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).

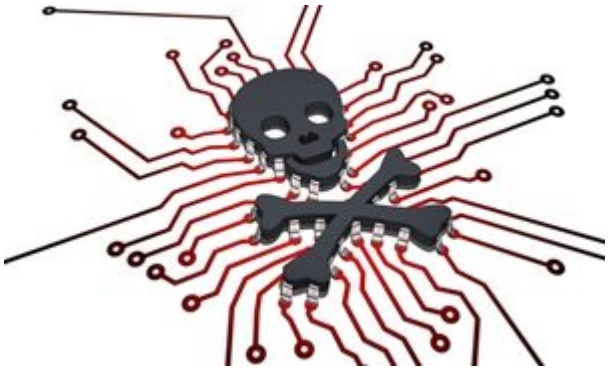
Concrètement, les DSI (directions des systèmes d'information) gèrent les politiques de sécurité dans 65% des cas, alors que les directions générales des services tendent à se désengager (impliquées dans 54% des cas, contre 80% en 2012). Dans 21% des cas, des élus y ont contribué. Enfin, on notera que 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]

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

---

Des serveurs Linux attaqués par le ransomware Fairware



Des serveurs Linux attaqués par le ransomware Fairware

Des exploitants de serveurs Linux signalent des attaques qui entraînent la disparition du dossier Internet du serveur et la non disponibilité des sites pendant une durée indéterminée.

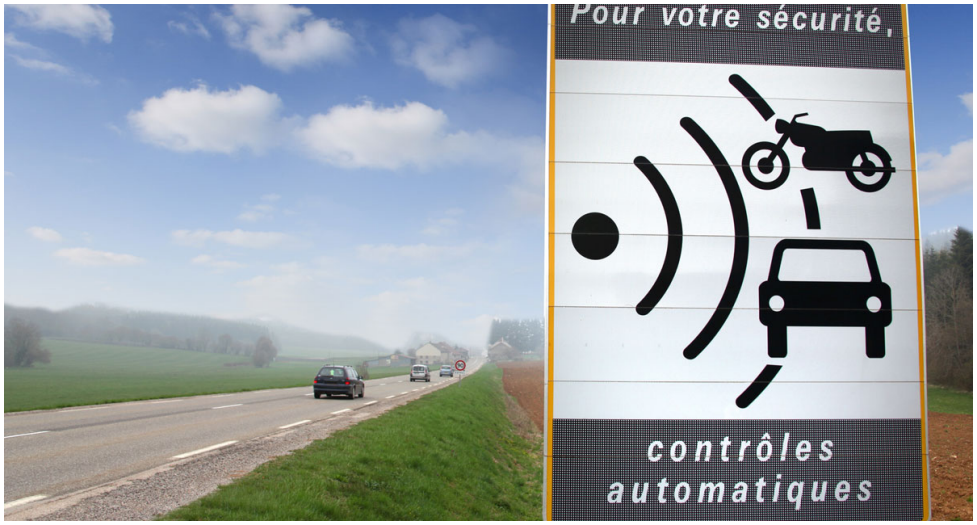
Les participants aux forums de BleepingComputer se plaignent également de l'attaque : d'après la description fournie par une des victimes, cela ressemble plus à une attaque via force brute contre SSH. Notons qu'à chaque fois, le dossier Internet est supprimé et il ne reste que le fichier read_me qui contient un lien vers une page Pastebin où apparaît la demande de rançon.
Les individus malintentionnés promettent de rendre les fichiers contre 2 bitcoins et expliquent que le serveur de la victime a été infecté par le ransomware Fairware. Toutefois, à en croire Lawrence Abrams de chez Bleeping Computer, cette affirmation pourrait ne pas être tout à fait exacte.
« Si l'attaquant télécharge un programme ou un script pour réaliser « l'attaque », il s'agit alors bel et bien d'un [ransomware]. Malheureusement, nous ne disposons pas pour l'instant des informations suffisantes. Tous les rapports montrent que les serveurs ont été compromis, mais je n'ai pas encore eu l'occasion de le vérifier » a déclaré l'expert.
La demande de rançon contient l'adresse d'un portefeuille Bitcoin. La victime est invitée à réaliser le paiement dans les deux semaines, sans quoi les individus malintentionnés menacent d'écouler les fichiers sur le côté. Le message publié sur Pastebin possède le contenu suivant : « Nous sommes les seuls au monde qui pouvons vous rendre vos fichiers . Après l'attaque contre votre serveur, les fichiers ont été chiffrés et envoyés vers un serveur que nous contrôlons. »
Le message contient également une adresse email pour l'assistance technique, mais il est interdit à l'utilisateur d'y envoyer un message uniquement pour confirmer si les attaquants possèdent bien les fichiers perdus. Lawrence Abrams affirme que pour l'instant, il ne sait pas ce que les attaquants font avec les fichiers. Vu que les fichiers sont supprimés, il serait plus logique pour les conserver de les archiver et de les charger sur un serveur et non pas de les chiffrer et de gérer des clés individuelles.
En général, les ransomwares sont diffusés via l'exploitation de vulnérabilités ou par la victime elle-même qui est amenée, par la ruse, à exécuter le malware. Dans le cas qui nous occupe, rien ne trahit ce genre d'activité. Une des victimes indiquait sur le forum de Bleeping Computer que son serveur Linux avait été épargné en grande partie par l'attaque et que les fichiers de la base de données avaient été préservés. Ce commentaire indiquait également que les individus malintentionnés avaient laissé le fichier read_me dans le dossier racine.
La suppression de fichiers et le refus de confirmer leur vol sont des comportements inhabituels pour des individus malintentionnés qui travaillent avec des ransomwares. « Il est tout à fait possible qu'il s'agisse d'une escroquerie, mais dans ce cas c'est un mauvais business pour les attaquants » explique Lawrence Abrams. « Si l'escroc ne respecte pas sa promesse après le paiement de la rançon, il aura mauvaise réputation et plus personne ne le paiera. »
Toutefois, le message sur l'infection via le ransomware et la menace de publier les données volées sont en mesure de confondre la victime et de l'amener à répondre aux exigences des attaquants. Fairware n'est pas la première cybercampagne accompagnée d'une telle menace. L'année dernière, les exploitants du ransomware Chimera, avaient adopté une astuce similaire, même si leur malware n'était pas en mesure de voler les fichiers ou de les publier sur Internet.
Lawrence Abrams explique que les victimes de ransomwares devraient s'abstenir de payer la rançon, mais si elles décident d'agir ainsi, elles doivent au moins confirmer que le bénéficiaire du paiement possède bien les fichiers.
Article original de Securelist

