ACTUAL-IT

LE MAGAZINE D'INFORMATION DE L'ÉCONOMIE NUMÉRIQUE

N° 02
octobre 2016

La cybersécurité, clé de voûte de l'économie numérique en Côte d'Ivoire

LA CYBERSECURITÉ, CLÉ DE VOÛTE DE L'ÉCONOMIE NUMÉRIQUE EN CÔTE D'IVOIRE

André A. APETE, Directeur de Cabinet du Ministère de l'Economie Numérique et de la Poste

Dans notre précédent propos éditorial, nous faisions état de ce que le développement prodigieux des TIC au cours des dernières décennies est constitutif de la 4ème révolution industrielle transformatrice de notre espace économique et sociétal, avec des enjeux de progrès incommensurables. L'Économie numérique, et généralement, la Société numérique issue de ce nouveau paradigme tend à rendre notre monde bicéphale. Il est, hélas, que tous les maux observables à l'échelle de la société dite réelle, le sont également au niveau du cyberespace qui est un milieu à part entière.

Eu égard aux enjeux de cette nouvelle frontière du développement qu'est le cyberespace, il est capital et impératif pour toutes les parties prenantes d'y garantir la sécurité, sans laquelle rien de probant n'est possible.

L'absence ou l'insuffisance de sécurité engendrant des actes de nature criminelle, la Cyber-sécurité est en définitive l'antidote de tout ce qui est constitutif de crime dans le cyberespace.

Nous retiendrons qu'à travers sa résolution N0 181 prise à Guadalajara de 2010, l'Union Internationale des Télécommunications définit le concept de Cyber-sécurité en ces termes : «*On entend par cyber-sécurité l'ensemble des outils, politiques, concepts de sécurité, mécanismes de sécurité, lignes directrices, méthodes de gestion des risques, actions, formations, bonnes pratiques, garanties et technologies qui peuvent être utilisés pour protéger le cyber-environnement et les actifs des organisations et des utilisateurs. Les actifs des organisations et des utilisateurs comprennent les dispositifs informatiques connectés, le personnel, l'infrastructure, les applications, les services, les systèmes de télécommunications, et la totalité des informations transmises et/ou stockées dans le cyber-environnement. La cyber-sécurité cherche à garantir que les propriétés de sécurité des actifs des organisations et des utilisateurs sont assurées et maintenues par rapport aux risques affectant la sécurité dans le cyber-environnement. Les objectifs généraux en matière de sécurité sont les suivants: (la) disponibilité, (l') intégrité et (la) confidentialité.*»
Quant à la Cybercriminalité, la loi ivoirienne N° 2013-451 du 19 juin 2013, la définit comme étant l'ensemble des infractions pénales qui se commettent au moyen d'un système informatique ou sur un réseau de télécommunications ou un système d'information ».
Ces clarifications au plan des définitions faites, quelles sont les principales manifestations en matière de cybercriminalité ?
L'intrusion à visée criminelle dans un système d'information a entre autres finalités :

- le vol de données de toute nature, données personnelles, données économiques et commerciales, données sécuritaires et stratégiques, de savoir-faire;
- le sabotage d'infrastructures critiques telles que réseaux de télécommunications, réseaux électriques, services de sécurité, systèmes d'information stratégiques (banques, Etat..)etc.
- l'espionnage, les attaques à l'image.

Au regard des statistiques disponibles, il apparait qu'en Côte d'Ivoire les crimes se rapportant au cyberespace sont à 97% des arnaques rendues possibles, en très grande partie, par un excès de confiance des victimes en leurs agresseurs. Il s'agit donc pour l'essentiel des actes que l'on qualifie de Cyber-escroquerie. Aussi importe-t-il d'inviter nos compatriotes à plus de vigilance et de rigueur relativement à leurs échanges dans le cyberespace.

Quoi qu'il en soit, sécuriser le cyberespace ivoirien est d'un enjeu capital pour cette nouvelle économie portée par le numérique qui charrie d'importants flux de capitaux et de valeurs. Fort heureusement, de vigoureuses mesures prises par le Gouvernement, à travers le Ministère de l'Économie Numérique et de la Poste (MENUP), sont de nature à donner confiance aux cyber-citoyens de notre pays. Dans ce registre, peuvent être citées, entre autres :

- la prise de mesures légales telles que la loi relative à la lutte contre la cybercriminalité, celle relative aux transactions électroniques, et la loi sur la protection des données à caractère personnel ;
- l'identification des abonnés aux services de télécommunications/TIC (téléphone et internet) ;
- la mise en place d'institutions de gouvernance du Cyberespace telles que l'Autorité de Régulation des Télécommunications/TIC chargée entre autres, de la sécurité des réseaux et des systèmes d'information, de la gestion des noms de domaine internet du point CI;
- la création de structures opérationnelles de gestion et de veille sécuritaire telles que le Computer Emergency Response Team (CICERT) au sein de l'ARTCI;
- la mise en place au sein du Ministère en Charge de la Sécurité d'une Direction chargée des traces Technologiques (DITT), avec le soutien de l'ARTCI, à travers une plateforme technique de lutte contre la cybercriminalité (La PLCC).

Aujourd'hui, les résultats des dispositions prises par l'Etat de Côte d'Ivoire sont probants, car l'image du pays est restaurée et les cyber-escrocs sont désormais retracés, identifiés et traduits devant les juridictions compétentes.

