Menacé de chantage sur Skype, un lycéen se suicide| Le Net Expert Informatique

	Menacé de chantage sur Skype, un lycéen se suicide

Après avoir été menacé par son interlocutrice virtuelle de voir une « vidéo intime » diffusée sur Internet s'il refusait de la payer, un jeune homme s'est donné la mort dans sa chambre.

Mercredi 4 juin, un peu avant 20 heures, à Castelsarrasin (Tarn-et-Garonne), un lycéen de 18 ans – qui s'appellerait Quentin – est attendu à la table familiale pour dîner. En l'absence de réponse à leurs appels, ses parents se rendent dans sa chambre. Et le découvrent dans une mare de sang, un couteau planté en plein coeur.
Quentin est déclaré mort peu après l'arrivée des secours. Les policiers qui leur font suite se concentrent sur son ordinateur portable, resté allumé. Ils y découvrent les causes probables de son suicide grâce à la fenêtre de conversation restée ouverte sur sa messagerie vidéo Skype : un chantage à la webcam.

Une jeune femme le menace de diffuser une vidéo intime
Les enquêteurs remontent le fil de la discussion et constatent que Quentin s'était filmé nu pour son interlocutrice. Celle-ci l'avait ensuite menacé de diffuser cet enregistrement sur internet s'il refusait de payer une certaine somme d'argent sur le champ. Pris de panique, Quentin se serait donné la mort pour éviter un scandale.
Le parquet de Montauban a ouvert une enquête préliminaire.
« La Dépêche du midi », qui avait d'abord évoqué l'hypothèse d'un chagrin d'amour avant de retenir celle du chantage, précise que la mère du lycéen l'aurait découvert avec une « corde au cou ». Mais évoque également, comme RTL, une « mare de sang ».
Le jeune homme, décrit comme un « très bon élève » de terminale au lycée professionnel de Beaumont-de-Lomagne, n'avait jamais parlé de suicide à ses proches. Les centres d'intérêt de son probable profil Facebook tournaient essentiellement autour des mangas.

Un scénario similaire à Brest, en 2012
Ce suicide rappelle un drame similaire survenu à Brest en octobre 2012. Un jeune homme de 18 ans s'était dénudé par webcam, sur Facebook, à la demande d'une jeune femme rencontrée en ligne qui faisait de même. Avant d'interrompre le « jeu » au bout de 10 minutes en le menaçant : « J'ai une vidéo porno de toi, si tu ne me donnes pas 200 euros, je vais détruire ta vie. »
Paniqué à l'idée de voir la vidéo diffusée à ses amis Facebook, le lycéen s'était pendu après avoir laissé un SMS d'adieu à ses parents. L'adresse IP de la femme provenait de Côte d'Ivoire, où des maîtres chanteurs connus sous le nom de « brouteurs » sont devenus des professionnels de ce genre de pratique.

Source : http://tempsreel.nouvelobs.com/faits-divers/20150605.OBS0251/menace-de-chantage-sur-skype-un-lyceen-se-suicide.html
Par Alexis Orsini

L’Afrique a besoin de cybersécurité| Le Net Expert Informatique

L’Afrique a besoin de cybersécurité

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.

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.
Le Security Day, qui se tiendra les 15 et 16 mars 2016 à Dakar, sera l'occasion d'aborder l'ensemble de ces sujets.

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

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

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

Source : Newsletter n°3 FIC
https://www.forum-fic.com/site/FR/Newsletter/S_inscrire_a_la_newsletter,C58881,I58949.htm

Cybercriminalité : Une stagiaire dérobe 1 million de FCFA à son patron

Cybercriminalité : Une stagiaire dérobe 1 million de FCFA à son patron

Mardi 17 février 2015-Kadija Koné stagiaire dans une agence Rechercher agence de transfert d'argent a été épinglée par la Police de Lutte contre la Cybercriminalité (PLCC), pour escroquerie Rechercher escroquerie , faux et usage de faux Rechercher faux et usage de faux portant sur la somme d'un 1000 000 FCFA dérobé à son patron.