Réagissez à cet article

Original de l’article mis en page : Fairware attaque des serveurs Linux – Securelist

---

Est-ce que la cour de cassation a finalement jugé illégal le signalement des radars par Facebook ?



Est-ce que la cour de cassation a finalement jugé illégal le signalement des radars par Facebook ?

La cour de cassation a jugé que les pages Facebook sur lesquels les internautes s'informent de la localisation de contrôles de police sur les routes ne sont pas illégales au regard de l'état actuel du code pénal, qui interdit les avertisseurs radars.

Le fait d'utiliser un réseau social comme Facebook pour prévenir ses amis ou d'autres internautes de la géolocalisation de contrôles routiers et de radars automatiques n'est pas une violation de la loi pénale, a tranché cette semaine la cour de cassation, dont l'arrêt est cité par Le Figaro.

La haute juridiction s'était penchée sur la question à la demande du parquet de Montpellier, qui s'était pourvu en cassation après la décision de la cour d'appel de Montpellier de relaxer des individus qui avaient créé une page Facebook intitulée « *le groupe qui te dit où est la police en Aveyron* ».

Alors que la douzaine d'internautes avait été condamnée en première instance en décembre 2014, au motif que l'utilisation d'un tel groupe Facebook violerait le code de la route qui interdit les avertisseurs de radars depuis 2012, la cour de Montpellier avait adopté une lecture plus littérale de l'article R413-15 du code de la route, pour estimer que ça n'était pas la même chose.