Toutefois, il est important de noter qu'en matière de sécurité de l'espace numérique, la capacité des structures et des hommes qui en ont la charge, doit être en progrès continu, en vue de faire face efficacement aux enjeux d'un domaine en perpétuelle mutation technologique.

Ici, plus que partout ailleurs, le rôle en synergie de tous les acteurs et parties prenantes du cyberespace est gage d'efficacité et de succès. Ainsi :

- le Régulateur sectoriel veillera à la sécurisation du point CI, à la fiabilité des données d'identification des abonnées aux réseaux de télécommunications, et s'assurera à travers des audits que des systèmes critiques d'information tels que ceux des banques, des opérateurs de télécommunications disposent des meilleures protections qui soient ;
- les opérateurs de télécommunications/TIC, les concepteurs de plateformes et de dispositifs intelligents destinés aux traitements et à la conservation des données prendront toutes les dispositions techniquement pertinentes, pour s'assurer de façon effective que les gigabits de données que les utilisateurs du cyberespace font circuler à travers leurs réseaux et systèmes sont protégés et parfaitement sécurisés;
- les utilisateurs du cyberespace feront preuve de la plus grande vigilance quant aux mesures de sécurité à observer.

Il nous faut noter qu'en la matière, non moins déterminante est la coopération internationale, car le monde numérique est sans frontière spatiale…
C'est donc ensemble que tous, chacun dans son rôle, nous assurerons la sécurité indispensable à une vie de progrès dans le cyberespace de plus en plus englobant dans un univers numérique.

N° 02
octobre 2016

Directeur de Publication :
André A. APETE
Rédacteur en chef :
Serge COFFIE

Comité de rédaction :
Salimata DEMBELE
Zenab KARIM
Christiane YANGNI-ANGATE
Eric CONTAYON
Modibo SAMAKE
Ahmed SAKO

Contributeurs :
Gilles GREBO
Kaboré BABA

Conception :
Gilles GREBO

Coordinatrice :
Christiane YANGNI-ANGATE,
Service Communication
20 34 73 89

BILÉ Diéméléou Amon Gabriel, Directeur Général de l'ARTCI

«L'ARTCI est l'organe de l'État en matière de sécurité des réseaux et des systémes d'information. Elle apporte aux forces de l'ordre les compétences techniques nécessaires dans le cadre des investigations de cybercriminalité.»

BILÉ Diéméléou est le Directeur général de l'Autorité de régulation des télécommunications en Côte d'Ivoire(ARTCI). Il dévoile les dangers de la cybercriminalité pour le pays et ouvre une lucarne sur sa structure et ses attributions.

Quelles sont les principales menaces que fait peser la cybercriminalité sur la construction d'une économie numérique en Côte d'Ivoire ?

Les menaces sont de divers ordres à savoir :

- **sur le plan économique :** c'est un préjudice financier direct déclaré de plus de 30 milliards de FCFA entre 2009 et 2015. Par ailleurs, la contre-publicité de l'activité cybercriminelle en Côte d'Ivoire affecte l'image de marque du pays, réduisant considérablement l'attractivité du pays et partant les investissements dans le secteur numérique;

- **sur le plan sociétal :** le développement de la cybercriminalité a pour effet de faire baisser la confiance des populations dans l'usage des TIC, frein incontestable du développement de l'économie numérique. En effet, le sentiment d'insécurité peut avoir pour effet de réduire le taux d'usage des TIC et leurs services offerts, ce qui aura incontestablement un effet défavorable sur le développement du secteur de l'économie numérique, qui est d'un enjeu important pour l'économie nationale. De plus, le basculement précoce des jeunes dans la cybercriminalité a une influence négative sur la scolarité, car la plupart de ceux qui s'y engagent, abandonnent l'école et se retrouvent sans formation, ni éducation;

- **sur le plan de la coopération internationale :** les relations avec les autres pays sont altérées et le leadership de la Côte d'Ivoire est mis à mal au niveau international, notamment en ce qui concerne son positionnement au niveau de la sécurité numérique.

Quel est le champ de compétence de l'ARTCI en matière de sécurité du cyberespace ?

L'ordonnance 2012-293 relative aux technologies de l'information et de la communiation qui a créé l'ARTCI lui confère des compétences juridictionnelles en matière de recherche, de constatation et de sanction d'infractions liées aux TIC dans la limite de ses prérogatives. A cet effet, elle dispose d'agents assermentés dotés du statut d'officiers de police judiciaire. Elle a également pour mission de protéger le cyberespace national avec la possibilité de recourir à la force publique (Police, Gendarmerie, etc.).

En somme, l'ARTCI est l'organe de l'Etat en charge de la sécurité dans le cyberespace. Elle apporte aux forces de l'ordre les compétences techniques nécessaires d'investigations numériques.

Quels sont les instruments de lutte contre la cybercriminalité dont dispose l'ARTCI ?

