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~~
n° NOR MCCA614354C

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 ».

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

Données personnelles : le « Privacy Shield » dans la dernière ligne droite

Données personnelles : le « Privacy Shield » dans la dernière ligne droite

Le Privacy Shield (« bouclier de protection des données personnelles »), un accord politique censé encadrer l'utilisation des données personnelles des citoyens Européens par les entreprises sur le sol américain, a été validé par les Etats membres, vendredi 8 juillet.

Pour la première fois, les Etats-Unis ont donné à l'Union européenne l'assurance écrite que l'accès des autorités aux données personnelles serait soumis à des limitations claires, des garde-fous et des mécanismes de contrôle, tout en écartant la surveillance de masse indiscriminée des données des Européens » s'est réjoui la commission dans un communiqué.

Le Privacy Shield est censé remplacer le Safe Harbor, un accord similaire qui a été invalidé par la Cour de justice de l'Union européenne (CJUE), qui a notamment cité le peu de cas que faisaient les agences de renseignement américaines des données personnelles des citoyens européens stockées sur le sol américain.
Les entreprises du numérique, placées dans une situation juridiquement inconfortable depuis l'annulation du Safe Harbor, ont salué cette étape supplémentaire sur le chemin de l'adoption définitive. « Même si les négociations n'ont pas été faciles, nous félicitons la commission et le ministère du commerce américain pour leur travail de restauration de la confiance dans les transferts des données entre l'UE et les Etats-Unis », a dit John Higgins, le directeur général de DigitalEurope, un lobby rassemblant notamment Google, Apple, Microsoft et IBM, qui dit aussi espérer que grâce au Privacy Shield « l'Europe puisse à nouveau se concentrer sur la manière dont les flux de données peuvent jouer un rôle dans la croissance économique ».

DE NOMBREUX OBSTACLES DEMEURENT

L'accord, entre la commission et les Etats-Unis, doit encore être validé par le collège des commissaires européens, avant son adoption définitive qui devrait intervenir le 12 juillet prochain, après des mois d'âpres négociations. Ce n'est pas la fin du débat autour de cet accord contesté.
L'accord n'a pas fait consensus auprès des Etats membres, les diplomates représentant plusieurs pays – l'Autriche, la Slovénie, la Bulgarie et la Croatie, selon l'agence Reuters – se sont abstenus. Un moyen d'« exprimer leur méfiance vis-à-vis du texte » anticipait, jeudi lors d'une conférence, David Martinon, ambassadeur français pour la cyberdiplomatie et l'économie numérique, cité par le site Silicon.fr.
Par ailleurs, cet accord, sera très certainement contesté devant les tribunaux après son adoption. Max Schrems, l'Autrichien tombeur du prédécesseur du Privacy Shield, pourrait attaquer l'accord devant les juridictions européennes.
Dans le même ton, La Quadrature du Net, association française de défense des libertés numériques, a dénoncé un accord qui « ne présente pas les garanties suffisantes pour la protection de la vie privée des Européens. Il passe sciemment à côté du cœur de l'arrêt de la CJUE invalidant le Safe Harbor : la surveillance massive exercée via les collectes de données des utilisateurs. »
Article original de Martin Untinsinger

Réagissez à cet article

Original de l’article mis en page : Données personnelles : le « Privacy Shield » dans la dernière ligne droite

---

L’accord entre l’Europe et les Etats-Unis sur les données personnelles sur le point d’être adopté

L’accord entre l’Europe et les Etats-Unis sur les données personnelles sur le point d’être adopté

Les Etats membres de lUE ont donné leur feu vert au «Privacy Shield», qui vient remplacer laccord «Safe Harbor» invalidé en octobre par la justice européenne.

Le «Privacy Shield» est sur la rampe de lancement. La Commission européenne l'a annoncé ce vendredi matin : le nouvel accord-cadre sur les transferts de données personnelles depuis le Vieux Continent vers les Etats-Unis a reçu le feu vert des Etats membres de l'Union, moins quatre abstentions (l'Autriche, la Slovénie, la Bulgarie et la Croatie, selon l'agence Reuters). Il devrait être adopté formellement par la Commission mardi prochain. Ce «bouclier de confidentialité» vient ainsi succéder à l'accord dit «Safe Harbor» (ou «sphère de sécurité»), invalidé il y a neuf mois par la justice européenne.

