisés dans les limites du territoire national par une entité de droit français et en application des lois et normes françaises.

Une circulaire « politique »

*La **circulaire** s'appuie toutefois sur des textes de loi, et notamment sur les articles L211-1 et L211-4 du Code du Patrimoine, utilisés dans le **Référentiel général de gestion des Archives**. Mais, concrètement, cela traduit d'une part une méconnaissance de l'informatique en règle générale, d'autre part des mesures qui ne sont pas réalistes.*
Responsable juridique du Syntec Numérique, Mathieu Coulaud nous explique tout d'abord que cela ne pénalise pas que Google ou Microsoft, mais aussi des acteurs européens ; l'Allemand T-Systems héberge par exemple de nombreuses données des collectivités territoriales françaises. D'autre part, il s'étonne « qu'aucune consultation et d'étude d'impact n'aient été réalisées ». Pour lui, cette circulaire est donc purement politique dans le sens où :
• Rien n'a été fait pour ouvrir le dialogue et s'informer des conséquences d'une telle mesure
• Cela dénote une incompréhension de la part des pouvoirs publics mais aussi les dissonances entre les différents ministères
« Nous avions écrit au directeur du SIAF (Service Interministériel des Archives de France) en 2015. Nous avons reçu sa réponse en janvier 2016, qui était en somme une fin de non-recevoir », poursuit Mathieu Coulaud. « Pour nous, ils confondent sécurité et localisation des données ». Effectivement, car même l'Anssi ne semble pas avoir été consultée, elle qui prépare un label « Secure Cloud » sensé garantir la souveraineté des données hébergées.

***Exclusif** : ce mercredi 6 juillet a lieu une réunion interministérielle qui réunit notamment Bercy, Matignon et le ministère de la Culture. Les administrations vont donc se parler et le sujet sera vraisemblablement à l'ordre du jour.*
« Nous avons déjà été reçus par différents ministères (Economie, Culture, etc.) mais sans rien obtenir. Plusieurs recours sont possibles, notamment concernant l'accès à la commande publique. Nous estimons qu'il existerait avec cette circulaire une vraie discrimination entre les acteurs, ce qui est contraire à la loi. Le ministère de la Culture assure que tout est viable juridiquement, mais je n'ai rien pu vérifier », ajoute Mathieu Coulaud qui souligne : « nous nous réservons des actions possibles d'influence et de droit ».

Une double lecture

Le rappel du cadre légal a rapidement fait réagir de toutes parts. « Je ne peux m'empêcher de penser qu'il s'agit de fausses bonnes nouvelles pour les prestataires de services comme pour les collectivités locales », estime Christophe Lejeune, directeur général de l'entreprise nantaise Alfa Safety qui persiste : « Enfermer dans un cadre strictement national un service innovant comme le cloud est un contre-sens ». Pour le Syntec Numérique, la circulaire va à rebours du projet de loi République Numérique, crée des barrières protectionnistes et freinera la transformation numérique. Sans compter qu'elle ne dit rien sur la nature des données en elles-mêmes. « Si un DSI envoie un smiley, cela devient un trésor national !« , ironise Mathieu Coulaud.
Mais à bien y regarder, la circulaire en question n'est-elle pas fondamentalement positionnée pour défendre les enjeux nationaux ? Et pourquoi pas faire émerger un nouveau « cloud souverain » français, voire des alternatives logicielles en mode cloud ? Opportuniste, l'hébergeur du Nord OVH rappelle non seulement son implantation en France mais aussi ses certifications et finalement qu'il est un « acteur national responsable, capable d'héberger sans risque les données issues du travail et des archives des différentes institutions publiques ; créant ainsi un Cloud véritablement souverain et fonctionnel ».

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

Original de l'article mis en page : Les collectivités locales forcées d'utiliser un « cloud souverain » ?

Le nombre de cyberattaques contre des cibles françaises double chaque année

Le nombre de cyberattaques contre des cibles françaises double chaque année

Le salon international Eurosatory de défense et de sécurité s'ouvre lundi près de Paris alors que les cyberattaques contre des cibles françaises se multiplient.

Le salon international Eurosatory de défense et de sécurité s'installe comme tous les deux ans à partir de lundi à Villepinte, près de Paris. Cette manifestation qui rassemble les stratèges et les industriels du monde entier met de plus en plus l'accent sur deux concepts devenus incontournables : l'utilisation des drones et les outils de la cyberguerre. Une demi-douzaine de conférences se tiendront cette semaine sur la cybermenace et sur les moyens de la contrer ou de la mettre en œuvre. En France, depuis l'adoption du livre blanc 2013 et la loi de programmation militaire 2014-2019, la dimension « cyber » de nos armées « a changé de braquet », comme le confie au *JDD* l'un des meilleurs experts gouvernementaux de ce dossier.