Les principaux instruments sont:

- **la loi 2013-451 relative à la lutte contre la cybercriminalité :** elle définit le cadre légal de la lutte contre la cybercriminalité;
- **la Plateforme de Lutte Contre la Cybercriminalité (PLCC):** elle est une plateforme collaborative mise en place à l'initiative de l'ARTCI et regroupe des agents de l'ARTCI et des fonctionnaires de Police issus de la Direction de l'Informatique et des Traces Technologiques (DITT). Il s'agit du principal organe opérationnel de lutte contre la cybercriminalité en Côte d'Ivoire:
- **CI-Computer Emergency Response Team (CI-CERT) :** il a été en mis en place par l'ARTCI. C'est un centre de réponse aux incidents informatiques qui a pour mission de protéger le cyberespace national, et d'assurer la mise en œuvre rapide de mesures correctives en cas d'incidents de sécurité; par ailleurs, ce centre contribue à la protection des infrastructures critiques de l'Etat contre tous types d'attaques informatiques (intentionnelles ou accidentelles).

Quels sont le plan d'action et le modèle de gouvernance de la stratégie nationale de lutte contre la cybercriminalité ?

Le projet de stratégie nationale de cybersécurité est un document stratégique qui définit les orientations stratégiques de l'Etat ivoirien en matière de cybersécurité et les moyens pour les mettre en œuvre. Le projet de stratégie initié par l'ARTCI a enregistré le concours de tous les acteurs locaux pour son élaboration. Le projet final a été soumis au Ministère de l'Economie Numérique et de la Poste pour adoption. En ce qui concerne le modèle de gouvernance, la démarche est de proposer la création de paliers stratégiques qui assureront la mise en œuvre de la stratégie nationale de cybersécurité. Cette stratégie est définie à travers 3 niveaux de responsabilité, à savoir:

- une entité managériale stratégique de haut niveau qui définira les orientations stratégiques en matière de cybersécurité;
- des entités de contrôle et de suivi en charge d'assurer le suivi et la maintenance opérationnelle du plan d'action;
- des entités opérationnelles qui ont pour mission de mettre en œuvre une ou plusieurs parties du plan d'action.

Le plan d'action définit des actions à court, moyen et long terme qui s'étendent sur la période 2016 à 2020.

La sensibilisation étant un volet important de la sécurité numérique et de la lutte contre la cybercriminalité, quelles sont les campagnes menées par l'ARTCI ?

La sensibilisation est en effet un pilier essentiel de la stratégie nationale de lutte contre la cybercriminalité. L'ARTCI a déjà réalisé de nombreuses campagnes de sensibilisation par le biais de ses centres techniques, notamment CI-CERT et la PLCC. En effet, les campagnes de sensibilisation sur la cybercriminalité menées par la PLCC avaient pour cibles:

- les fonctionnaires de police;
- les élèves et les étudiants;
- les agents et les employés d'établissements financiers et de transfert d'argent.

En outre, des actions de sensibilisation et d'information sont régulièrement menées par CI-CERT à travers son site internet et l'ensemble de ses canaux de communication en ligne (réseaux sociaux, newsletter, etc.).
Par ailleurs, des campagnes de sensibilisation à plus grande échelle sont en cours de préparation dans le cadre de la mise en œuvre de la stratégie nationale de cybersécurité. Elles devraient démarrer cette année et s'étendre dans la continuité, conformément au plan d'action national.

Peut-on affirmer que les actions engagées dans le domaine de la sécurité numérique permettent de juguler la cybercriminalité et quelles sont les actions à mener dans un proche avenir ?

De nombreux efforts ont été faits par l'Etat ivoirien pour lutter contre la cybercriminalité et assurer le développement de la confiance numérique, gage certain de l'établissement d'une économie numérique prospère. Les efforts consentis ont permis d'améliorer l'indice global de cybersécurité de la Côte d'Ivoire défini par l'UIT. De plus, la baisse des cas de blacklistage des adresses IP ivoiriennes sur les plateformes de commerce électronique mondial est un signe encourageant. Enfin, selon les rapports statistiques fournis par la PLCC, la répression systématique des actes de cyberescroquerie (broutage) a eu pour effet de réduire le nombre de ces infractions.
Cependant, ces efforts consentis dans le cadre de la lutte contre la cybercriminalité doivent être renforcés et soutenus, afin de maintenir la dynamique dans laquelle le pays s'est engagé. A cet effet, les principales actions que l'ARTCI prévoit de mener dans le cadre de la lutte contre la cybercriminalité sont :

- assurer l'adhésion de CI-CERT au FIRST, qui est la première et la plus grande communauté mondiale des équipes de réponses aux incidents de sécurité informatique;
- établir un plan d'audit des infrastructures critiques de l'Etat;
- renforcer la sensibilisation à travers l'organisation d'une campagne nationale d'information;
- renforcer les capacités des agents de CI-CERT et les fonctionnaires de Police de la PLCC;
- renforcer les moyens matériels et humains de la PLCC.

Computer Emergency Response Team

CI-CERT (Côte d'Ivoire – Computer Emergency Response Team) est le CERT national ivoirien, mis en place par l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire (ARTCI). Dotée de ressources humaines spécialisées en sécurité des systèmes d'information, l'équipe offre une assistance technique proactive et réactive aux entreprises et aux particuliers, dans le cadre du traitement d'incidents de sécurité.
CI-CERT est le point focal national en matière de veille et de monitoring de sécurité, de traitement de vulnérabilités, de détection et d'alertes des incidents de sécurité, en s'appuyant sur son réseau mondial de partenaires.

Lieutenant-Colonel Guelpétchin OUATTARA, Directeur Général de la DITT

«La DITT concentre plusieurs métiers des technologies numériques qu'elle met au service de la sécurité. Elle est de ce fait le pont entre deux administrations essentielles pour notre pays.»