Deux ans de négociation

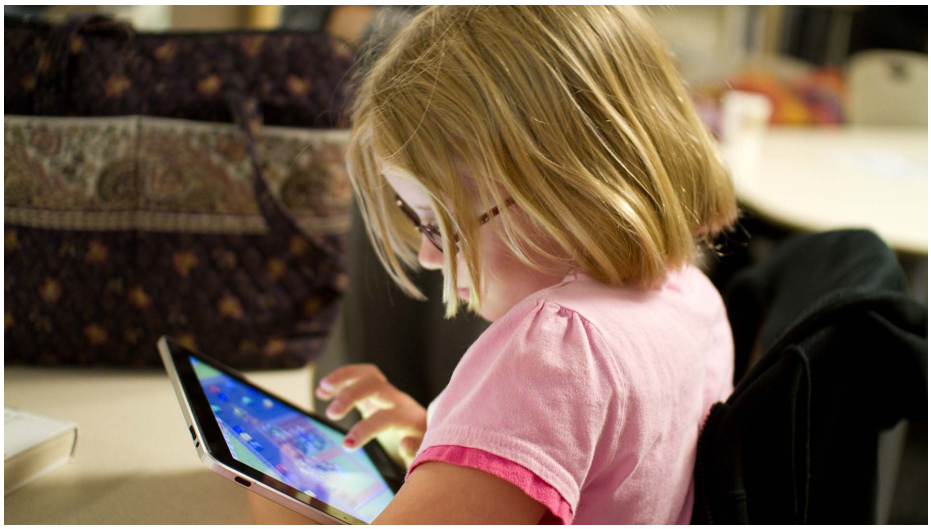
Mis en place en 2000, le Safe Harbor était censé garantir aux citoyens européens un niveau de protection suffisant de leurs données personnelles transférées sur le sol américain : les entreprises qui y adhéraient s'engageaient à respecter les normes de l'UE en la matière… via une certification annuelle qu'elles pouvaient s'autodécerner. Une «garantie» minimale qui a volé en éclats en 2013 avec les révélations d'Edward Snowden sur les pratiques de surveillance massive de la NSA, et notamment le programme Prism, qui permet à l'agence américaine d'accéder aux données stockées par les géants du Net.
Article original de Amaelle Guiton
Photo Dado Ruvic. Reuters

Réagissez à cet article

Original de l’article mis en page : Données personnelles : laccord entre lEurope et les Etats-Unis sur le point dêtre adopté – Libération

---

Attention aux ondes des tablettes et smartphones pour les enfants !



Attention aux ondes des tablettes et smartphones pour les enfants !

Un rapport publié par l'agence de la sécurité sanitaire met en garde les parents sur l'exposition des enfants aux ondes. Elle recommande un usage modéré et encadré des technologies sans fil. Elle suggère aussi une révision de la réglementation.

Attention aux technologies sans fil ! Telle est la mise en garde que vient de formuler l'agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail (Anses) ce vendredi, dans un rapport portant sur le sujet hautement sensible de l'exposition aux radiofréquences et à la santé des enfants. Dans celui-ci, elle note « des effets possibles sur les fonctions cognitives et le bien-être » et recommande de limiter et d'encadrer l'usage de ces technologies.

Dans le cadre de ce travail, ce sont les enfants de moins de six ans qui ont fait l'objet d'un suivi particulier. L'Anses avait été saisie par les pouvoirs publics afin de vérifier si les dispositions réglementaires à propos des appareils radioélectriques destinés aux plus jeunes sont suffisamment protectrices en matière de santé et de sécurité. Il ressort que « les enfants pouvaient être plus exposés que les adultes » du fait de leurs spécificités morphologiques et anatomiques.

C'est ce que détaille à France Info Olivier Merckel, chargé de l'évaluation des risques. « Les enfants sont plus exposés que les adultes aux champs électromagnétiques : l'épaisseur du crâne chez les enfants est plus petite que chez les adultes donc on a une exposition globale plus importante ». En outre, les « caractéristiques de certains de leurs tissus » contribuent à cette vulnérabilité accrue. Il faut donc redoubler de vigilance quant à l'exposition des petits.
Le problème, c'est la généralisation des équipements de transmissions sans fil dans leur environnement. « Les données disponibles sur l'exposition montrent une forte expansion de l'usage des nouvelles technologies sans-fil, notamment chez les très jeunes enfants », relève le rapport. Il y a le smartphone, il y a la tablette, il y a les objets connectés, il y a le babyphone, il y a les jouets radiocommandés… et beaucoup d'autres appareils dédiés à la surveillance du petit ou à l'occuper.

LES ENFANTS SONT PLUS EXPOSÉS QUE LES ADULTES
Or, on le devine aisément : plus la source émettrice est proche, plus l'intensité et la quantité du rayonnement sont élevées. En la matière, des appareils comme des smartphones ou des babyphones peuvent légitimement constituer une source d'inquiétude, car ils sont en général très près de la tête – que ce soit pour parler au téléphone ou bien pour entendre les bruits de bébé et s'assurer que tout va bien.

QUELS EFFETS POTENTIELS ?
L'Anses souligne toutefois que « les données actuelles ne permettent pas de conclure à l'existence ou non d'un effet des radiofréquences chez l'enfant sur le comportement, les fonctions auditives, les effets tératogènes et le développement, le système reproducteur, les effets cancérogènes, le système immunitaire, la toxicité systémique ». Des études plus approfondies seront sans doute nécessaires.
L'Anses mentionne toutefois deux cas où à un effet des radiofréquences est possible : les fonctions cognitives d'abord. « Les résultats montrant des effets aigus se basent sur des études expérimentales dont la méthodologie est bien maîtrisée », note le rapport. Un effet négatif sur le bien-être peut aussi être envisagé, même s'il « pourrait cependant être lié à l'usage du téléphone mobile plutôt qu'aux radiofréquences qu'ils émettent ». Bref ce serait plus ce serait la manière dont on s'en sert le problème.