UN RÉSEAU SOCIAL N'EST PAS UN DISPOSITIF D'AVERTISSEUR RADAR

Cet article interdit les « *dispositifs ou produits visant à avertir ou informer de la localisation d'appareils, instruments ou systèmes servant à la constatation des infractions à la législation ou à la réglementation de la circulation routière* ». Toute la question était de savoir si un groupe Facebook, ou équivalent, pouvait être assimilé à un « *dispositif visant à avertir ou informer de la localisation* » de contrôles de sécurité routière.

.La cour de cassation apporte une réponse claire puisqu'elle indique que « *l'utilisation d'un réseau social, tel Facebook, sur lequel les internautes inscrits échangent des informations, depuis un ordinateur ou un téléphone mobile, ne peut être considérée comme l'usage d'un dispositif de nature à se soustraire à la constatation des infractions relatives à la circulation routière incriminée par l'article R.413-15 du code de la route* ».

Peu importe, au final, que les internautes en question aient utilisé des messages cryptiques pour se faire comprendre (du genre « les poulets cuisent au soleil à 500 mètres du rond point »). Même s'ils avaient communiqué de façon très explicite, la loi ne l'interdit pas, au grand dam de la gendarmerie qui doit de temps en temps rappeler que signaler des contrôles routiers, c'est aussi aider des personnes recherchées qui peuvent être appréhendées par ce biais.

Nul doute, dès lors, que des propositions visant à compléter la loi devraient parvenir sur nos écrans dans les prochaines semaines ou les prochains mois.

Article de Guillaume Champeau

Réagissez à cet article

Original de l'article mis en page : Signaler des radars avec

Facebook ? La cour de cassation juge que c’est légal – Politique – Numerama

---

Directive NIS adoptée: quelles conséquences pour les entreprises?

Directive NIS depuis juillet. Des changements pour les entreprises?

En juillet dernier, le Parlement européen a adopté la directive NIS (Network and Information Security). Les opérateurs de services ainsi que les places de marché en ligne, les moteurs de recherche et les services Cloud seront soumis à des exigences de sécurité et de notification d'incidents.

C'est fait ! La directive NIS a été approuvée le 6 juillet par le Parlement européen en seconde lecture, après avoir été adoptée en mai dernier par le Conseil de l'Union européenne. Cette directive est destinée à assurer un « niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne ». Les « opérateurs de services essentiels » et certains fournisseurs de services numériques seront bien soumis à des exigences de sécurité et de notification d'incidents de sécurité.

Sécuriser les infrastructures

Du côté des fournisseurs de services numériques, les places de marché en ligne, les moteurs de recherche et les fournisseurs de services de Cloud actifs dans l'UE sont concernés. Ils devront prendre des mesures pour « assurer la sécurité de leur infrastructure » et signaler « les incidents majeurs » aux autorités nationales. Mais les exigences auxquelles devront se plier ces fournisseurs, seront moins élevées que celles applicables aux opérateurs de services essentiels.

Publication de la Directive NIS au Journal officiel de l'Union européenne
Adoption de la directive NIS : l'ANSSI, pilote de la transposition en France

---

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 : Directive NIS adoptée: quelles conséquences pour les entreprises?

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 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

---

Cybersécurité et Cyberdéfense : leviers de l’intelligence économique

La transition numérique en Afrique étroitement liée à l’intelligence économique

---

La numérisation de la société africaine s'accélère : la part du numérique dans les services, les produits, les métiers ne cesse de croître. Réussir la transition numérique est devenu un enjeu continental. Vecteur d'innovation et de croissance, la numérisation présente aussi des risques pour l'Etat, les acteurs économiques et les citoyens. La cybercriminalité, l'espionnage, la propagande, le sabotage ou l'exploitation excessive de données personnelles menacent la confiance et la sécurité dans le numérique et appellent une réponse collective.