Directeur général de la Direction de l'Informatique et des traces technologiques (DITT), le Lieutenant-Colonel Guelpétchin OUATTARA, présente l'organe dont il a la gestion et donne les missions à lui assignées.

Quels sont le rôle et la mission de la Direction de l'Informatique et des Traces Technologiques (DITT) ?

La DITT a pour rôle:

- **d'identifier et de piloter les projets technologiques pour la sécurité.** A ce titre, plusieurs projets ont connu un aboutissement dont le Centre d'Appel d'Urgence et la vidéoprotection de Yamoussoukro. Le projet phare actuel est le projet de vidéoprotection de la ville d'Abidjan pour lequel, le BNETD, l'ANSUT et la DITT concentrent respectivement les efforts du Ministère de l'Économie Numérique et de la Poste (MENUP) et du Ministère d'État, Ministère de l'Intérieur et de la Sécurité (MEMIS);
- **d'assister et d'appuyer les enquêteurs pour toutes leurs problématiques liées aux technologies numériques;** cet appui se fait grâce au Laboratoire de Criminalistique Numérique (LCN) de la DITT qui développe deux activités novatrices que sont le digital forensic et l'analyse de données numériques;
- **la DITT a pour mission de conduire les enquêtes pénales de cybercriminalité;** Pour ce faire, elle héberge la Plateforme de Lutte Contre la Cybercriminalité (PLCC) qui est, encore une fois, l'émanation de la coopération entre le MENUP et le MEMIS. En effet, la PLCC est le fruit de l'accord de partenariat signé entre l'ARTCI et la Direction Générale de la Police nationale.

En somme, la DITT concentre plusieurs métiers des technologies numériques qu'elle met au service de la sécurité. Elle est de ce fait le pont entre deux administrations essentielles pour notre pays.

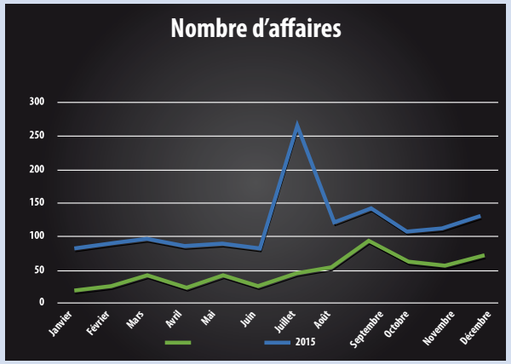
Quel est l'état des lieux de la cybercriminalité en Côte d'Ivoire ?

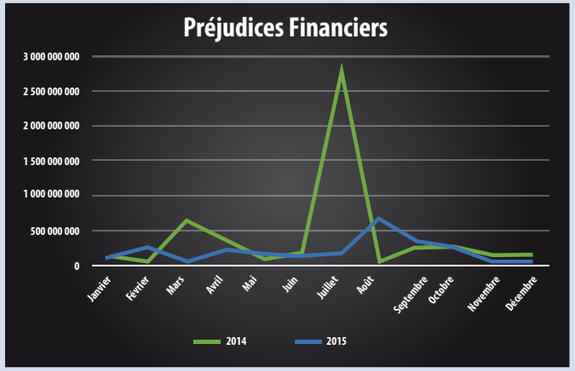
Pour les détails, il faut consulter les statistiques de l'année 2015 publiées sur le site web de la PLCC (http://cybercrime.interieur.gouv.ci/) mais les chiffres montrent une intensification de la lutte avec le triplement du nombre d'affaires prises en charge par la PLCC passant de 564 en 2014 à 1409 en 2015, ainsi que la baisse du préjudice financier constaté. La PLCC a déféré devant les tribunaux 159 personnes en 2015 contre 63 en 2014.
Les cyberdélinquants sont des jeunes âgés en moyenne de 25 ans qui ont eu une scolarité difficile ou ont abandonné leurs études autour de la classe de 3eme. Il faut noter cependant qu'ils n'utilisent pas de procédés techniques avancés (hacking) pour commettre leurs crimes mais plutôt le pouvoir de persuasion. Leur comportement criminel tend à répondre à une agression ou à une «injustice subie» telle que la pauvreté, le chômage, la *«dette coloniale»* etc. Quant aux victimes, elles sont des personnes âgées, ayant en moyenne 45 ans, qui proviennent la plupart du temps de classe sociale moyenne. Elles ont une trop grande confiance au monde virtuel et donc leur naïveté ou leur cupidité joue un rôle décisif dans la perpétration du crime.
La cybercriminalité en Côte d'Ivoire est essentiellement constituée d'infractions classiques facilitées par les TIC. En des termes plus clairs, il s'agit généralement d'escroquerie, de chantages et d'extorsions basés sur des images sexuelles, etc. De ce fait, il faut retenir que les infractions de cybercriminalité ici ne présentent aucun défi technologique. Les délinquants n'ont rien de génies en informatique. Ce sont juste des escrocs à l'imagination fertile qui utilisent le potentiel d'internet pour amplifier leurs méfaits. Le terme cyber-escroc est beaucoup plus adapté dans notre cas.

