

Le Cameroun se couvre contre la cybercriminalité | Le Net Expert Informatique



Le Cameroun se couvre contre la cybercriminalité

Un atelier initié par l'Ecole nationale supérieure polytechnique et financé par le Fonds spécial des activités de sécurité du ministère des Postes et télécommunications, veut mettre fin à la vulnérabilité des systèmes d'information des administrations publiques.

La rencontre de Yaoundé intervient en réponse aux intrusions malveillantes, dans le réseau d'interconnexion électronique, des systèmes d'information de l'administration mis en place par le ministère des Postes et télécommunications (Minpostel). Ce phénomène, explique le patron dudit département, Jean Pierre Biyiti bi Essam, cause de nombreuses pertes à l'Etat.

Les chiffres donnent en effet des sueurs froides, interpellant les pouvoirs publics pour une mise sur pied immédiate de nouvelles mesures de lutte contre un fléau planétaire. En 2014, les administrations camerounaises ont accusé plus de 14 milliards de FCfa de manque à gagner du fait de la cybercriminalité. En 2012, la compagnie aérienne nationale Camair-Co a perdu 2 millions FCfa en vente de billets ; Ecobank s'est fait hacker 43 comptes en 24 heures avec 3 milliards de FCfa, l'opérateur Mobile Telecommunications Networks (Mtn) a perdu un 1,8 milliard d'envoi de crédits. Plusieurs personnalités et représentations diplomatiques n'ont pas échappé aux attaques en ligne.

Le phénomène de la cybercriminalité a pris une envergure mondiale et sa propension, au Cameroun, a contraint le Jean Pierre Biyiti bi Essam à se rendre au front le 8 septembre à Yaoundé, pour le lancement d'un atelier de formation des personnels des administrations publiques. Il est question de sensibiliser les personnes en charge desdits systèmes sur les risques qui planent sur les réseaux des administrations, d'améliorer le niveau de sécurité des outils utilisés.

Un premier forum sous-régional sur la cybersécurité et la cybercriminalité s'était tenu du 24 au 27 février 2015 au Palais des congrès de Yaoundé. Organisée en partenariat avec l'Union internationale des télécommunications et le Commonwealth Telecommunication Office (CTO) en collaboration avec Interpol, la Communauté économique et monétaire des Etats de l'Afrique centrale (Cemac) et la Communauté économique des Etats de l'Afrique centrale (Ceeac), cette rencontre avait permis de mener des réflexions en vue de l'harmonisation des stratégies de lutte contre le phénomène, des régulations et réglementations en matière de cybersécurité et cybercriminalité, des moyens et outils de lutte, l'adoption de bonnes pratiques visant à créer une culture de cybersécurité en Afrique centrale, le renforcement des capacités et le partage des connaissances ainsi que la protection de l'enfant en ligne.

TIC

Les technologies de l'information et de la communication (TIC) se développent de manière exponentielle et irréversible, induisant une nouvelle civilisation ayant pour socle l'économie dite numérique. Force est cependant de souligner que les TIC s'accompagnent d'une poussée vertigineuse d'infractions et crimes de toute nature. Les atteintes aux biens renvoient à la fraude des cartes bancaires, à la vente, par petites annonces ou aux enchères, d'objets volés ou contrefaits, à l'encaissement d'un paiement sans livraison de la marchandise et autres arnaques de la même veine, au piratage d'ordinateurs, à la gravure pour soi ou pour autrui de musiques, films ou logiciels, etc. Les atteintes aux personnes se réfèrent quant à elles à la propagation d'images pédophiles, à la diffusion, auprès des enfants, de photographies à caractère pornographique ou violentes, de méthodes de suicide, de recettes d'explosifs ou d'injures à caractère racial, d'atteinte à la vie privée, etc.

Selon un rapport publié en 2011, McAfee, une société de sécurité informatique basée aux Etats-Unis, indique le «.cm» du Cameroun fait partie des cinq noms de domaine les plus risqués de la planète (.cm, .com, .cn, .ws, .info), avec un taux de risque de 36,7% sur environ 27 millions de noms de domaines analysés. Ce fléau a connu une flambée sans précédent entre juin 2009 et juin 2010. Les cybercriminels sont allés jusqu'à pirater le site officiel des services du Premier ministre en créant un site web frauduleux («<http://www.govcamonline.com/>») dont la page d'accueil portait les mêmes informations, jusqu'aux appels d'offres lancés sur le vrai site.

C'est ainsi que de nombreuses personnes, tant du Cameroun qu'ailleurs, se sont vues extorquer d'importantes ressources. Bien d'autres sites web camerounais ont également fait l'objet de cyberattaques à l'instar la douane, en 2008, du ministère des Domaines et des Affaires foncières au cours de la même année, de l'université de Yaoundé I en 2009, des quotidiens La Nouvelle Expression et Cameroon Tribune en 2011, etc.

Mesures de sécurité à parfaire

Le Cameroun a développé un certain nombre d'applications visant à automatiser les procédures, dans le cadre de la politique de mise en place de la gouvernance électronique. Il s'agit notamment de Sigipes, Sydonia, Depmi, e-Guce, etc. De même, les activités de transfert électronique d'argent, de consultation des comptes bancaires en ligne et bien d'autres services encore, se développent de manière étonnante. Le monde étant devenu un village planétaire, ces applications n'échappent pas aux menaces cybernétiques. D'où l'implémentation de systèmes visant à lutter contre les cyberattaques.

Une loi (n°2010/012) relative à la cybersécurité et à la cybercriminalité a été promulguée en fin 2010. Elle vise à instaurer la confiance dans l'utilisation des réseaux de communications électroniques et des systèmes d'information, à fixer le régime juridique de la preuve numérique. Elle protège également les droits fondamentaux des personnes physiques, notamment le droit à la dignité humaine, à l'honneur et au respect de la vie privée, entre autres.

Au plan institutionnel, trois structures sont en charge de la gestion de la question de cybersécurité et de la cybercriminalité au Cameroun. D'une part, le Minpostel est chargé de l'élaboration et de la mise en œuvre de la politique de sécurité des communications électroniques et des systèmes d'information, en fonction de l'évolution technologique et des priorités du gouvernement dans le domaine. L'Agence nationale des technologies de l'information et de la communication (Antic), en collaboration avec l'Agence de régulation des télécommunications (ART), assure, pour le compte de l'Etat, la régulation, le contrôle et le suivi des activités liées à la sécurité des systèmes d'information et des réseaux de communications électroniques ainsi que la certification électronique.

Le Cameroun a également entrepris, depuis 2009, de mettre en place, avec le concours de la République de Corée, une plateforme de sécurité appelée PKI (Public Key Infrastructure, ou infrastructure à clé publique), en vue de sécuriser les transactions gouvernementales en ligne. Ce dispositif donne les moyens suffisants au pays d'ouvrir le marché de la certification, dans lequel l'Antic représente à la fois les autorités de certification racine et de certification gouvernementale. Cette architecture s'inscrit dans le cadre des mesures techniques à prendre en vue de garantir la sécurité des transactions gouvernementales dans le cyberspace national. La plateforme de sécurité permet aussi, grâce aux services d'authentification, de non répudiation, d'intégrité et de confidentialité, de prémunir les données et les échanges électroniques gouvernementales d'attaques provenant de cybercriminels.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet... ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

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

Source : <http://237online.com/article-97191-securite-le-cameroun-se-couvre-contre-la-cybercriminalite.html>