UN USAGE RAISONNABLE
Est-ce que cela veut dire qu'il faut tenir les enfants loin de ces sources d'émission ? En clair, faut-il les priver de portable jusqu'à un âge avancé, retirer les jouets high tech et vérifier que la chambre n'est pas trop exposée ? Pour Olivier Merckel, il faut prendre quelques mesures, mais ne pas non plus exagérer. Les jeunes de moins de 13 ans peuvent passer « quelques appels, quelques SMS par jour » mais « certainement pas plusieurs heures ».
Un usage maitrisé. Tel est donc le conseil général donné par l'Anses à l'attention des parents. « L'Agence recommande aux parents d'inciter leurs enfants à un usage raisonnable du téléphone mobile, en évitant les communications nocturnes et en limitant la fréquence et la durée des appels ». Mais des actions doivent aussi être engagées du côté des pouvoirs publics, au niveau français ou européen.

UNE RÉGLEMENTATION À REVOIR
Pour l'Anses, il convient d'actionner plusieurs leviers, à commencer par l'obligation de soumettre l'ensemble des dispositifs radioélectriques, et notamment ceux destinés aux enfants, « aux mêmes obligations réglementaires en matière de contrôle des niveaux d'exposition et d'information du public que celles encadrant les téléphones mobiles ». L'agence demande aussi de reconsidérer les niveaux de référence visant à limiter l'exposition environnementale.
Les pouvoirs publics doivent également « réévaluer la pertinence du débit d'absorption spécifique (DAS) ». Il s'agit d'un indicateur utilisé pour l'établissement des valeurs limites d'exposition des personnes, à des fins de protection contre les effets sanitaires connus et avérés (effets thermiques) des radiofréquences. Il convient également de « développer un indicateur représentatif de l'exposition réelle des utilisateurs de téléphones mobiles », « quelles que soient les conditions d'utilisation ».

UN DÉBAT PERMANENT
La question des ondes et de leurs effets potentiels sur la santé a donné lieu à une littérature scientifique abondante. L'Anses elle-même publiait déjà en octobre 2013 un avis dans lequel elle notait à l'absence d'effets avérés sur la santé mais suggérait quand même de prendre des mesures de précaution, en particulier du côté des enfants et des utilisateurs intensifs. La publication avait toutefois fait l'objet de critiques dans la société civile, au sein d'associations spécialisées.
Deux ans auparavant, le centre international de recherche sur le cancer déclarait que les champs électromagnétiques de radiofréquence sont peut-être cancérogènes. Mais là encore, les conclusions avaient été discutées. Ainsi, des organisations professionnelles avaient estimé que le risque soulevé par les experts n'avait pas été clairement démontré par un lien évident de cause à effet et, que de ce fait, la poursuite des travaux scientifiques est indispensable.
Article original de Julien Lausson

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 : Ondes : les enfants doivent moins utiliser les tablettes et smartphones

---

Peut-on communiquer les données personnelles du défunt à ses ayants droit ?

Peut-on communiquer les données personnelles du défunt à ses ayants droit ?

Toute personne physique justifiant de son identité a le droit dobtenir la communication des données personnelles qui la concernent. En revanche, est exclue la communication de ces données aux ayants droit qui ne sauraient être regardés comme des « personnes concernées ».

Mme et MM. D., ayants droit de Mme E. D., décédée le 2 août 2012, ont demandé à la Banque de France, dernier employeur de la défunte, la communication du relevé des derniers appels téléphonique qu'elle avait passé avec le corps médical avant son décès.
Après le refus de la Banque de France, ils ont déposé une plainte le 1er février 2013 auprès de la Cnil.
La Cnil ayant confirmé le refus de la Banque de France dans une décision du 29 mai 2013, ils saisissent le tribunal administratif de Paris qui, par un jugement du 9 décembre 2014, a directement transmis cette requête au Conseil d'Etat.

Le Conseil d'Etat se prononce dans un arrêt du 8 juin 2016.
Il rappelle qu'aux termes du dernier alinéa de l'article 2 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, « la personne concernée par un traitement de données à caractère personnel est celle à laquelle se rapportent les données qui font l'objet du traitement ».
En outre, aux termes de l'article 39 de cette même loi, « toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel en vue d'obtenir (…) la communication, sous une forme accessible, des données à caractère personnel qui la concernent (…) ».
Ainsi, il résulte de ces dispositions qu'elles ne prévoient la communication des données à caractère personnel qu'à la personne concernée par ces données. C'est donc à bon droit que la présidente de la Cnil a pris la décision attaquée à l'égard de Mme et MM. D., qui ne pouvaient, en leur seule qualité d'ayants droit, être regardés comme des « personnes concernées ».
Article original de Céline Solomides