Le second pilier de l'intelligence économique est par définition la sécurité du patrimoine immatériel. Composante indispensable au développement. Le problème est que ce patrimoine est de plus en plus numérisé en Afrique comme partout dans le monde. A cela il faut rajouter le fait que la technologie est injectée à forte dose dans les entreprises pour améliorer la croissance et la compétitivité. Il y va de même pour les Etats.
Dans ce contexte, l'utilisation, l'accès et l'exploitation de la technologie est en forte croissance. Ce qui a pour implication d'exposer les données stratégiques. Il faut alors disposer de mécanismes efficaces pour protéger ce patrimoine. « La cybersécurité est la prévention des risques de sécurité et de sûreté liés à l'emploi des technologies de l'information. Elle est à ce titre un volet de « l'intelligence des risques » elle-même composante de l'intelligence économique. » Bernard Besson.
De nouveaux crimes, risques, infractions et menaces sont apparus dans le cyberespace africain : utilisations criminelles d'internet (cybercriminalité), espionnage politique, économique et industrielle, attaques contre les infrastructures critiques de la finance, des transports, de l'énergie et des communications à des fins de spéculation, de sabotage et de terrorisme.
Émanant de groupes étatiques ou non-étatiques, les cyberattaques n'ont aucune contrainte de distances, de frontières et même d'espaces ; peuvent être complètement anonymes ; ne nécessitent plus de coûts et de moyens importants et peuvent présenter de très faibles risques pour l'attaquant…[lire la suite]

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.

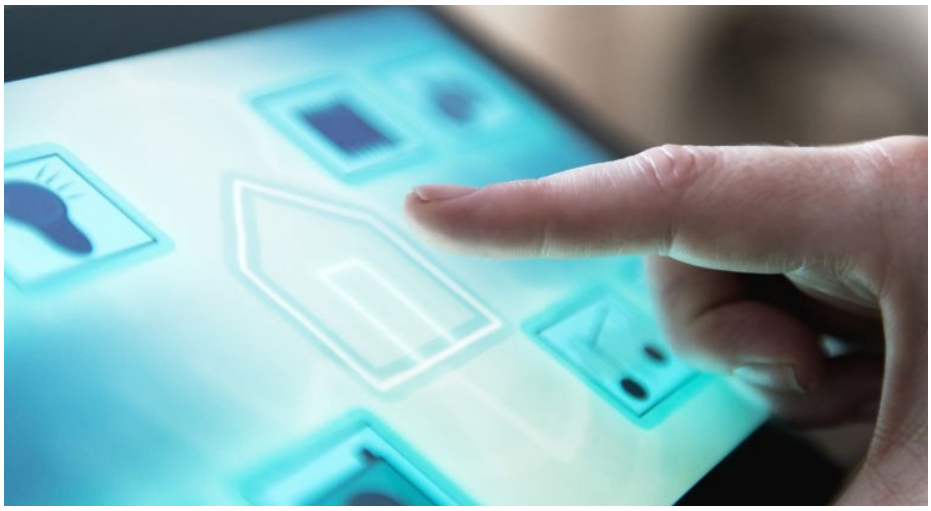
Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Cybersécurité et Cyberdéfense : leviers de l’intelligence économique. »

Jusqu’où les Objets connectés sont les maillons faibles de la cybersécurité ?



Jusqu’où les Objets connectés sont les maillons faibles de la cybersécurité ?

La Chine s'impose parmi les principaux pays créateurs d'objets quotidiens connectés à l'internet, mais elle génère ainsi de gigantesques failles sécuritaires exploitables par des pirates informatiques, a prévenu mardi John McAfee, créateur américain du logiciel antivirus portant son nom.

S'exprimant devant une conférence spécialisée à Pékin, M. McAfee a cité des précédents, dans lesquels des pirates sont parvenus à distance à prendre le contrôle de coffre-forts, de systèmes de chauffage, mais aussi d'ordinateurs de bord d'automobiles ou d'aéroplanes.