En effet, et pour subvenir aux soucis financiers de son ex compagnon, la stagiaire en question a frauduleusement retiré la somme de 1 581 550 FCFCA, sur le compte géré par son patron entre septembre 2014 et janvier 2015. Le patron ayant constaté les faits a avisé la PLCC Rechercher PLCC et porter plainte contre X.
Après enquêtes, la PLCC Rechercher PLCC a fini par mettre le grappin sur Kadija Koné, qui d'ailleurs ne mettra aucune difficulté pour reconnaitre les faits qui lui sont reprochés.
« Je voulais octroyer un prêt à usure à mon ex copain. J'ai retiré 1 000 000 FCFA sur le compte géré par mon patron. En retour et comme convenu j'ai reçu en récompense un acompte de 450 000 FCFA, ensuite mon ex devait me rembourser à hauteur de 1 200 000 FCFA », aurait-elle révélé dans les locaux de la PLCC. La stagiaire a été déférée devant le parquet pour escroquerie, faux et usage de faux.
Selon la nouvelle loi sur la cybercriminalité, cette dernière risquerait une peine allant jusqu'à 20 ans de prison ferme, et une amende de 40 millions de FCFA.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://koaci.com/cote-divoire-cybercriminalite-stagiaire-derobe-million-fcfa-patron-pour-aider-copain-elle-risque-prison-98895.html
Par Donatien Kautcha, Abidjan

Le ministre de la Poste et des TIC appelle à « une culture nationale » en matière de cyber-sécurité

Le ministre de la Poste et des TIC appelle à « une culture nationale » en matière de cyber-sécurité

Abidjan – Le ministre de la Poste et des Technologies de l'information et de la communication, Bruno Nabagné Koné, appelle au développement d' »une culture nationale » autour de la question de la sécurisation des réseaux et services numériques qui, estime-t-il, est essentielle pour lutter efficacement contre la cybercriminalité en Côte d'Ivoire.

Pour le ministre Nabagné Koné qui procédait lundi à l'ouverture d'un séminaire sur la cyber-sécurité organisé par l'Autorité de régulation des télécommunications/TIC de Côte d'Ivoire (ARTCI) autour du thème principal « Développement d'une stratégie nationale en matière de cyber sécurité », il s'agit notamment d'élever la question au rang de celles relevant de la sécurité nationale.
Le séminaire qui s'étendra sur deux jours se veut, selon le DG de l'ARTCI, Bilé Diéméléou, une lucarne d'échanges et de partage d'expériences afin de présenter les actions entreprises par sa structure dans l'accomplissement de sa mission visant à développer la cyber-sécurité.
La rencontre sera également l'occasion d'établir les bases du développement d'un partenariat public/privé fort en matière de cyber-sécurité avec la centaine de structures conviées, a-t-il ajouté.
Le ministre Nabagné Koné déplorait, à l'occasion, le fait que le traitement de la question de la sécurisation des réseaux et services numériques, « considérée comme la 5ème roue du carrosse dont on peut se passer », n'a pas toujours suivi le niveau d'évolution enregistré ces dernières années en Côte d'Ivoire en matière de TIC et même dans le monde.
C'est pourquoi, il appelle à une culture nationale en la matière et qui, selon lui, permettra de faire du souci de la sécurisation du cyber espace ivoirien une question de sécurité nationale.
Le ministre des TIC rappelait auparavant le danger que laisse planer la cybercriminalité sur le développement global de la Côte d'Ivoire, un phénomène qui, a-t-il reprécisé, va au-delà de la perception commune l'assimilant abusivement aux petites escroqueries commises au moyen des outils de moderne de communication.
La cybercriminalité est plutôt le fait pour une personne de s'introduire de façon malveillante dans des systèmes d'information, a-t-il fait comprendre, relevant que c'est cet aspect des choses qui rend le phénomène si préoccupant.
« Que des personnes entrent dans nos systèmes, c'est de cela que nous avons peur et c'est face à cela que nous devons prendre des mesures », a fait remarquer M. Nabagné Koné.
Il a notamment relevé le fait que le phénomène, s'il n'est pas efficacement combattu, pourrait consacrer un recul de l'usage des TICS qui partirait d'une méfiance légitime des populations vis-à-vis des solutions offertes.
« Sans confiance, la réaction des utilisateurs sera le rejet et c'est notre société qui recule », a laissé entendre le ministre.
« Les personnes malveillantes dans le cyberespace ou en ligne sont nombreuses, organisées et leurs motivations sont très diverses: politiques, criminelles, terroristes ou activistes. La cyber-sécurité doit faire partie intégrante du progrès technologique », a-t-il, pour ce faire, appelé.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://news.abidjan.net/h/526302.html