Réagissez à cet article

Original de l'article mis en page : Impossibilité de communiquer les données personnelles du défunt à ses ayants droit

Les magistrats du palais de justice de Ouagadougou outillés pour combattre la cybercriminalité

	Les magistrats du palais de justice de Ouagadougou outillés pour combattre la cybercriminalité

La Commission de l'Informatique et des Libertés (CIL) en partenariat avec les tribunaux du palais de justice de Ouagadougou, organise un séminaire de sensibilisation des magistrats et greffiers du palais de justice de Ouagadougou aux « enjeux de la protection des données personnelles et de la vie privée des citoyens à l'ère du numérique ». Ce séminaire se déroule à Ouagadougou ce mardi 28 juin 2016.

« Aucune personne n'est, de nos jours, à l'abri des actes cybercriminels, quel que soit son statut, son rang ou l'état de ses connaissances », a lancé Marguerite Ouédraogo/Bonané, présidente de la CIL. Si de nos jours la cybercriminalité avance à grand pas dans le monde entier, force est de constater que les initiatives pour l'affronter ne manquent pas. La lutte contre cette nouvelle forme de criminalité impose donc que de « nouvelles approches soient développées et que toutes ses dimensions soient maitrisées », a-t-elle reconnu. Dans l'optique de protéger les données des justiciables en justice, la CIL entend informer et sensibiliser les magistrats aux droits des personnes dont les données sont utilisées. « Notre mission aujourd'hui c'est de les informer et de les sensibiliser aux droits des personnes dont les données sont utilisées », a confié marguerite Ouédraogo/Bonané. A l'en croire, la protection des données couvre tout le territoire. Par conséquent, tous les Burkinabé sont concernés par cette protection. Elle révèle que ce séminaire ouvert aux magistrats permettra à ces derniers de protéger les données des justiciables comme le stipule « notre loi ».

Des communications qui seront faites dans ce séminaire

Plusieurs communications seront faites durant ce séminaire. En substance, une communication sera faite à l'intention des magistrats pour leur faire connaitre le cadre juridique et institutionnel des données personnelles au Burkina Faso. Une autre sera de leur faire connaitre la communication sur l'enquête judiciaire et la protection des données personnelles face à l'enquête judiciaire. Aussi, la formation sur l'utilisation de l'internet et des réseaux sociaux leur sera-t-elle donnée.

Vu l'importance de ce séminaire qui est focalisé sur les acteurs de la justice, Dieudonné Manly, Conseiller Technique du ministère de la justice, accorde un peu plus de crédit à l'ordre du jour quand il affirme qu' « aujourd'hui la cybercriminalité a pris de l'ampleur et il va falloir outiller les magistrats afin qu'ils puissent faire face à ce phénomène ». Aussi, pense-t-il que les thèmes choisis sont bien réfléchis et que ces thèmes vont, à son avis, « permettre aux magistrats de faire face à la cybercriminalité ».

Article original de Armand Kinda

Réagissez à cet article

Original de l’article mis en page : Lutte contre la cybercriminalité : les magistrats du palais de justice de Ouagadougou outillés pour en faire face

---

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

---

Réagissez à cet article

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

---

Inquiétantes intrusions dans les réseaux d’entreprises

Inquiétantes intrusions dans les réseaux d’entreprises

Les intrusions dans les réseaux informatiques des entreprises se sont multipliées en France ces derniers mois et labsence de vols de données laisse craindre des tentatives de sabotages ou dattaques terroristes, a déclaré lundi le directeur général de lAgence nationale de la sécurité des systèmes dinformation (Anssi).

Le Secrétariat général de la défense et la sécurité nationale (SGDSN) et l'Anssi, deux services rattachés à Matignon, ont présenté lundi les trois premiers arrêtés liés à la protection des opérateurs d'importance vitale dans la santé, la gestion de l'eau et l'alimentation, qui entreront en vigueur le 1er juillet.
« Il y a de plus en plus d'attaquants, ce sont des agents dormants qui préparent les choses », a expliqué Guillaume Poupard à des journalistes. « Il y a eu beaucoup de cas à traiter ces derniers mois ».
Ces intrusions, par exemple par le biais d'emails piégés envoyés dans les entreprises, permettent aux attaquants de cartographier un réseau en toute discrétion et, en passant d'un réseau à l'autre, de pénétrer dans des zones inattendues.
« Ils prennent pied progressivement (..) et on les retrouve très profond au sein des réseaux d'entreprises, à des endroits où il n'y a même plus d'informations secrètes à voler, par exemple sur les systèmes de production de contrôle qualité », a ajouté Guillaume Poupard.
Ce nouveau type d'intrusion est d'autant plus inquiétant qu'il est presque plus facile d'entrer dans un réseau pour en modifier le fonctionnement ou en prendre le contrôle que pour voler des données, a-t-il souligné.
Au contraire de la banque, de l'aérospatiale et de l'automobile, habitués à surveiller de près leurs réseaux, l'industrie est encore mal préparée, étant moins sujette aux vols de données, a noté Guillaume Poupard.
« L'idée que des gens qui depuis l'autre bout du monde puissent chercher à détruire leur système de production c'est un nouveau scénario qui n'a pas vraiment d'équivalent dans le monde réel », a-t-il souligné.
Pour mieux défendre les PME, « un des maillons faibles », cible rêvée d'un attaquant, il prône le recours aux solutions de « cloud computing » des spécialistes de la sécurité numérique et à l'intégration de systèmes de protection dans les machines outils et les automates industriels dès leur conception. (Cyril Altmeyer, édité par Jean-Michel Bélot)