Selon lui, le nombre de cyberattaques contre des cibles françaises double chaque année et le niveau de sophistication des agressions également. « Un individu aujourd'hui peut nous faire autant de mal qu'un État », précise notre source. Chaque jour en France, les unités informatiques liées aux institutions ou aux entreprises du secteur de la défense sont agressées par des milliers d'attaques. Des raids visant à saturer des adresses liées au ministère de la Défense se multiplient et il peut arriver que le compte personnel du ministre soit visé avec intention de nuire. Au point qu'aujourd'hui pas une seule clé USB ne peut entrer dans une installation de défense française sans être passée par une « station blanche » de décontamination.

Détruire sans avoir à bombarder

Mais le plus grand risque serait évidemment que nos unités militaires engagées sur un théâtre d'opérations soient attaquées en pleine action. Le pacte défense cyber lancé début 2014, et renforcé après les attentats de 2015, a prévu un investissement de plus d'un milliard d'euros et le triplement des effectifs militaires et civils concernés. « Aujourd'hui, plus un seul déploiement d'une unité sur le terrain ne se conçoit sans un accompagnement cyber », indique notre source.

Un officier général « cyber » est affecté en permanence auprès de l'état-major au Centre de planification et de conduite des opérations (CPCO). Il ne s'agit pas seulement de se protéger lors d'une attaque mais aussi de se défendre lorsqu'elle est en cours ou même d'attaquer en cas de besoin. Tout comme le fait depuis longtemps Israël contre ses adversaires au Moyen-Orient, l'État hébreu étant avec les États-Unis, la Chine et la Russie l'un des quatre pays les plus avancés dans ce domaine avec des moyens dix à vingt fois plus importants que ceux de la France. Mais on réfléchit à Paris à l'idée de créer une cyberarmée à l'image de l'US Cyber Command américain. Pour se préparer à ces guerres invisibles où l'on peut détruire une installation ennemie sans avoir à la bombarder ou à brouiller ses radars depuis un ordinateur pour mieux déclencher des raids plus… conventionnels.

Article original de François Clemenceau – Le Journal du Dimanche

---

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

Original de l’article mis en page : Faut-il investir dans la guerre invisible? – leJDD.fr

---

Dénoncez les hôtes Airbnb, Paris vous le rendra…

Dénoncez les hôtes Airbnb, Paris vous le rendra…

La mairie de Paris appelle les voisins à dénoncer les hôtes Airbnb non déclarés aux services municipaux.

Dans le dernier chapitre d'une bataille en cours sur l'économie de partage en France, la ville de Paris demande aux résidents de dénoncer leurs voisins qui ne sont pas correctement enregistrés comme meublé ou hôte du site Airbnb.
Selon le site Europe1.fr, les services municipaux ont créée une nouvelle section sur le portail open data de la ville qui répertorie les résidents qui se sont inscrits comme un hôte Airbnb. 126 résidences sont aujourd'hui listées comme locations saisonnières sur la plate-forme Airbnb alors que le site revendique plus de 41 000 logements (35 185 appartements et 5 827 chambres). Paris serait une des destinations les plus populaires sur sa plate-forme selon Airbnb. Et avec la carte publiée par la ville de Paris, il est facile de repérer les hôtes en règle, c'est à dire qui auront déclarés ces revenus et encaissés la taxe de séjour reversée ensuite à la mairie. C'est une des batailles engagées depuis plusieurs mois par les hôteliers qui crient à la concurrence déloyale. La ville de Berlin a également engagé un bras de fer avec Airbnb pour limiter les locations de meublés sur la plate-forme.

Dans une interview avec Europe1, Mathias Vicherat, chef de cabinet pour le maire de la ville, indique espérer que les résidents utiliseront les informations sur le portail de données ouvertes pour faire pression sur leurs voisins qui ne respectent pas les règles. Les hôtes Airbnb en violation avec les règlements de la ville pourraient faire face à une amende de 25 000€ s'ils louent plus de quatre mois par an leurs logements à des touristes. « On souhaite que cela provoque un espèce de choc de conscience de civisme, et que les gens se mettent en règle d'eux-mêmes, sans attendre d'être éventuellement signalé par un de leurs voisins », dit-il. La mairie explique qu'il n'est pas question d'appeler à la dénonciation comme durant la Seconde Guerre Mondiale où cinq millions de lettres anonymes avaient été envoyées à la police ou la Gestapo… [Lire la suite]

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
Article de Serge Leblal

Source : *Paris incite ses habitants à dénoncer les hôtes Airbnb – Le Monde Informatique*

Il est nécessaire d’éduquer et de former les élèves à la cybersécurité ! | Le Net Expert Informatique

	Il est nécessaire d’éduquer et de former les élèves à la cybersécurité !