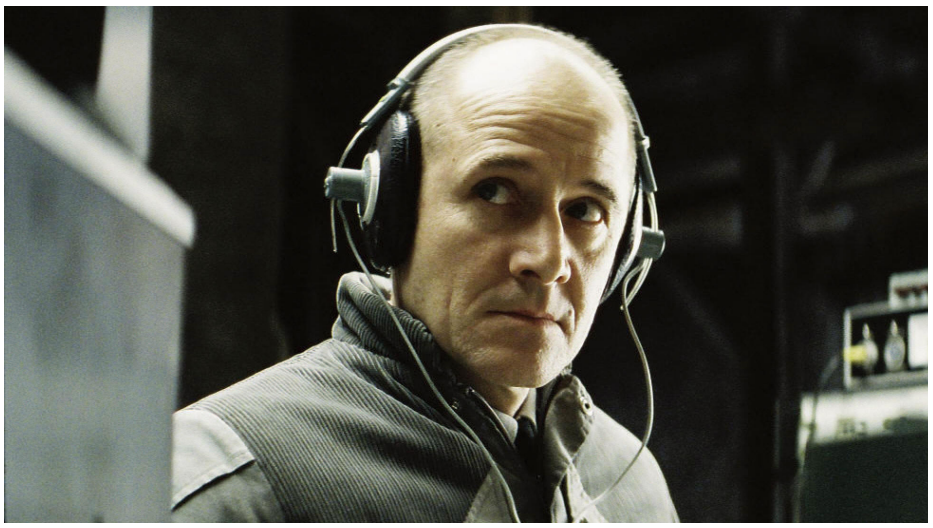
« La Chine prend la tête des progrès sur les objets intelligents, depuis les réfrigérateurs jusqu'aux thermostats, et c'est le maillon faible de la cybersécurité », a-t-il martelé, disant vouloir « lever un drapeau rouge » d'avertissement.
« Il y a tellement plus de ces objets, et plus vous en connectez ensemble, plus les risques de piratage augmentent », a encore souligné John McAfee.
L'excentrique septuagénaire avait fait fortune aux débuts d'internet dans les années 1990, après avoir mis au point un logiciel antivirus qui porte son nom et est maintenant la propriété d'Intel.
Plombé par la crise financière de 2008, il avait défrayé la chronique en 2012 après la mort de son voisin au Belize, pays où il vivait à l'époque et qu'il avait fui après l'ouverture d'une enquête de la police locale.
M. McAfee a livré à Pékin un discours au ton sombre et inquiétant, à l'heure où sa nouvelle société MGT Capital se prépare à lancer de nouveaux produits de cybersécurité d'ici la fin de l'année.
« Notre espèce n'a jamais été confrontée jusqu'ici à une menace de cette ampleur. Et pour l'essentiel, nous n'en prenons pas conscience », a-t-il averti.
« Vous pouvez penser que j'exagère, que je tombe dans l'alarmisme. Mais je compte parmi mes amis beaucoup de +hackers+ (pirates) qui ont les capacités de faire d'énormes dégâts si l'envie leur en prend », a-t-il ajouté.
A l'instar de Xiaomi, fabricant de smartphones ayant élargi son offre dans l'électroménager « intelligent », nombre d'entreprises chinoises intègrent désormais une connexion wi-fi à des produits variés, des autocuiseurs pour riz aux purificateurs d'air, permettant aux usagers de les allumer à distance depuis leur téléphone.
De telles connexions créent de graves failles qui accentuent les vulnérabilités de leurs réseaux, selon John McAfee.
Dans un entretien avec des journalistes à Pékin, l'Américain a cependant noté « n'avoir entendu parler d'aucune » attaque informatique de grande ampleur en Chine sur l'année passée, tandis que les Etats-Unis en enregistraient « des centaines ».

Original de l'article mis en page : Objets connectés : le créateur de l'antivirus McAfee met en garde la Chine contre les failles de sécurité | La Provence

---

Collectes massives et illégales par le

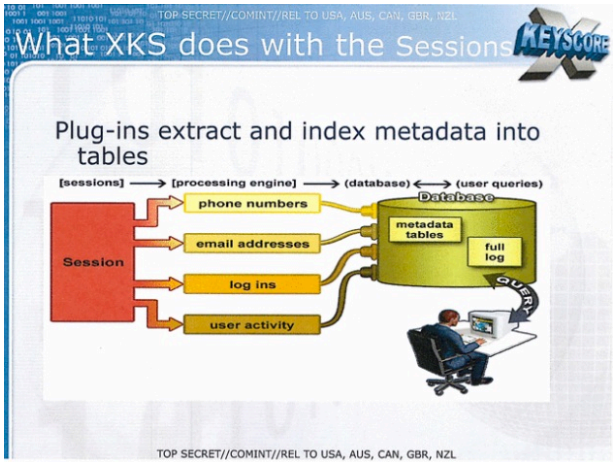
Renseignement allemand



Collectes massives et illégales par le Renseignement allemand

Après avoir réalisé un contrôle sur place des services de renseignement, la Cnil allemande a dressé un bilan extrêmement critique des activités du Bundesnachrichtendienst (BND) en matière de collecte d'informations sur Internet.