Réagissez à cet article

Original de l’article mis en page : SAFRAN : France : Inquiétantes intrusions dans les réseaux dentreprises

L’Etat français (ANSSI) va certifier les Cloud de confiance

L’Etat français (ANSSI) va certifier les Cloud de confiance

L'Agence nationale pour la sécurité des systèmes d'information (Anssi) s'apprête à certifier les Cloud de quelques prestataires. Deux niveaux de labellisation sont attendus.

L'Agence nationale pour la sécurité des systèmes d'information (Anssi), dépendant du Premier ministre, est engagée dans un processus qui aboutira à la qualification des fournisseurs de Cloud. Les prestataires présentant le niveau de sécurité requis recevront donc un label de l'Agence, qui permettra aux entreprises et administrations de recourir à leurs services en se basant sur les garanties fournies par l'Etat français. « *Huit prestataires se sont lancés dans ce processus de qualification* », assure Guillaume Poupard, le directeur général de l'Anssi, qui a appelé les grands acteurs du Cloud américains à rejoindre le mouvement. « *La qualification n'est pas un outil de protectionnisme* », reprend Guillaume Poupart. Selon lui, les AWS et autre Microsoft (pour Azure) sont en train d'étudier une éventuelle qualification. Façon de dire aussi qu'il n'est pas acquis qu'ils se soumettent un jour aux exigences de l'Anssi.
Notons que, sur ce dossier, l'Anssi travaille en coordination avec ses homologues allemands du BSI (l'Office fédéral de la sécurité des technologies de l'information) : un prestataire homologué outre-Rhin recevra automatiquement son label dans l'Hexagone et vice-versa.

Deux niveaux : Cloud Secure et Cloud Secure +

Ce label étatique fait suite à une démarche entamée dès la mi-2014. A cette époque, l'Anssi avait publié un premier référentiel et appelé les entreprises à le commenter. Un grand nombre de commentaires, parfois critiques, avaient été remontés à l'Agence. Depuis, cette dernière a réuni un comité restreint pour travailler à une seconde version du référentiel, largement inspiré de la norme ISO 27 001.

Guillaume Poupard, directeur général de l'Anssi.

En réalité, la démarche doit accoucher de deux niveaux de qualification : Cloud Secure et Cloud Secure +. Dans la première, selon des déclarations publiques d'un membre de l'Anssi en octobre dernier, on retrouve des bonnes pratiques assez classiques : contrôles d'accès physiques, authentification forte avec mots de passe hachés et salés, chiffrement logiciel et hébergement des données en Europe. Le niveau le plus élevé ira plus loin, imposant une authentification multi-facteurs, un chiffrement matériel (via HSM) ou encore un hébergement en France. Parmi les acteurs figurant dans la liste des premiers prestataires certifiés, on devrait retrouver Thales, Orange ou Oodrive, qui se présentait en octobre dernier comme l'acteur pilote de la qualification Secure Cloud +. Notons qu'à l'époque, l'Anssi indiquait que les OIV – les quelque 250 organisations identifiées comme essentielles au fonctionnement de la nation – pourraient se voir imposer le recours à des prestataires certifiés Secure Cloud +. Les premiers arrêtés encadrant les politiques de sécurité des OIV n'y font toutefois pas référence à ce jour.

Cloud Secure + : les Américains out ?

« *Nous nous sommes engagés à nous conformer à cette norme auprès de certains clients* », explique Laurent Seror, le président d'Outscale, le fournisseur de Iaas né sous l'impulsion de Dassault Systèmes. « *Etant donné que nous sommes déjà certifiés ISO 27 001, je considère que nous sommes prêts. Ne pas être certifié juste au moment de la sortie du référentiel ne sera pas pénalisant compte tenu de la longueur des cycles de décision* », ajoute Laurent Seror. Ce dernier relève toutefois que, par construction, le niveau Cloud Secure + restera difficile à atteindre pour les grands prestataires américains. D'abord parce qu'ils ne possèdent pas, à ce jour, de datacenter en France (à l'exception de Salesforce). Mais, au-delà de ce seul élément, d'autres questions se posent. Selon lui, chez AWS, un administrateur américain, donc soumis au Patriot Act, peut accéder à toutes les machines virtuelles, quelle que soit la zone où ces dernières sont hébergées. « *On en est sûr à 99% en raison de la nature d'une fonction qu'ils proposent pour la migration entre deux régions géographiques. Celle-ci suppose l'existence d'un réseau à plat entre toutes les plates-formes.* »
La question de la localisation des données reste un élément central de la politique de certains pays européens souhaitant reconquérir leur souveraineté dans le Cloud. Lors du débat au Sénat sur le projet de loi pour une République numérique (porté par Axelle Lemaire), un amendement, déposé par les sénateurs du groupe communiste et prévoyant d'obliger les entreprises à stocker les données personnelles des citoyens français sur le territoire européen, a été voté. « *Cet amendement n'était pas téléguidé*, assure aujourd'hui Guillaume Poupard. *Je l'ai découvert au moment des débats.* » Le 29 juin, une commission mixte paritaire doit harmoniser les versions de ce projet de loi sorties respectivement des débats à l'Assemblée et au Sénat. Rien ne permet d'affirmer que ledit amendement, absent de la version votée par le Palais Bourbon, soit présent dans la mouture finale du texte de loi.
Article original de Reynald Fléchaux