Il est désormais du devoir des institutions et de l'Éducation nationale d'encadrer les plus jeunes afin de les aider à devenir des citoyens numériquement responsables.

À l'occasion du mois européen de la cybersécurité, qui se tiendra en octobre, il est primordial de penser à faire évoluer les pratiques d'Internet des jeunes Français et de leur en inculquer les bases d'un usage sécurisé. C'est un fait, aujourd'hui les enfants de 9 à 16 ans utilisent quasiment tous Internet (93 %), et ce malgré les risques qu'il comporte (1).

Avec l'arrivée des objets connectés (smartphones, tablettes, accessoires, etc.) pouvant s'avérer être, pour certains individus parmi les plus jeunes, une réelle addiction, les cyber-risques ne cessent de croître. La formation de nos chères têtes blondes à devenir des utilisateurs responsables d'Internet et à être au fait de ses enjeux de sécurité ne doit pas seulement se limiter à celles des parents, les institutions et l'Éducation nationale doivent également y participer.

L'importance de différents niveaux d'apprentissage de la cybersécurité

Les écoles sont comme une seconde maison pour les enfants, où les enseignants viennent complémenter les parents en termes de connaissances, d'enseignement et de discipline. Voilà pourquoi l'École apparaît tout naturellement comme une bonne option pour dispenser une véritable éducation en matière de cybersécurité.

Aujourd'hui, une telle contribution est vitale dans la préparation des enfants au monde virtuel. Des sujets tels que la cyber-civilité, la cyber-image, la cyber-hygiène et la cybersécurité pourraient, par exemple, être mieux appréhendés et expliqués dans une salle de classe. Or, à ce jour, la plupart des écoles n'offrent seulement qu'un bref aperçu de ce qu'est la cybersécurité.

Bien entendu, l'enseignement de la sécurité du « cyber-life » se doit de différer en fonction de l'âge de l'élève, mais quelques règles de base sont communes à tous afin de mieux les prémunir dans le cadre de leurs interactions tant dans leur vie sociale que digitale !

Pour les plus jeunes, c'est au moment où l'intérêt des enfants pour l'univers digital est minime qu'il faut les sensibiliser à la cybersécurité. Des règles et enseignements simples pourraient être inculqués comme leur apprendre à demander l'autorisation à leurs parents avant d'utiliser un appareil, être sensibilisé à la dangerosité de communiquer avec des personnes inconnues sur le Net ou encore la nécessité de prévenir ses parents en cas d'échange bizarre sur le Net, etc.

Quant aux préadolescents, la cyberéducation doit intervenir au moment où ils commencent à jouer en ligne, à regarder des vidéos sur le Net, à créer leur propre compte sur les réseaux sociaux, etc. Afin qu'ils puissent surfer en toute sécurité, il est primordial de leur enseigner quelques bases de sécurité par exemple l'importance de créer un mot de passe efficace et sécurisé, la manière de reconnaître un site/une application sûr(e), les risques de vol existant en ligne, les dangers du téléchargement et du partage de contenu personnel sur le Web, etc.

Vient ensuite la période de l'adolescence, où les jeunes aiment se retrouver et échanger sur des sites Internet communautaires au sein desquels le risque de partage d'informations personnelles et d'interaction avec des inconnus est omniprésent. L'adolescence se présente également comme une période au cours de laquelle il faudrait renforcer l'apprentissage des adolescents en termes de pratiques éthiques, de reflet d'image, de sûreté et de sécurité des outils, etc., l'idée étant de faire des adolescents des citoyens numériques responsables et conscients de dangers que représente la Toile (addiction, hacking, phishing, cyberharcèlement, etc.).

Espérons que les actions menées par les associations et les professionnels concernés à l'occasion du mois européen de la cybersécurité s'imposent comme un détonateur dans la prise de conscience des politiques et de l'Éducation nationale quant à la nécessité de l'apprentissage numérique des plus jeunes afin de mieux protéger et sécuriser les individus et le monde de demain.

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source :
http://www.lesechos.fr/idees-debats/cercle/cercle-140152-il-est-necessaire-deduquer-et-de-former-les-eleves-a-la-cybersecurite-1160311.php?XMmKySpwheCXjjJG.99

Un électeur peut-il utiliser la liste électorale ? | Le Net Expert Informatique

Un électeur peut-il utiliser la liste électorale ?

