

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



« 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 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 POUVAIENT 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 forte sensibilisation pourra évidemment contribuer à réduire le nombre d'arnaques venant de Côte d'Ivoire.

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 POUVAIENT 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 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 connectés, 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 chercheur 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 « Méchanciciel ». 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 complètement 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 clés 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 AKEOK



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, contenus, 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.



Contactez-nous

Réagissez à cet article

Denis JACOPINI était présent aux cotés de grands experts en cybersécurité à Abidjan pour le 8ème IT Forum 2016



Denis JACOPIN était présent à l'IT Forum 2016 les 7 et 8 juin derniers. Invité aux cotés des plus grands Experts en Cybersécurité, la 8ème édition de ce Forum a eu pour thème Protection des Données, Gestion de l'identité numérique, Protection des transactions à l'ère du numérique : Risques, Enjeux et Stratégies de mise en oeuvre. Voici ses impressions.

Je tiens enfin à remercier tous les partenaires et sponsors sans qui ce Forum n'aurait pas été possible, et enfin, je tiens à remercier chaleureusement le public présent et attentif jusqu'aux ultimes minutes des dernières interventions des panélistes dont j'ai eu l'honneur et le privilège de faire partie.

Durant ces deux jours j'ai à la fois côtoyé des professionnels d'excellente facture et de réputation internationale proposant des produits relatifs à la cybersécurité et d'aide à la transformation numérique., et je me suis retrouvé face à un public d'une attention universitaire, des chefs de grandes entreprises et de grands DSI (Directeurs des Systèmes d'Information) venu écouter les avis et les conseils d'experts et surtout réfléchir avec nous aux moyens à mettre en œuvre pour aider la Côte d'Ivoire à négocier le virage vers un numérique plus sécurisé pour les entreprises et plus rassurant pour les utilisateurs.

Dès l'ouverture de l'IT Forum, nous avons été réconfortés par le discours de Monsieur Bruno Nabagné Koné, Ministre de l'Economie numérique et de la Poste, Côte d'Ivoire rassurant l'assemblée de sa volonté de permettre à son pays une évolution vers un numérique de confiance en ces mots: « Pas de développement économique sans cyber sécurité »



Quelques mots échangés avec Monsieur Bruno Nabagné Koné, Ministre de l'Economie numérique et de la Poste m'ont rassuré. Il compte bien tout mettre en œuvre pour respecter ces propos : « Pour que nos pays puissent continuer à tirer le meilleur profit de ces technologies, il faut un environnement où les utilisateurs sont en confiance. ».

Ce n'est plus seulement au plus haut niveau de l'état, ni au niveau des autorités du pays que cette révolution à lieu. J'ai pu assister à une des étapes essentielles vers une transformation des mentalités numériques et reste persuadé que désormais la Côte d'Ivoire pourra aussi compter sur ses DSI pour mettre en application sans relâche les règles de base d'un vrai hygiène informatique.

De part notre expérience et notre expertise, nous accompagnerons la Côte d'Ivoire dans sa démarche de sensibilisation, de qualification et surtout nous l'aiderons à redorer son blason terni par l'image d'un pays ayant sur son sol brouteurs et autres arnaqueurs.

Ce forum a aussi été l'occasion à l'assemblée d'avoir enfin, après un déballage de solutions de sécurité protégeant d'un nombre très restreint de problèmes, une liste d'un grand nombre d'attaques que la Côte d'Ivoire a à craindre et va devoir combattre sans relâche ces prochaines années.

Au cours de nos interventions, nous avons apporté la preuve à l'auditoire que la solution pour lutter contre la cybercriminalité ne peut pas être techniques. En effet, sur un ensemble de 11 techniques d'attaques courantes, Denis JACOPINI a démontré que seulement 3 pouvaient être maîtrisées par la mise en place de solutions techniques parfois coûteuses.

La prochaine étape, indispensable à mon sens, sera la lourde tâche consistant à faire évoluer les mentalités et les comportements des utilisateurs, dernier maillon de la chaîne sur lequel aucun garde fou technique n'est en mesure de totalement compenser son manque de connaissance des bonnes pratiques. Il restera donc une faille essentielle à combler, celle de l'humain qu'il sera nécessaire d'accompagner avec tact et pédagogie.

Photo : Mathieu Photo & Camera



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.