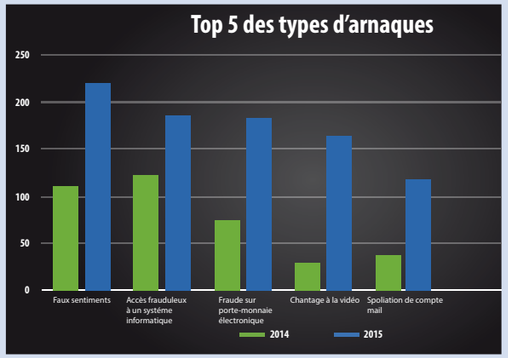
Quelles sont les actions concrètes menées en vue de lutter contre la cybercriminalité ?

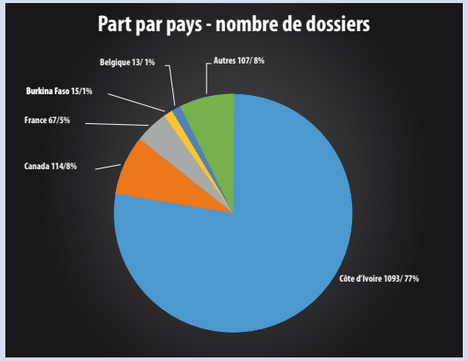
Le premier axe de lutte est la répression, c'est-à-dire la recherche et la condamnation des délinquants. La répression est d'autant plus efficace que la PLCC a élargi

RAPPORT D'ACTIVITÉ 2015









Comparé à l'année 2014, le nombre d'affaires traitées par la PLCC en 2015 augmente significativement. Il passe de 564 à 1409 affaires soit près de 150 %. Cela est surtout le signe d'une intensification des activités de la PLCC. Nous constatons une hausse du nombre d'affaires pendant les vacances scolaires (juillet-septembre). Cela s'explique par le nombre important des cyberdélinquants encore élèves ou étudiants. Le nombre de personnes interpellées est en forte augmentation (77,56 %) par rapport à l'année 2014 du fait du volume d'affaires traitées en 2015.
Contrairement au nombre d'affaires qui est en hausse, le préjudice total (consommé + tenté) en 2015 estimé à 3 980 833 882 FCFA a connu une baisse de 23,2%, comparé au préjudice de 2014 qui était de 5181663744 FCFA. Plusieurs éléments pourraient expliquer cette baisse, mais cela est le fait du nombre important de petites escroqueries.

Le ratio de victimes résidant en Côte d'Ivoire est de plus en plus important : 77,57 %. La raison est principalement le nombre important d'escroqueries locales, liées aux services de paiement par téléphone mobile dont les victimes résident essentiellement en Côte d'Ivoire. Le développement de l'internet mobile et la généralisation des réseaux sociaux en Côte d'Ivoire font également apparaître des infractions autrefois commises contre des personnes à l'extérieur du pays. Globalement et naturellement, les résidents des pays francophones restent les principales cibles des actes de cyberdélinquance perpétrés à partir de la Côte d'Ivoire. Il faut faire remarquer une flambée des infractions entre pays africains, principalement entre le Bénin, le Burkina Faso, le Cameroun, le Niger et la Côte d'Ivoire.

son réseau de coopération.
Le second axe est la coopération. Coopération avec les polices d'autres pays, généralement les pays francophones du Nord comme du Sud, mais également plusieurs pays européens comme l'Espagne, l'Italie et le Royaume-Uni, etc. Coopération avec les entreprises privées nationales et multinationales qui opèrent dans le domaine des TIC. Ce sont tous les opérateurs de téléphonie et d'internet de Côte d'Ivoire, mais aussi les grands groupes internationaux comme Western Union, Moneygram, Facebook avec qui les rapports sont quotidiens et bien suivis. Au niveau des organisations internationales, la DITT est membre du groupe de coordination d'INTERPOL Globale Center for Innovation (IGCI - Singapore) pour la lutte contre les « sextorsion ». Elle est membre du réseau 24/7 du G8 pour le gel des preuves numériques. Enfin la DITT participe intensément aux activités du comité technique cybercriminalité de FRANCOPOL ainsi qu'à celles de la FRANCOPHONIE NUMÉRIQUE.

Le troisième axe de lutte est la sensibilisation qui aide à prévenir les crimes. La PLCC est présente sur internet avec son site web et sa page Facebook qui fait référence mondialement avec plus de 47.000 abonnés actuellement. En plus des conseils et de la diffusion des cas résolus, la PLCC est présente sur le terrain avec les conférences, des formations, des stands lors d'expositions, des émissions radio et télé, etc. Les cibles sont extrêmement variées allant des entreprises aux élèves et étudiants en passant par les parents d'élèves. En 2015, une trentaine d'actions de terrain ont été menées par la PLCC contre une quinzaine en 2014.

Que dire des moyens de la DITT pour lutter efficacement contre la cybercriminalité ?

La réponse précédente traite un peu des moyens. Notamment la coopération et la sensibilisation. En dehors des moyens organisationnels, des procédures et des idées mises en place, la logistique et les finances qui sous-tendent toute l'activité sont essentielles. Ces moyens ne suffisent jamais, mais la PLCC a pu bénéficier de contributions remarquables des structures signataires de l'accord. Elle souhaite que ces contributions soient à minima confirmées en 2016. Je n'en dirai évidemment pas plus sur nos moyens, les criminels nous lisent aussi…

La population ivoirienne a-t-elle bien perçu les dangers que représente la cybercriminalité ? Que faire pour qu'elle puisse s'approprier cette lutte ?