Tout électeur peut obtenir de sa mairie une copie de la liste électorale à condition de s'engager à ne pas en faire un usage commercial.
A noter : la Commission d'accès aux documents administratifs (CADA) considère que l'accès aux listes électorales peut s'exercer par consultation gratuite sur place ou par envoi de copies, sur support papier ou informatique.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source :
http://www.aide.cnil.fr/selfcnil/site/template.do;jsessionid=16F67A95B36120F226D2F8E337B98601?name=Liste+%C3%A9lectorale+%3A+un+%C3%A9lecteur+peut-il+l%27utiliser+%3F&id=175

Le secteur public ciblé par la cybercriminalité | Le Net Expert Informatique

Le secteur public ciblé par la cybercriminalité

« Au cours du second trimestre, nous avons assisté à une mutation dans l'univers des menaces. Les pirates informatiques font désormais preuve de davantage de sophistication et de créativité afin de renforcer et de réinventer leurs méthodes d'attaques existantes », observe Raimund Genes, CTO de Trend Micro. « La vision éthérée de la cybercriminalité n'est plus d'actualité. Ce trimestre a démontré que les dommages potentiels des cyberattaques vont bien au-delà de simples bugs logiciels. Le piratage d'avions, de voitures intelligentes et des chaines de TV est en effet devenu une réalité. »

Les hackers identifient et affinent leurs approches de façon plus stratégique, ciblant ainsi leurs victimes de manière plus sélective afin d'améliorer le taux d'infection de leurs attaques. Une tendance qui reflète une réelle progression de plusieurs méthodes d'attaques traditionnelles, avec notamment un bond de 50% de l'utilisation du kit d'exploitation Angler et de +67% pour les menaces utilisant des kits d'exploitation en général. Les attaques ciblant les banques en ligne sont par ailleurs en forte augmentation dans l'hexagone, avec plus de 60% du nombre de PC infectés entre le premier et le second trimestre 2015. D'autre part, l'adware Opencandy et le malware Upatre ont été particulièrement actifs en France ce trimestre, avec respectivement 12 773 et 3 854 PC infectés. Le malware Dyre arrive quant à lui en 4ème position avec 1 469 infections.

De même, les administrations ont été les cibles privilégiées de cyberattaques au cours du second trimestre, avec les piratages massifs des données de l'Internal Revenue Service (le fisc américain) en mai et du système de l'U.S. Office of Personnel Management (une agence gouvernementale américaine responsable de la fonction publique) en juin. Le piratage des données de l'OPM constitue un modèle du genre avec, à la clé, la divulgation de données personnelles identifiables portant sur près de 21 millions d'individus. D'autres agences gouvernementales ont été impactées par des campagnes ciblées utilisant des macros malveillantes, de nouveaux serveurs C&C (Command & Control), de nouvelles vulnérabilités, ainsi que la faille zero-day Pawn Storm.

En se penchant sur le panorama global des menaces au cours du second trimestre, on remarque que les États-Unis jouent un rôle majeur, que ce soit en tant que pays d'origine mais également en tant que cible de nombreuses attaques. Les liens malveillants, le spam, les serveurs C&C et les ransomware y sont tous très présents.

Parmi les points essentiels du rapport :

Des attaques perturbant les services publics : réseaux de diffusion, avions, véhicules automatisés et routeurs résidentiels présentent non seulement un risque d'infection élevé par malware, mais sont également susceptibles d'avoir des répercussions sur l'intégrité physique de leurs utilisateurs.

Le succès d'attaques ransomware ou ciblant les terminaux de points de vente (PoS), aubaine pour les cybercriminels solitaires en quête de notoriété : en déployant les attaques FighterPoS et MalumPoS, ainsi que keylogger Hawkeye, les hackers solos "Lordfenix" et "Frapstar" ont démontré que la force de frappe d'individus isolés est aujourd'hui indéniable.

La lutte des gouvernements contre la cybercriminalité : Interpol, Europol, le département américain de la sécurité nationale et le FBI ont contribué à démanteler des réseaux botnets majeurs et déjà bien établis. D'autre part, l'inculpation de Ross Ulbricht, fondateur de Silk Road, a mis en lumière la nature obscure et redoutable du Dark Web.

Les impacts nationaux et politiques d'attaques ciblant des organisations gouvernementales : la redoutable attaque sur l'OPM a prouvé que la confidentialité de nos données personnelles n'est pas avérée. Les macros malveillantes, les tactiques d'island-hopping (piratage d'une entité tierce avant de remonter vers la cible finale) et les serveurs C&C comptent parmi les tactiques les plus utilisées pour cibler les informations gouvernementales lors d'attaques.

De nouvelles formes de menaces visant les sites web publics et les dispositifs mobiles : alors que les menaces ciblant les logiciels sont toujours d'actualité, les vulnérabilités des applications web se montrent tout aussi dangereuses. Les assaillants savent tirer parti de toute vulnérabilité existante, tandis que les applications personnalisées nécessitent une prise en charge toute aussi personnalisée afin de neutraliser ces passerelles potentielles d'intrusion.

Le rapport

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.globalsecuritymag.fr/Trend-Micro-identifie-de-nouvelles,20150917,55924.html