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Le Net Expert Informatique – Expert cybercriminalité, Expert déclarations CNIL, Expert sécurité Informatique, Expert Judiciaire en Informatique, formateur cybercriminalité, formateur CNIL, consultant cybercriminalité, Avignon Vaucluse Aix en Provence Montpellier Marseille Limoges Paris – Denis JACOPINI présent à Abidjan pour le IT Forum 2016 les 7 et 8 juin 2016

Code de la communication – La loi contre la cybercriminalité à réviser

	Code de la communication – La loi contre la cybercriminalité à réviser
---	---

Les internautes et les utilisateurs des réseaux sociaux espèrent que le projet de code de la communication a abrogé l'article 20 de la loi sur la lutte contre la cybercriminalité. Le gouvernement tiendra-t-il une promesse faite en 2014 ?



Le gouvernement tiendra-t-il les promesses faites par ses anciens membres ? La révision, voire l'abrogation de l'article 20 de la loi sur la lutte contre la cybercriminalité, fait partie des dispositions les plus attendues du projet de code de la communication. Adopté jeudi en conseil des ministres, et attendu incessamment devant les bureaux du Parlement, le projet reste, pour l'instant, inaccessible. Le sort de l'article 20 de la loi contre la cybercriminalité qui avait été abrogé dans l'avant-projet de texte soumis au gouvernement demeure encore inconnu.

Le président de la République ayant déjà affiché sa volonté de supprimer les peines de prison pour sanctionner certains délits de presse comme les injures ou la diffamation, on voit mal comment le Conseil des ministres aurait pu enlever du projet la disposition finale qui a indiqué, entre autres, l'abrogation du fameux article 20. Sanctionnant de peine de prison pouvant aller jusqu'à cinq ans, et d'amende pouvant s'élever jusqu'à 100 millions d'Ariary, toute personne coupable d'injures, de diffamation ou d'atteinte à la dignité d'une personne, par le biais de tout type de support, écrit, audio-visuel ou électronique, le fameux article 20 a soulevé un tollé aussi bien dans le milieu de la presse que parmi les utilisateurs des réseaux sociaux.

La ministre de la Justice et celui de la Communication de l'époque, pour calmer les esprits, avaient alors promis que des ajustements pourraient être apportés au texte s'il devait se trouver en contradiction avec le code de la Communication qui était alors en cours d'élaboration.

Or, en instituant les peines de prison et les amendes exorbitantes pour toute diffamation ou injure faite par voie électronique, la loi, sur la lutte contre la cybercriminalité est entrée en contradiction avec l'esprit qui avait guidé l'élaboration du Code de la communication.

Risque de maintien

De l'eau a, pourtant, coulé sous le pont depuis la validation du texte par le monde médiatique. Vu les relations de la présidence avec les internautes, notamment les utilisateurs du réseau social Facebook, il n'est pas impossible que les autorités aient préféré laisser tel quel l'article 20 de la loi sur la lutte contre la cybercriminalité. L'objectif étant que, comme l'aiment le dire les responsables de la communication des autorités, « limiter le confort de l'internaute qui se trouve devant son clavier et qui se croit intouchable ».

Certaines sources laissent par ailleurs entendre que durant ce long intervalle de temps entre la validation de l'avant-projet et son adoption en conseil des ministres, l'Exécutif a trouvé le temps de réintégrer les dispositions qui avaient été jugées liberticides par les professionnels des médias, et de retirer les articles plus « libéraux », tel que celui qui a abrogé l'article 20 de la loi contre la cybercriminalité. Il semblerait même que le texte, dans une de ses versions manipulées par le Gouvernement, fasse référence à cet article 20 en indiquant que certaines peines seront appliquées sans préjudice de celles prévues par la loi sur la lutte contre la cybercriminalité.

Attendue depuis sa promulgation en 2014, la révision de la loi sur la lutte contre la cybercriminalité, notamment en ce qui concerne l'abrogation de son article 20, pourrait finalement être une réalité maintenant que le code de la communication est en passe d'être adopté. Tout comme la fameuse loi peut encore rester telle une épée de Damoclès suspendue au-dessus de la tête des professionnels des médias, mais aussi des internautes et des utilisateurs des réseaux sociaux.



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.



[Contactez-nous](#)

Réagissez à cet article

Les pays arabes mutualisent leurs forces pour faire face à la cybercriminalité



Un atelier sur la sécurité informatique réunit les pays arabes depuis lundi dernier à Tunis. La rencontre qui devrait être clôturée ce vendredi vise à évaluer la prédisposition des Etats concernés à faire face aux attaques informatiques d'après le président du Centre arabe régional de la cybersécurité cité par le webmanagercenter.com.



La rencontre qui devrait être clôturée vendredi dernier vise à évaluer la prédisposition des Etats concernés à faire face aux attaques informatiques d'après le président du Centre arabe régional de la cybersécurité.