La population ivoirienne n'a pas encore pris la mesure des dangers de la cybercriminalité. C'est la raison pour laquelle nous pensons que la sensibilisation doit être un axe majeur. Cette année, la PLCC travaille sur une vaste compagne de sensibilisation avec un cabinet conseil en communication de la place. Cette sensibilisation demandera la contribution et l'appui de tous les acteurs intéressés par cette lutte. Un environnement TIC plus sûr est profitable non seulement aux acteurs TIC, mais également aux entreprises de façon générale. Nous devons fédérer nos efforts pour atteindre cet objectif commun qui consiste à bâtir un cyberespace sûr et des transactions électroniques crédibles dans un écosystème de confiance. Notre sécurité et nos performances économiques en dépendent.

SÉCURITÉ INFORMATIQUE

L'entreprise face à la sécurité des applications et des terminaux mobiles

Les défis actuels des entreprises ne sont plus les mêmes que ceux d'hier. La bataille se tient désormais dans un monde virtuel caractérisé par la mobilité et la connectivité. De plus en plus d'utilisateurs et d'entreprises utilisent des smartphones comme outils de communication mais aussi pour la planification, la gestion et l'organisation de leurs vies professionnelle et privée. La multiplication des technologies digitales permet aux utilisateurs d'adapter facilement leur environnement de travail à leurs nouveaux usages.

En 2015, l'utilisation des appli mobiles a augmenté de 58% selon le spécialiste du tracking mobile, Flurry. Cet usage, s'il n'est pas contrôlé et sécurisé, peut mettre en péril le système d'informations d'une entreprise. Il est primordial pour les entreprises d'agir rapidement. Une gestion globale et intégrée des terminaux mobiles, des applications et de la sécurité au sein du système informatique est donc un véritable enjeu. Le risque ne vient plus seulement du fait qu'un terminal extérieur se connecte à un serveur interne. Les menaces peuvent désormais venir d'un terminal externe infiltré par une application malveillante. En effet, les smartphones collectent et compilent un nombre croissant d'informations sensibles dont l'accès doit être contrôlé afin de protéger la vie privée de l'usager et ce qui est du domaine de la propriété intellectuelle de l'entreprise. Un nouveau défi pour le DSI : gérer un parc informatique mobile multiplateforme, composé de terminaux professionnels et personnels, et d'une multitude d'applications qui posent autant de risques potentiels pour le système d'informations de l'entreprise. La croissance de ces risques implique donc une recrudescence des cyberattaques.

L'avènement du Bring Your Own Device (BOYD)

Le concept est né de l'avènement des portables, smartphones et tablettes ; ils sont entrés dans les habitudes personnelles des salariés et ils en font usage dans leur milieu professionnel. Ainsi, Gartner a prédit en 2014 que d'ici à 2018, il y aura deux fois plus d'appareils personnels utilisés à des fins professionnelles que d'appareils appartenant aux entreprises. Si les DSI ont tenté d'y résister, ils n'ont pas réussi pour la seule raison que ces outils de connexion nomades permettent aux employés d'améliorer leur productivité. Pourtant, ces terminaux intelligents sont des portes ouvertes aux attaques informatiques et permettent aux hackers d'entrer dans les réseaux informatiques des entreprises. Cette pratique pose plus généralement des questions relatives à la sécurité de l'information et à la protection des données, ainsi que des préoccupations sociales et juridiques.

Les risques provoqués par ces nouveaux matériels

En ouvrant son système d'information à ce nouveau type d'équi-

pement, une entreprise s'expose à d'éventuelles failles de sécurité encore méconnues du grand public. En effet, les règles de sécurité de l'entreprise ne sont en général pas suffisamment adaptées à la prolifération du BYOD et au déferlement des nouvelles technologies. Tant et si bien qu'elle doit dorénavant faire face à l'apparition de multiples applications malveillantes que l'utilisateur lambda télécharge, sans avoir conscience de leurs conséquences parfois nocives.

Les entreprises font ainsi face à des problèmes de distinction entre les données professionnelles et les données personnelles, de propriété sur les données, de sécurité de l'échange de données entre des terminaux privés et le réseau professionnel, de stockage des données et d'exposition supplémentaire à des risques de cyber hacking et d'intrusions malveillantes via des appareils ne leur appartenant pas.

Face à la montée en puissance du phénomène BYOD, les entreprises doivent trouver des solutions adéquates pour sécuriser réseaux et applications. La majorité des entreprises se fient à des systèmes de sécurité dépassés pour contrer les nouvelles menaces mobiles et applicatives. On retrouve ce même décalage dans la méthode avec laquelle les entreprises gèrent les risques de pertes des données applicatives stockées dans le cloud.

En effet, elles essaient très souvent de limiter ce risque en plaçant sur une liste noire une ou plusieurs applications cloud de synchronisation et de partage de fichiers dans l'entreprise. Le recours aux listes noires revient à étouffer les problèmes. Au vu de la multitude d'applications et de services de synchronisation et de partage disponibles, une règle de liste noire n'est pas suffisamment efficace et exhaustive pour les repérer tous.

Quelles solutions pour les entreprises ?