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 du 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 : L'Etat français va certifier les Cloud de confiance

---

Cybercriminalité : « Il faut qu'on voie que la Côte d'Ivoire réagit » | CIO MAG

Cybercriminalité : « Il faut qu'on voie que la Côte d'Ivoire réagit »

« L'enjeu qu'a la Côte d'Ivoire aujourd'hui, c'est justement de dire de manière internationale tout ce qu'elle est en train de mettre en œuvre ici », assure Denis Jacopini, expert informatique assermenté spécialiste en cybercriminalité et protection des données personnelles. Membre de la Compagnie nationale française des experts de Justice en Informatique et techniques associées (CNEJITA), il a participé du 7 au 8 juin 2016 à Abidjan, à la 8ème édition de l'IT Forum Côte d'Ivoire sur la « Transformation numérique face à la protection des utilisateurs ». Loin des clichés et des idées reçues, le professionnel du crime en ligne a confié à CIO Mag l'image que la Côte d'Ivoire donne de l'extérieur et fait des propositions allant dans le sens de l'amélioration de la lutte contre la cybercriminalité. Sensibilisation des décideurs, opérations coup de poing, médiatisation des arrestations… la Côte d'Ivoire est, selon lui, en bonne voie pour renforcer la confiance dans son environnement numérique.

7 juin 2016. Denis Jacopini à la 8ème édition de l'IT Forum Côte d'Ivoire qui s'est déroulée du 7 au 8 juin dernier à la Maison de l'Entreprise, à Abidjan, sur le thème : « Transformation numérique face à la protection des utilisateurs ».

CIO Mag : Quelle image la Côte d'Ivoire donne-t-elle de l'extérieur dans le domaine de la cybercriminalité ?
Denis Jacopini : Depuis quelques années, la Côte d'Ivoire est connue en Europe comme le pays d'Afrique où se passent la très grande majorité des arnaques sur internet, à un point où lorsque quelqu'un reçoit un email qui vient de Côte d'Ivoire, il pense automatiquement à une arnaque, au mieux se méfie, au pire supprime le message sans même lui accorder la moindre attention. Ainsi, associer la Côte d'Ivoire à des arnaqueurs, n'est pas bon pour l'image du pays. Ceci dit, ma présence ici m'a réconforté.
En lisant la presse spécialisée, dont CIO Mag, je savais déjà que la Côte d'Ivoire réagissait face à ce phénomène, qu'elle mettait en place des méthodes et qu'elle engageait des actions pour permettre à la fois aux directeurs de systèmes d'information – DSI – et aux utilisateurs d'augmenter en compétence et de se soucier de ce problème de sécurité. Et, en venant ici, ça m'a réconforté. Je m'en suis surtout rendu compte au travers du discours du ministre de l'Economie numérique et de la Poste (à l'ouverture de la 8ème édition de l'IT Forum Côte d'Ivoire, NDLR). Il a fait une présentation de la manière dont il voit l'évolution de la Côte d'Ivoire dans le domaine du numérique. Son discours a été rassurant en indiquant que le pays avait à la fois une démarche active dans la cybersécurité et accordait une attention particulière aux moyens permettant d'associer confiance et développement numérique.
On a facilement pu remarquer que le ministre maîtrise le sujet et qu'il sait de quoi il parle. Il est prêt à emmener avec lui le pays dans cette transformation numérique. Quasiment toutes les entreprises vont devoir assurer cette métamorphose. Le pays doit pouvoir les accompagner dans cette transformation numérique. L'enjeu qu'a la Côte d'Ivoire aujourd'hui, c'est justement de dire de manière internationale tout ce qu'elle est en train de mettre en œuvre ici.