(CIO Mag) – Un atelier sur la sécurité informatique réunit les pays arabes depuis lundi dernier à Tunis. La rencontre qui devrait être clôturée ce vendredi vise à évaluer la prédisposition des Etats concernés à faire face aux attaques informatiques d'après le président du Centre arabe régional de la cybersécurité cité par le webmanagercenter.com.

Le directeur général de l'agence tunisienne de sécurité informatique, lui, indique que Tunis a pris très tôt des initiatives pour lutter contre la cybercriminalité. Mohamed Naoufel Frikha, repris par nos confrères, rappelle qu'un travail important a été réalisé depuis 1999 avec la création du premier centre en Afrique, le troisième dans le monde arabe.

Le rendez-vous de Tunis entend amener les pays arabes à créer des centres de cyber-alerte. Leur nombre est très insuffisant dans l'espace arabophone puisque seuls dix pays en disposent. Des représentants de treize Etats prennent part aux échanges.

Article de Ousmane Gueye



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.



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Cybercriminalité: les pays

Denis JACOPINI présent à Abidjan pour le IT Forum 2016 les 7 et 8 juin 2016



Cybersécurité en Afrique : état des lieux et perspectives



Avec 20% de sa population connectée à Internet, l'Afrique est un continent en voie de connexion au cyberspace. Une partie des pays du continent profite des retombées économiques du numérique mais ceux-ci doivent aussi faire face aux cybermenaces qui mettent en péril leur développement dans le cyberspace. Dès lors, comment se construit la cybersécurité en Afrique?

L'ENJEU DE LA CONNECTIVITÉ AVANT CELUI DE LA CYBERSÉCURITÉ

Avant d'évoquer pleinement la question de la cybersécurité en Afrique, il convient au préalable de poser une série de constats sur le niveau de connectivité du continent africain... [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.



[Contactez-nous](#)

Article original : *Cybersécurité en Afrique : état des lieux et perspectives* – SOLUCOMINSIGHT

Auteur : JULIEN DOUILLARD Consultant

Réagissez à cet article

Denis JACOPINI participera au 8e IT-Forum à Abidjan les 2 et 3 juin 2016



La 8e édition du IT-Forum (Forum des décideurs et acteurs des Technologies de l'Information) se déroulera les 2 et 3 juin prochain à Abidjan.

IT FORUM ^{8^{ème} EDITION}

Des conférences seront animées en plénières par des spécialistes, des Experts-Consultants et des Universitaires. Ce sera le lieu de faire des exposés, de partager des expériences, de former et d'informer les participants.

Les enjeux de la transformation numérique et plus globalement de l'appropriation des nouvelles technologies modifient considérablement notre mode de vie. La sécurisation des données et des dispositifs de paiement comporte des failles qu'il comporte d'améliorer pour apporter la confiance nécessaire au climat des affaires.

De nombreuses études viennent conforter ce constat et tendent à démontrer le potentiel de croissance du secteur.

En Côte d'Ivoire, les transactions mobiles s'élèvent à 15 milliards de FCFA par jour soit 22,5 millions d'Euros.

Des montants qui donnent le vertige et qui poussent les sites marchands notamment les opérateurs de télécommunications à prendre des mesures de sécurité de plus en plus importantes... mais qui montrent aussi rapidement leurs limites !

Au fil des années, la Côte d'Ivoire s'est imposée comme l'un des leaders naturels dans le domaine des transactions mobiles en Afrique.

En insistant sur la priorité à donner à la protection des données et des transactions (mobile banking, eCommerce),

Devenu un rendez-vous incontournable depuis une décennie, l'IT Forum s'impose aujourd'hui comme l'une des

rencontres les plus importantes.

QUAND

Jeudi 2 juin 2016 à 08:00 – Vendredi 3 juin 2016 à 18:00 (Heure : Côte d'Ivoire) – Ajouter au calendrier

LIEU

Maison de l'entreprise – CGECI (Confédération Générale des Entreprises de Côte d'Ivoire – Patronat ivoirien), Avenue Lamblin, Abidjan, Lagunes, Côte d'Ivoire, Abidjan, Plateau, Cote d'Ivoire –

PROGRAMME

<http://www.ciomag-event.com/8eme-edition-it-forum-cote-d-ivoire>



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.