Mettre en application les règles de conformité et isoler les terminaux qui ne répondent plus aux normes. Un terminal non conforme étant une cible de choix pour une attaque malveillante à l'encontre de l'entreprise, il est souhaitable de mettre en place des politiques d'usage et de conformité strictes. Ainsi, des règles de mise en quarantaine peuvent servir à bloquer l'accès au réseau et/ou à supprimer de façon sélective les données d'entreprise stockées sur un terminal. Elles contribuent à limiter la perte de données et à respecter les exigences réglementaires en matière de conformité, ce qui peut éviter à l'entreprise de faire les gros titres à la rubrique «*Victimes de cybercriminalité* ».

L'International Data Corporation (IDC) a établi un lien entre les logiciels piratés et la cybercriminalité. Les malwares téléchargés délibérément sur un logiciel piraté par des cybercriminels servent ensuite comme un vecteur pour lancer des attaques. Les cybercriminels pourraient utiliser des logiciels malveillants pour voler des mots de passe, imiter un site bancaire et avoir un libre accès à un système d'exploitation.

En fait, les consommateurs et les entreprises du monde entier ont 33% de risque de rencontrer des malwares lorsqu'ils installent des logiciels piratés ou achètent des ordinateurs avec des logiciels piratés. Les Africains courent d'autant plus de risques d'être victimes d'une cyber-attaque, avec un continent qui représente 10% des incidents global de cybercriminalité.

Par ailleurs, il semble indiqué de ne plus inscrire systématiquement sur une liste noire les applications de stockage du cloud personnel, et privilégier plutôt les fonctionnalités de gestion ou de conteneurisation des applications fournies, pour permettre aux collaborateurs de stocker leurs données dans un cloud d'entreprise sécurisé. L'approche qui consiste à éviter la dissémination des données d'entreprise plutôt que de bloquer un nombre toujours plus important d'applications cloud, offre l'avantage non négligeable de séparer les données d'entreprise des données personnelles.

Nul doute qu'avec les appareils mobiles, les professionnels de la sécurité IT chargés de garantir la protection des informations d'entreprise font face à de nouveaux défis. À mesure que le rôle joué par ces appareils, leur évolution et leurs exigences spécifiques gagnent en importance dans l'entreprise, le contrôle nécessaire à la sécurisation des données doit progresser de concert. Les plus grandes organisations TIC gagneraient donc à la fois à développer une expertise interne et à faire appel aux professionnels de la sécurité de l'information.

Les solutions Microsoft

Le cloud computing offre une alternative abordable par répartition à l'achat d'une suite logicielle complète. Des services cloud de confiance auprès d'une compagnie de grande réputation comme Microsoft permettent d'accéder aux mises à jour de sécurité gratuitement, parce que les serveurs cloud peuvent mettre en commun les ressources de tous les clients, afin d'offrir la protection la plus sophistiquée au moindre coût.

Microsoft Enterprise Mobility + Security (EMS) est une solution complète, économique et rapide qu'une organisation peut mettre en œuvre pour répondre aux questions de management et de sécurité.

Sécuriser l'accès et la diffusion des données de l'entreprise

Microsoft Azure Rights Management permet, d'une part, d'élaborer et de mettre en œuvre les stratégies complètes de chiffrement, d'identification et d'autorisation et, d'autre part, de sécuriser les fichiers et les données de la messagerie d'entreprise sur l'ensemble des supports. Microsoft Advanced Threat Analytics aide à repérer les activités comportementales suspectes, quasiment en temps réel, et prévenir les actes de malveillance avant qu'elles ne causent des dommages à l'entreprise.

Proposer aux utilisateurs un accès unique à l'ensemble de leurs applications

Avec Microsoft Azure Active Directory Premium, l'organisation peut gérer, à l'échelle de l'entreprise, l'intégralité des identités et des accès à toutes les applications et à tous les devices, sur leurs datacenters ou dans le Cloud. Ceci aide à améliorer la productivité et à réduire les coûts de support technique grâce aux expériences en libre-service et d'authentification unique : une expérience utilisateur homogène, quel que soit l'appareil, grâce à un seul nom d'utilisateur et un seul mot de passe.

Gérez intégralement et simplement les devices iOS, Android et Windows depuis une console unique

Avec Microsoft Intune, l'entreprise pilote, depuis le Cloud, l'ensemble des appareils Windows, iOS, Android de manière centralisée. Face au volume croissant et à la diversité grandissante des appareils BYOD et des appareils d'entreprise, utilisés aujourd'hui par les collaborateurs, Microsoft Enterprise Mobility + Security permet de contrôler les accès aux applications et aux données de l'entreprise grâce à la solution de gestion des périphériques mobiles (MDM) et à la solution de gestion des applications mobiles (MAM) de Microsoft.

Le piratage des logiciels en Afrique a un niveau record : le cas d'utilisation de la chose réelle

Laisseriez-vous des pirates dans votre maison, ou près de votre famille ou de votre entreprise ? Très probablement pas – cependant, les gens dans toute l'Afrique involontairement s'exposent eux-mêmes à de graves-préjudices en laissant des logiciels piratés dans les coins les plus secrets de leur vie numérique. En fait, 80% des logiciels en Afrique sont piratés, et si chaque unité du logiciel était un vrai pirate, menaçant à la fois votre sécurité personnelle et professionnelle, on parlerait alors de sécurité nationale.
Les entreprises du Moyen-Orient et d'Afrique dépensent $ 8 milliards USD par an pour corriger les problèmes provoqués par les malwares chargés sur des logiciels piratés. Les consommateurs dépensent plus de 2 milliards USD , selon une étude conjointe menée par IDC et l'Université Nationale de Singapour (NUS).
En comparant cela aux $18 milliards USD que la piraterie maritime coûte au monde entier, on peut conclure que le piratage de logiciels est une menace qui coûte trés cher à l'entreprise.