Côte d'Ivoire : Deux caissières d'une agence Western Union épinglée

Côte d'Ivoire : Deux caissières d'une agence Western Union épinglée

L'équipe de la PLCC a épinglé récemment Dames Wamien Ahou Chantal et Oulobo Ahou Véronique, toutes deux caissières d'une maison de transfert d'argent de la place.
L'interpellation fait suite à l'exploitation d'une information anonyme selon laquelle ces dames se sont rendues complices d'un cybercriminel au fait de recevoir de ce dernier par SMS, des codes de transaction. Et ce, en vue de retirer des fonds. La contrepartie de ce concours frauduleux serait qu'elles prendraient 10% et expédieraient le reliquat au cybercriminel via orange money.

Après interrogatoire, les nommées WAMIEN AHOU CHANTAL ET OULOBO AHOU AHOU VERONIQUE ont reconnu sans ambage avoir rencontré un certain nommé GYPY ainsi que les faits qui leur sont reprochés.
De l'acte délictueux, elles ont avoué avoir retiré quatre (04) mandats Western-Union d'un montant total de 1 225 207 FCFA. De cette somme, elles ont également fait l'aveu d'avoir pris 106 000 FCFA et expédié le reste au cybercriminel par orange money.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.connectionivoirienne.net/106570/cote-divoire-cybercriminalite-deux-caissieres-dune-agence-western-union-epinglee

Chronique de Jawad Kerdoudi, président de l’IMRI: « La cybercriminalité, migration du crime réel vers le virtuel »

	Chronique de Jawad Kerdoudi, président de l’IMRI: « La cybercriminalité, migration du crime réel vers le virtuel »

Comme chaque semaine, l'Institut Marocain des Relations Internationales (IMRI) publie une chronique sur l'actualité. Cette semaine, son président Jawad Kerdoudi s'est intéressé à « La cybercriminalité, migration du crime réel vers le virtuel ».

La récente attaque aux Etats-Unis des systèmes informatiques de Sony Pictures relance le problème de la cybercriminalité. Celle-ci est définie comme l'ensemble des infractions pénales spécifiques liées aux technologies de l'information et de la communication. Ces infractions concernent plusieurs secteurs tels que le « carding » qui porte sur le piratage des cartes bancaires, le « skimming » criminalité qui s'attaque aux automates, le « phising » qui est une pêche des informations bancaires et commerciales, et enfin les escroqueries sur internet de toutes sortes qui englobent la xénophobie, la pedopornographie, l'incitation à l'usage des stupéfiants, le proxenétisme, le terrorisme, et le piratage téléphonique au préjudice des opérateurs.
Ce phénomène prend de plus en plus d'ampleur avec le développement d'internet qui est certes un moyen formidable de communication, mais également un instrument puissant de pouvoir et de guerre. Selon le Computer Crime Research Center, seuls 12% des cybercrimes étaient connus par la police et la justice en 2004. Plusieurs scandales ont défrayé la chronique, dont celui de la NSA en 2013 provoqué par Edward Snowden. Le coût global des cyberattaques a été estimé à 300 milliards d'euros pour les entreprises en 2013. Les Etats-Unis perdent entre 17,5 à 87,5 milliards d'euros par an, et 556 millions de personnes dans le monde ont été victimes de cybercriminalité. Cette situation risque d'empirer du fait du développement extraordinaire des investissements dans le secteur technologique numérique tels que ADSL, L4G, WIFI, Cloud. Le phénomène risque de s'amplifier également par la dématérialisation des processus, le développement du e-commerce et du e-learning, la croissance des paiements en ligne, l'augmentation des utilisateurs du Web qui a enregistré un taux de croissance de 46% entre 2012 et 2013. Le haut lieu mondial de la cybercriminalité pour la création de logiciels malveillants est la Chine, suivie par la Russie, les Etats-Unis, le Brésil et le Royaume-Uni. Pour les machines détournées la première place appartient aux Etats-Unis, suivie par la Chine, la Corée du Sud, l'Allemagne et la France. Enfin par les crimes relatifs aux arnaques sur internet, la palme revient à l'Afrique en particulier la Côte d'Ivoire et le Nigeria.