[Contactez-nous](#)

Réagissez à cet article

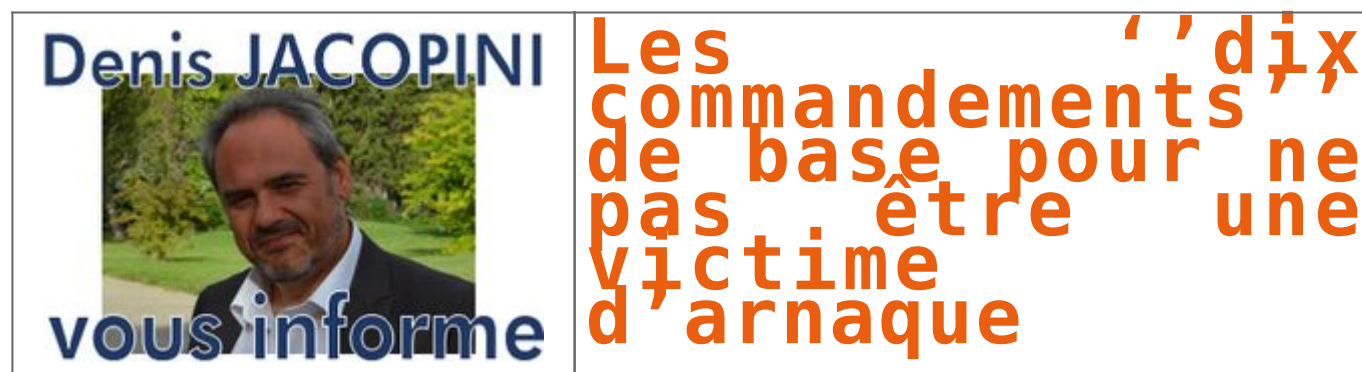
Sources :

IT-Forum 2016 – 8e édition du Forum des décideurs et acteurs des Technologies de l'Information

<http://it-forum.ci>

<https://www.eventbrite.fr/e/inscription-it-forum-2016-8eme-edition-24951266911>

Les ‘ ‘dix commandements’ ’ de base pour ne pas être une victime d'arnaque



Les cybercriminels continuent de faire de nombreuses victimes à travers le monde. Si des moyens de répression de cette activité criminelle sont entrepris dans nos différents pays, l'un des moyens les plus efficaces de l'éradiquer reste la prévention.



Dans cet article, la Plateforme de lutte contre la cybercriminalité (PLCC) fait un rappel en 10 points des mesures à prendre pour naviguer sur la toile en toute sécurité.

- 1- Changer régulièrement vos mots de passe. (Un site = Un mot de passe unique)
- 2- Aucune autorité judiciaire, de police ne possède d'adresse mail gratuite de type Hotmail, Yahoo, Gmail...
- 3- Ne divulguez pas d'informations personnelles sur Internet. Prenez le temps de sécuriser vos comptes ainsi que ceux de vos enfants. Ne rendez pas visibles vos contacts sur Facebook ou autre réseau sociale.
- 4- Allez toujours sur une adresse commençant par <https://>, officielle et habituelle pour vous connecter à votre compte bancaire, à votre messagerie ou autres réseaux sociaux.
- 5- Evitez d'envoyer des photos ou vidéos, de vous, à caractère sexuelle ou tout autre position indélicate.
- 6- Ne versez jamais d'argent par Mandat Cash ou Western Union à une personne que vous ne connaissez pas, que vous n'avez jamais rencontrée physiquement.
- 7- Méfiez-vous des trop bonnes affaires. Ne cédez jamais à la précipitation. Les bases d'une transaction sont les mêmes dans la réalité et sur Internet. Une annonce trop alléchante cache souvent une arnaque. Renseignez-vous, comparez les prix et les produits avant d'acheter.
- 8- Cessez tout contact si votre interlocuteur (que vous ne connaissez pas) vous demande de l'argent sous prétexte de frais, de maladie, de transport...
- 9- Remettez vous souvent en question. Il n'y a pas de profil type de victime, personne n'est à l'abri sur Internet. Les cyberdélinquants jouent parfois sur notre confiance excessive en nos capacités.
- 10- Ayez un anti-virus efficace et à jour sur votre ordinateur.

Une fois de plus, la PLCC vous exhorte à la prudence !... [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.



[Contactez-nous](#)

Réagissez à cet article

Source : *Lutte contre la cybercriminalité: Voici les ''dix commandements'' de base pour ne pas être une victime d'arnaque*

Une Afrique de plus en plus connectée mais qui doit faire face aux cybermenaces mondiales



Avec un taux de croissance au niveau des TIC de l'ordre de 30% sur un marché de plus d'un milliard de personnes, l'Afrique représente le nouvel Eldorado du monde numérique.