Le site Netzpolitik a dévoilé le contenu d'un rapport jusque là confidentiel produit en juillet 2015 par Andrea Voßhoff, le commissaire à la protection des données en Allemagne, qui accable les services de renseignement allemands. Le rapport a été réalisé après la visite de l'homologue de la Cnil dans la station d'écoutes Bad Aibling, opérée conjointement en Bavière par l'agence allemande du renseignement, la Bundesnachrichtendienst (BND), et par la National Security Agency (NSA) américaine.
Malgré les difficultés à enquêter qu'il dénonce, Voßhoff dénombre dans son rapport 18 violations graves de la législation, et formule 12 réclamations formelles, qui obligent l'administration à répondre. Dans un pays encore meurtri par les souvenirs de la Stasi, le constat est violent.
L'institution reproche au BND d'avoir créé sept bases de données rassemblant des informations personnelles sur des suspects ou simples citoyens lambda, sans aucun mandat législatif pour ce faire, et de les avoir utilisées depuis plusieurs années au mépris total des principes de légalité. Le commissaire a exigé que ces bases de données soient détruites et rendues inutilisables.



Parmi elles figure une base assise sur le programme XKeyScore de la NSA, qui permet de réunir et fouiller l'ensemble des informations collectées sur le Web (visibles ou obtenues par interception du trafic), pour les rendre accessibles aux analystes qui veulent tout savoir d'un individu et de ses activités en ligne. Alors que XKeyScore est censé cibler des suspects, Voßhoff note que le programme collecte « un grand nombre de données personnelles de personnes irréprochables », et cite en exemple un cas qu'il a pu consulter, où « pour une personne ciblée, les données personnelles de quinze personnes irréprochables étaient collectées et stockées », sans aucun besoin pour l'enquête…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : Le Renseignement allemand pris en flagrant délit de collectes massives illégales – Politique – Numerama

Ce que Facebook sait (espionne) sur vous

	Ce que Facebook sait (espionne) sur vous

Si vous vous êtes déjà demandé pourquoi Facebook semble connaître une quantité alarmante de chose sur vous; comme tous les sites Web que vous visitez, pour qui vous votez, et quelle quantité vous buvez, voici pourquoi.

Où que vous alliez, quoi que vous fassiez (si c'est en ligne) les chances sont que Mark Zuckerberg vous observe, et apprend.
Facebook recueille des données lorsque vous êtes sur d'autres sites, dans les applications, et dans Facebook lui-même; développant un profil de 98 *« points de données »* sur vous.
Facebook a récemment déployé une mise à jour de son outil Ad Préférences qui révèle un peu plus les données recueillies par Facebook (tout est fait pour vous servir des publicités *« personnalisées »*).
Certaines d'entre elles sont assez alarmantes (comme si vous êtes enceinte, votre race, et votre titre d'emploi) toutes ces données sont récoltées tranquillement, sans avoir un formulaire à remplir.
Voici les 98 *« points de données »* que Facebook sait probablement de vous, où s'il ne les connait pas encore, il essaye de les apprendre, selon le Washington Post.