C.M : Selon vous quels sont les actions sur lesquelles la Côte d'Ivoire doit miser pour véritablement restaurer son image et créer un environnement numérique de confiance ?
D.J : A mon avis, ça devrait passer par une médiatisation des arrestations. Il y a des milliers de délinquants ayant organisé et mené des arnaques en tous genres à partir de cybercafés. On apprend de temps en temps sur la presse francophone spécialisée que se sont produites des arrestations mais ça reste sur les journaux peux lus. Il faut vraiment s'intéresser à la Côte d'Ivoire et consulter la presse locale pour le savoir. A mon avis, les actions qui sont faites dans le pays mais aussi tous les accords et toutes les coopérations qui sont établis avec les autres pays doivent internationalement être connues et notamment par le grand public qui a besoin d'être rassuré car régulièrement victime d'actes originaires d'ici.
Lorsqu'il y a une coopération qui est mise en place avec l'ANSSI (l'Agence nationale de la sécurité des systèmes d'information, NDLR) en France, avec l'OCLCTIC, l'Office centrale de lutte contre la criminalité liée aux technologies de l'information et de la communication, en termes de formation et de sensibilisation en Côte d'Ivoire, il faut que cela se sache. Il faut qu'on voie que la Côte d'Ivoire réagit que les autorités se forment, sont en train de monter en compétence. Maintenant, ce qui manque, ce sont les preuves. Mais les preuves, ce sont effectivement les statistiques pouvant faire mention de l'évolution du nombre d'arrestations que j'espère suivies d'une chute considérable des arnaques qui pourraient venir rassurer les pays victimes. Il y aura toujours des arnaques, mais celles venant de Côte d'Ivoire doivent être combattues sans cesse pour finir par les rendre anecdotiques.

C.M : Hormis les arrestations, une forte sensibilisation de la jeunesse ivoirienne ne peut-elle pas également contribuer à réduire le nombre d'arnaques venant de la Côte d'Ivoire ?
D.J : D'après ce que j'ai compris, les adolescents ou les jeunes qui sont concernés sont des personnes qui, dans la société, sont déjà en marge des règles. Ils essaient de se débrouiller par leurs propres moyens sans passer par la case Travail, la case Honnêteté. C'est tout aussi grave que de se rapprocher de la drogue. Que fait le pays contre la drogue ? Ce qu'elle fait contre ce fléau, elle doit aussi le faire pour combattre la cybercriminalité. Comme dans d'autres régions du monde, s'attaquer à ce phénomène doit se faire en s'appuyant sur des entraides internationales.
« CE QUI MANQUE MAINTENANT CE SONT LES MOYENS POUR LES POUVOIRS PUBLICS DE MENER DES OPÉRATIONS COUP DE POING. GRÂCE À CELA, IL EST PROBABLE QUE LES JEUNES POUVANT ENCORE CHANGER DE VOIE, LE FERONT PAR PEUR.»
L'analyse des flux financiers au travers de réseaux et des trains de vie incohérents avec les revenus connus sont de bonnes pistes à suivre pour comprendre le phénomène de la cybercriminalité. Ce qui manque maintenant ce sont les moyens pour les pouvoirs publics de mener des opérations coup de poing. Grâce à cela, il est probable que les jeunes pouvant encore changer de voie, le feront par peur. Ensuite, pour ceux qui, influencés, n'auront pas envie de rentrer dans le droit chemin, je pense en effet qu'une une forte sensibilisation pourra évidemment contribuer à réduire le nombre d'arnaques venant de Côte d'Ivoire.

C.M : Parlant de moyens, n'est-il pas opportun de renforcer la coopération avec la France et des pays comme le Canada pour muscler les opérations terrain, ce d'autant plus que les populations de ces pays sont bien souvent ciblées par les arnaques venant de Côte d'Ivoire ?
D.J : Jusqu'à maintenant, la coopération n'y était pas. Elle était surtout en Europe. En dehors de l'Europe, c'était très difficile d'établir une coopération. Moi, il y a une question que je me pose : pourquoi d'ici ils vont essayer d'arnaquer la France ou le Canada ? Déjà parce qu'il n'y a pas de barrière au niveau de la langue. Puis, ce sont des pays qui ont des moyens. Qui sont prêts à payer pour rencontrer l'amour. On ne va pas essayer d'arnaquer un pays pauvre. Donc, on s'oriente vers ces pays-là.
Depuis maintenant quelques années, au-delà de l'évolution de la législation, la coopération internationale entre pays intérieurs et extérieurs de l'Europe s'est accentuée. Sans que ces pays n'aient forcément ratifié la Convention de Budapest, seul contrat officiel existant et contenant des protocoles d'entraides entre les autorités compétentes des différents pays impliqués, une entraide entre les organes judiciaires s'est naturellement créée. Aujourd'hui, l'entraide internationale est légion. C'est une forme de coopération qui n'a pas besoin de convention et qui, avec certains pays fonctionne très bien. En partie grâce à cela, la Côte d'Ivoire a commencé ces dernières années à s'attaquer au délinquants du numérique, réaliser des arrestations et amplifier ses actions…