15 & 16 mars 2016 | King Fahd Palace | Dakar - Sénégal
CYBERSÉCURITÉ ET CONFIANCE NUMÉRIQUE



3^{ème}
ÉDITION

Or, la surface d'attaque augmentant, les cybercriminels élargissent leur champ d'action. La cybercriminalité en Afrique est organisée et bien enracinée, en particulier au Nigéria, au Ghana et en Côte d'Ivoire. Désormais, l'Afrique n'est plus le théâtre des seuls cybercriminels mais aussi de cyberhacktivistes voire de hackers. Le Sénégal a été la victime de cyberattaques en janvier dernier revendiquées par le collectif anonymous du Sénégal. Par rebond des attaques massives menées en janvier en France suite aux attentats de Charlie Hebdo, les serveurs de l'agence de l'informatique de l'Etat du Sénégal sont tombés.

Devant ce désert cybernétique, les Etats d'Afrique tentent de réagir en relevant le défi de sécuriser leurs infrastructures réseau, leurs données et en formant leurs personnels. La France participe activement à la formation cyber des officiers et des techniciens par le biais de la coopération opérationnelle (ministère de la défense). Depuis 2013, une centaine d'officiers et sous-officiers ont été formés au Sénégal, au Niger et au Burkina Faso par les Eléments français au Sénégal.

SecurityDay 2016

Avec la présence des plus grands décideurs du monde de la confiance numérique, l'évènement SecurityDay 2016 vous ont proposé pendant deux jours des conférences sur le thème « cybersécurité et confiance numérique ».

Les SecurityDays ont pour objectif de réunir l'ensemble de l'écosystème numérique africain et d'accélérer le développement d'un espace de confiance afin d'accompagner l'essor du numérique en Afrique, vecteur durable de croissance économique et de développement.

Avec le soutien de l'ANSSI française et de l'ADIE sénégalaise, cet évènement unique en Afrique de l'Ouest est un cadre d'échanges entre experts militaires, civils, décideurs IT, chefs d'entreprise, industriels et utilisateurs finaux pour réfléchir conjointement aux problématiques liées à la cybersécurité en Afrique. ... [Lire la suite]



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, arnaques Internet...) et judiciaires (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.



[Contactez-nous](#)

Denis JACOPINI est expert informatique assermenté spécialisé en cybercriminalité en Afrique de l'Ouest

Suivez-nous sur



Réagissez à cet article

**La Lutte Contre la
Cybercriminalité en Côte
d'Ivoire. Plus qu'un enjeu
économique, une réputation à
la clé**

	La Lutte Contre la Cybercriminalité, en Côte d'Ivoire. Plus qu'un enjeu économique, une réputation à la clé
--	--

La Côte d'Ivoire a très longtemps souffert d'une image que l'on associait régulièrement aux diverses arnaques sur Internet. Le pays doit avant tout rassurer.

Il suffit d'analyser les principales arnaques sévissant sur les réseaux sociaux, sites de loisirs ou petites annonces en France pour qu'on constate que l'interlocuteur à l'identité fausse mais attrayante soit accessible à partir d'un numéro +225, l'indicatif de la cote d'ivoire.

Certes, Maliens et Nigériens font aussi partie de la fête, mais que ça soit Monsieur Loulou ROBERT, Monsieur Jean OVIDIE, Monsieur Alain BRULIN, se faisant passer tout à tour pour une personne intéressée par un véhicule, une poupée barbie ayant reçu un coup de foudre, votre meilleur ami à qui on a volé son téléphone et ses papiers ou bien une riche personne désirant partager son héritage, ces brouteurs sont Ivoiriens.

Devant l'ampleur du phénomène et l'enjeu majeur que représente la sécurité des systèmes d'information à l'échelle de la Côte d'Ivoire, de l'Afrique et du monde entier, les autorités et les acteurs économiques du pays ont commencé il y a quelques années à réagir en multipliant des actions de formations, de sensibilisation et de perfectionnements technologiques.

Cependant, dans le but de faciliter le développement économique en Côte d'Ivoire et en Afrique des principales entreprises en les rassurant, créer et organiser des forums en 2016 (Conférence internationale sur le renforcement de la cybersécurité et de la cyberdéfense dans l'espace francophone à Grand-Bassam en février dernier et le 8ème édition de l'IT Forum à Abidjan en juin prochain) est un bon début mais ne suffit pas.

En effet, enfin d'enrayer le phénomène de la cybercriminalité, il est important, essentiel et urgent que la Côte d'Ivoire et ses voisins de l'Afrique de l'ouest s'engage à adhérer pour une coopération internationale comme a commencé à le faire à ce jour (15/04/2016), un seul pays d'Afrique, l'Afrique du Sud, en signant la Convention de Budapest.

Source : Denis JACOPINI

Illustration : <http://abidjantv.net>

Etat des signatures et ratifications de la Convention de Budapest

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité »
« Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).



- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;



[Contactez-nous](#)

Réagissez à cet article