Qu'est-ce que Facebook sait sur vous

1. L'emplacement
2. L'âge
3. La génération
4. Le sexe
5. La langue
6. Le niveau d'éducation
7. Le domaine d'études
8. L'école
9. L'affinité ethnique
10. Le revenu et la valeur nette
11. La valeur de la propriété et le type
12. La valeur domestique
13. La surface du terrain
14. La superficie de la maison
15. L'année de construction de la maison
16. La composition du ménage
17. Les utilisateurs qui ont un anniversaire dans les 30 jours
18. Les utilisateurs qui sont loin de leur famille ou de leur ville natale
19. Les utilisateurs qui sont amis avec quelqu'un qui a un anniversaire, nouvellement marié ou engagé, récemment déménagé, ou a un anniversaire à venir
20. Les utilisateurs dans les relations à longue distance
21. Les utilisateurs qui ont de nouvelles relations
22. Les utilisateurs qui ont de nouveaux emplois
23. Les utilisateurs qui sont nouvellement engagés
24. Les utilisateurs qui sont nouvellement mariés
25. Les utilisateurs qui ont récemment déménagé
26. Les utilisateurs qui ont des anniversaires bientôt
27. Les parents
28. Les futurs parents
29. Les occupations, rangées par « type » (football, mode, etc.)
30. Les utilisateurs qui sont susceptibles de participer à la politique
31. Les conservateurs et les libéraux
32. La situation amoureuse
33. L'employeur
34. Le travail
35. Les fonctions du travail
36. Les statuts au travail
37. Les loisirs
38. Les utilisateurs qui possèdent des motos
39. Les utilisateurs qui ont l'intention d'acheter une voiture (et quel type / marque de voiture, et dans combien de temps)
40. Les utilisateurs qui ont acheté des pièces ou accessoires automobiles récemment
41. Les utilisateurs qui sont susceptibles d'avoir besoin de pièces ou de services automobiles
42. Le style et la marque de voiture que vous conduisez
43. L'année d'achat de votre voiture
44. L'âge de votre voiture
45. Combien d'argent l'utilisateur est susceptible de dépenser pour la voiture suivante
46. Lorsque l'utilisateur est susceptible d'acheter la voiture suivante
47. Combien d'employés possède votre entreprise
48. Les utilisateurs qui possèdent des petites entreprises
49. Les utilisateurs qui travaillent dans la gestion ou qui sont cadres
50. Les utilisateurs qui ont fait don à la charité (divisés par type)
51. Le système d'exploitation
52. Les utilisateurs qui jouent à des jeux de navigateur
53. Les utilisateurs qui possèdent une console de jeu
54. Les utilisateurs qui ont créé un événement sur Facebook
55. Les utilisateurs qui ont utilisé les paiements Facebook
56. Les utilisateurs qui ont passé plus que la moyenne sur les paiements Facebook
57. Les utilisateurs qui administrent une page Facebook
58. Les utilisateurs qui ont récemment téléchargé des photos sur Facebook
59. Le navigateur Internet
60. Le service de messagerie e-mail
61. Le passage précoce / tardif à la technologie
62. Les expatriés (divisés par le pays d'origine)
63. Les utilisateurs qui appartiennent à une coopérative de crédit, la banque nationale ou banque régionale
64. Les utilisateurs qui sont investisseurs (divisés par type d'investissement)
65. Le nombre de crédits
66. Les utilisateurs qui utilisent des cartes de crédit
67. Le type de carte
68. Les utilisateurs qui ont une carte de débit
69. Les utilisateurs qui effectuent un solde sur leur carte de crédit
70. Les utilisateurs qui écoutent la radio
71. La préférence dans les émissions télévisées
72. Les utilisateurs qui utilisent un appareil mobile (divisé par quelle marque ils utilisent)
73. Le type de connexion Internet
74. Les utilisateurs qui ont récemment fait l'acquisition d'un smartphone ou d'une tablette
75. Les utilisateurs qui accèdent à Internet via un smartphone ou une tablette
76. Les utilisateurs qui utilisent des coupons
77. Les types de vêtements achetés
78. Le temps passé dans les magasins
79. Les utilisateurs qui sont des « gros » acheteurs de bière, de vin ou de spiritueux
80. Les utilisateurs qui achètent dans les épiceries (et quelles types)
81. Les utilisateurs qui achètent des produits de beauté
82. Les utilisateurs qui achètent des médicaments contre les allergies, la toux / médicaments contre le rhume, les produits de soulagement de la douleur
83. Les utilisateurs qui dépensent de l'argent sur les produits ménagers
84. Les utilisateurs qui dépensent de l'argent sur les produits pour les enfants ou les animaux domestiques, et quels types d'animaux de compagnie
85. Les utilisateurs dont les ménages font des achats plus que ce qui est en moyenne
86. Les utilisateurs qui ont tendance à faire des achats en ligne
87. Les types de restaurants
88. Les types de boutiques et magasins
89. Les utilisateurs qui sont « réceptifs » aux offres des compagnies offrant des assurances auto en ligne, l'éducation ou des prêts hypothécaires plus élevés, les cartes prépayées / la TV par satellite
90. La durée du temps passé dans une maison
91. Les utilisateurs qui sont susceptibles de se déplacer rapidement
92. Les utilisateurs qui sont intéressés par les Jeux Olympiques, le football, le cricket ou le Ramadan
93. Les utilisateurs qui voyagent fréquemment, pour le travail ou pour le plaisir
94. Les utilisateurs qui font la navette jusqu'au travail
95. Les types de vacances d'un utilisateur
96. Les utilisateurs qui sont récemment revenus d'un voyage
97. Les utilisateurs qui ont récemment utilisé une application de voyage
98. Les utilisateurs qui participent à une multipropriété