C.M : Vous avez participé à l'IT Forum Côte d'Ivoire 2016 sur la sécurité des utilisateurs des services numériques. Partant de tout ce qui a été dit, comment entrevoyez-vous l'avenir de la Côte d'Ivoire dans 5 à 10 ans ?
D.J : La Côte d'Ivoire est en bonne voie pour sortir la tête de la cybercriminalité. Elle est en bonne voie parce que le combat commence obligatoirement par la sensibilisation des décideurs. Et ce forum a réuni des DSI, des directeurs de la sécurité numérique, des chefs d'entreprises, des officiels, donc des personnes qui décident de l'économie du pays. Si, nous formateurs, consultants, professionnels de la cybersécurité, on a bien fait notre travail pendant ces deux jours, il est clair que les visiteurs sont repartis d'ici avec de nouvelles armes. Maintenant, ceux qui auront été convaincus aujourd'hui ne seront pas forcément ceux qui seront les cibles de demain, des prochaines failles ou des prochaines attaques. Les prochaines victimes continueront à être les utilisateurs imprudents, ignorants et des proies potentielles qui n'ont pas pu être présentes à l'IT Forum. À force de sensibiliser les chefs d'entreprises, les DSI, et de faire en sorte que la sensibilisation à la cybersécurité et aux comportements prudents commence dès l'école, nous auront bientôt une nouvelle génération d'utilisateurs mieux formés et mieux armés.
Un autre phénomène qui tend à être inversé est celui de la faible importance accordée à la sécurité informatique. Quel que soit l'endroit dans le monde, la cybercriminalité est quelque chose d'inévitable et la sécurité informatique, en raison d'une course effrénée à la commercialisation à outrance, a trop longtemps été négligée par les constructeurs et les éditeurs de logiciels. Ils devront sans doute se conformer au concept « Security by design ».
Avant de miser sur sa R&D (Recherche et Développement) pour créer ou répondre à des besoins et commercialiser à tout prix pour rapidement la rentabiliser et ne chercher que les profits financiers, il deviendra bientôt obligatoire de penser sécurité avant de penser rentabilité. Avec l'évolution incoercible du numérique dans notre quotidien (objets connecté, santé connectée, vie connectée), il est indispensable que la sécurité des utilisateurs soit aussi le problème des inventeurs de nos vies numériques et pas seulement de ceux dont le métier est de réparer les bêtises des autres. La Côte d'Ivoire fait désormais partie des pays impliqués par ce combat et je n'ai aucun doute, ce pays se dirige droit vers une explosion de l'usage du numérique et une amélioration de sa lutte contre la cybercriminalité.

C.M : Au niveau international, quelle est la nouvelle tendance en matière de cybercriminalité?
D.J : Au Forum international de la cybercriminalité (FIC 2016), j'ai assisté à une présentation faite par un chercher en cybersécurité autour de l'étude de l'évolution d'un RAT (Remote Access Tool). Des virus utilisant des failles existent déjà mais la présentation portait sur une nouvelle forme de logiciel malveillant encore plus perfectionné en matière d'impacts et de conséquences sur les postes informatiques des victimes. On connaissait des failles en Flash, en Visual Basic et dans d'autres types de langages mais la faille en Java est une faille qui aujourd'hui peut toucher tous les ordinateurs puisqu'énormément de systèmes et de web services sont conçus autour du langage Java.
J'ai trouvé la présentation très intéressante et j'ai trouvé l'effet dévastateur pour tous ceux qui attraperont ce « Méchangiciel ». A la fin de la présentation, j'ai approché l'intervenant et lui ai demandé quel était le moyen de propagation utilisé par ce virus ingénieux du futur ? Il m'a répondu qu'il se propage tout simplement par pièce jointe dans un e-mail. Ça reste aujourd'hui le principal vecteur de propagation de systèmes malveillants. Surtout, si c'est bien monté avec ce qu'on appelle des techniques d'ingénierie sociale, c'est-à-dire des actes qui permettent de manipuler la personne destinataire du piège, par exemple un CV piégé transmis à une agence d'emploi, rien de plus normal, même s'il est piégé ! C'est pourquoi l'autre vecteur sur lequel j'insiste, c'est le vecteur humain, la sensibilisation des utilisateurs afin d'augmenter le taux de prudence qu'ils doivent avoir lorsqu'ils reçoivent un email. Un email piégé a des caractéristiques que l'on peut assez facilement identifier et qui permettent de dire qu'il y a un risque, et mettre une procédure en cas de doute. Pour moi, même s'il existe des lunettes 3D, des hologrammes, des choses complétement folles au niveau technologique, j'ai l'impression que la propagation de la cybercriminalité va pouvoir se faire encore pendant pas mal de temps dans de vulgaires pièces jointes, et probablement encore dans les arnaques et le phishing.
Une fois que le pirate aura obtenu les clefs il pourra mener son attaque par « Menace Persistante Avancée (Advanced Persistent Threat) », autre grande tendance déjà depuis quelques années et encore pour longtemps !
Article original et propos recueillis par Anselme AKEKO

Réagissez à cet article

Original de l’article mis en page : Cybercriminalité : « Il faut qu’on voie que la Côte d’Ivoire réagit » | CIO MAG