MINIMISER LES CONSÉQUENCES DE L'ATTAQUE
Pour se protéger contre la cybercriminalité, il est clair que le risque zéro n'existe pas. Il faut faire en sorte que si elle arrive, les conséquences de l'attaque soient minimes. Il faut pour cela renforcer les moyens matériels et humains, procéder à une modification de la législation, développer une culture de l'informatique, et associer le secteur privé à la lutte contre ce fléau. Il faut également privilégier l'approche préventive, c'est-à-dire qu'il faut augmenter les difficultés des attaques en diminuant les profits potentiels. Cela signifié le renforcement de la robustesse des infrastructures informatiques et de télécommunications. Il faut enfin s'appuyer sur des structures de veille et d'alerte telles que le CERT/CC américain. La coopération internationale est indispensable, car les pays qui ne sont pas dotés de lois contre la cybercriminalité sont des paradis numériques, où les cybercriminels peuvent lancer des attaques informatiques ou héberger des sites illicites en toute impunité. Elle a déjà commencé par la Convention de Budapest du 23 Novembre 2001 sur la cybercriminalité qui a le mérite de régler les problèmes de compétence et d'entraide entre Etats, et de les obliger à conserver certaines données pour permettre le traçabilité de l'information. Elle énumère plusieurs infractions (accès illégal, interception illégale, atteinte à l'intégrité des données et des systèmes) pour lesquelles chaque pays doit avoir un volonté politique et une coopération efficace de leurs services de justice et de police. Cette coopération internationale pose le problème de la gouvernance d'internet sur le plan mondial. Certains s'interrogent sur la pertinence d'une réglementation, d'autres demandent qu'elle soit déclarée comme un bien commun, et placée sous le contrôle de l'ONU ou d'un organisme intergouvernemental autonome.

QU'EN EST-IL DE CETTE QUESTION DE LA CYBERCRIMINALITÉ POUR LE MAROC ?
D'après Microsoft, le Maroc est 3,5 fois plus vulnérable aux logiciels malveillants que la moyenne mondiale. Le Maroc présente des failles touchant l'administration et les infrastructures qui constituent des menaces pour la sécurité nationale publique et économique. Preuve en est le piratage à partir du mois d'Octobre 2014 de documents confidentiels marocains relatifs à la diplomatie, au Sahara, et aux services de l'appareil de l'Etat. Le cybercriminel se fait appeler Chris Coleman, sévit sur un compte Twitter et n'a pas caché son objectif de nuire au Maroc. Une lecture officielle de ce cybercrime a été présentée le 11 Décembre 2014 devant la Chambre des Conseillers accusant les services spécialisés algériens d'avoir monté et accompagné cette opération. Dès lors, il faut que la cybercriminalité soit un chantier prioritaire pour le gouvernement, et passe du stade défensif à celui offensif. D'où la nécessité de créer une structure civile placée à un haut niveau, et qui aura par vocation la centralisation des informations et la coordination entre les services civils et militaires. Elle doit disposer également d'un centre de documentation chargé recueillir les statistiques spécifiques en vue de les analyser. Elle devra jouer un rôle opérationnel, signaler les contenus illicites sur internet, et apporter une assistance technique au profit du secteur public et privé. Elle sera également chargée de la formation et de la sensibilisation, et assurera les relations avec les Agences internationales chargées de lutter contre la cybercriminalité.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.aufait.ma/2014/12/23/chronique-de-jawad-kerdoudi-president-de-limri-la-cybercriminalite-migration-du-crime-reel-vers-le-virtuel_635947
par Jawad Kerdoudi, président de l'IMRI