Source : **Metro.co.uk**

Réagissez à cet article

Original de l’article mis en page : Voici 98 choses que Facebook sait sur vous

---

Retrouver l’auteur d’un E-mail à partir de l’adresse IP : Le demandeur condamné

Retrouver l’auteur d’un E-mail à partir de l’adresse IP : Le demandeur condamné

Le TGI de Meaux a débouté l'entreprise qui voulait obtenir de Numericable les noms, prénoms, adresses et coordonnées complètes de l'auteur d'un email frauduleux à partir de son adresse IP.

Dans une ordonnance de référé du 10 août 2016 repérée par Legalis, le tribunal de grande instance de Meaux (Seine-et-Marne) a débouté l'entreprise qui voulait obtenir de Numericable les données d'identification correspondant à l'adresse IP de l'auteur présumé d'un email frauduleux.
Comment en est-on arrivé là ? En début d'année, la société France Sécurité a préparé une proposition commerciale à l'attention d'Airbus Helicopters dans le cadre d'un appel d'offres. Dans la foulée, le distributeur d'équipements de protection individuelle a reçu un courriel d'un individu se faisant passer pour un employé d'Airbus et lui demandant de transmettre par courriel le fichier contenant la proposition… Suspectant la fraude, France Sécurité a contacté Airbus. Le nom associé au courriel était bien celui d'un de ses employés, mais il n'était pas l'auteur des courriels en question.

Usurpation d'identité
Dans un premier temps, une plainte a été déposée contre X pour usurpation d'identité. Parallèlement, le département informatique de France Sécurité a identifié l'adresse IP de l'expéditeur du courriel (transmis via Gmail) ainsi que le FAI hôte, à savoir : Numericable. Un procès-verbal de constat d'huissier a été établi. Ensuite, le 28 juin 2016, France Sécurité a déposé plainte auprès du procureur de la République près le tribunal de grande instance de Nantes. Et le 8 juillet 2016, l'entreprise a fait assigner devant le juge des référés du TGI de Meaux le câblo-opérateur. Le but : obtenir du tribunal qu'il ordonne au FAI de communiquer dans un délai de 48 heures les données d'identification correspondant à l'adresse IP en cause. Car, selon le demandeur, le câblo-opérateur est tenu de conserver les données permettant l'identification de son client et de déférer aux demandes de l'autorité judiciaire. Et ce en application de la loi pour la confiance dans l'économie numérique (LCEN) du 21 juin 2004. France Sécurité souhaitait également qu'une astreinte soit versée par Numericable en cas de dépassement de ce délai, en plus des frais irrépétibles… Sans succès.

L'adresse IP, une donnée personnelle
Le juge est parti du principe que l'adresse IP est une donnée à caractère personnel. Par ailleurs, il a considéré que la collecte de cette donnée constitue un traitement au sens de la loi informatique et libertés. Une telle collecte aurait donc dû faire l'objet d'une autorisation de la Commission nationale informatique et libertés (Cnil) accordée à France Sécurité. Cela n'a pas été le cas. Par ailleurs, le juge considère que le cadre juridique applicable dans ce dossier ne peut pas être celui de la LCEN de 2004. Selon lui, Numericable n'est pas visé en tant que « personne dont l'activité est d'offrir un accès à des services de communication au public » en relation avec « la création d'un contenu » en ligne.
Résultat : le TGI de Meaux a débouté France Sécurité de toutes ses demandes. L'entreprise a été condamnée aux entiers dépens et au versement de 2 000 euros au titre des frais irrépétibles…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : IP : Numericable n’a pas à communiquer les données d’identification