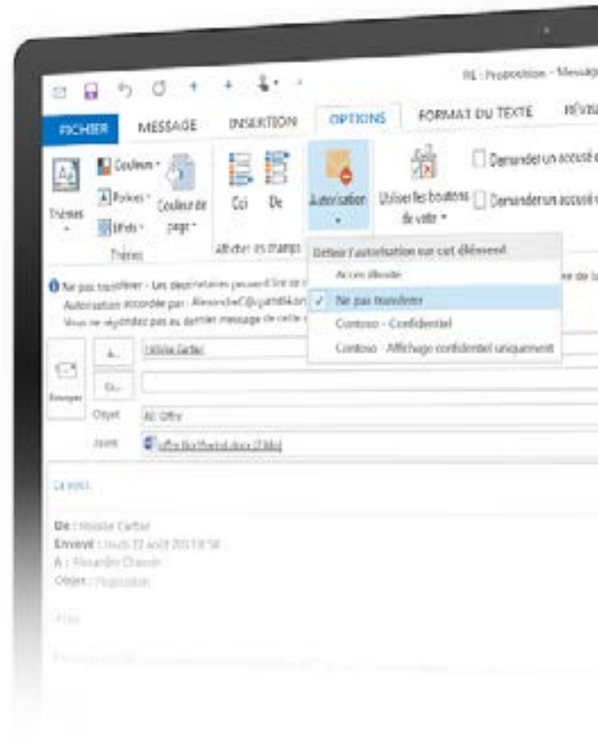
La bonne nouvelle est que le fait que vous soyez victime ou non dépend en grande partie de vous.

Rapport au risque/coût: 4 points à considérer :

- **gardez les criminels aux abois**
  Utiliser des logiciels piratés chez vous ou au travail revient à y inviter un criminel. Utiliser des logiciels authentiques éloigne les risques de compromission de la sécurité, en éliminant la possibilité d'installer des Chevaux de Troie et des backdoors à l'insu des usagers;

- **rentabilisez votre investissement**
  Protégez-vous en utilisant des logiciels authentiques. Un logiciel authentique coûte plus cher à l'achat, mais pas à long terme – surtout si l'on considère les coûts élevés associés à réparer les dommages causés par une cyber-attaque. L'achat d'un ordinateur avec un véritable système d'exploitation Microsoft préinstallé est la façon la plus rentable d'acquérir des licences de système d'exploitation Windows - sans les risques des coûts associés aux logiciels piratés dans le futur.
  Alternativement, le cloud computing offre une solution abordable à l'achat d'une suite logicielle complète. Des services cloud de confiance auprès d'une compagnie de bonne réputation, comme Microsoft, permettent d'accéder aux mises à jour de sécurité gratuitement, parce que les serveurs cloud peuvent mettre en commun les ressources de tous les clients, afin d'offrir la protection la plus sophistiquée sans aucun coût additionnel;

- **restez à jour**
  Un logiciel authentique permet de gagner en productivité, un temps de démarrage plus rapide, une plus grande autonomie, de meilleurs graphismes, personnalisation et performance. Plus important encore, il est livré avec les mises à jour de sécurité installées automatiquement.
  Il est également important que vous utilisiez des logiciels à jour. Windows XP est un exemple de logiciel désuet qui est encore largement utilisé en Afrique. Bien que la politique de support de Microsoft assure que les produits sont pris en charge pendant 10 ans, en avril 2014, Windows XP a atteint la fin de son cycle de vie de prise en charge, ce qui signifie que les mises à jour ne sont plus disponibles. Cela rentre dans la stratégie de Microsoft qui continue de développer de nouveaux logiciels qui répondent mieux aux besoins des clients et protègent des cyber-attaques dans un éco-systéme de plus en plus complexe.
  Dans cet esprit, l'utilisation des logiciels légitimes Windows 10 est un moyen efficace de se protéger des cybercriminels. Tandis que 43% des consommateurs n'installent pas de mise à jour de sécurité, la bonne nouvelle est, qu'avec le cloud computing, les nouveaux logiciels comme Windows 10, la sécurité est intégrée. Windows 10 inclut un moyen sans mot de passe pour vous connecter en utilisant juste un coup d'œil ou une touche, et les mises à jour sont disponibles automatiquement afin que le système soit toujours à jour. En revanche, un logiciel piraté n'obtiendra pas de mises à jour automatiques et donc sera vulnérable aux attaques;



- **augmentez vos perspectives économiques et d'affaires**
  A long terme, l'intérêt d'utiliser un logiciel authentique n'est pas seulement évident pour les consommateurs et les entreprises, mais pour les communautés et des économies entières. Un logiciel authentique stimule la croissance de l'économie et le processus de la propriété intellectuelle (PI).
  Il appartient aux consommateurs de prendre des décisions éclairées. Dans le même temps, le secteur public a la responsabilité d'éduquer ses citoyens sur les risques et également de mettre à jour la législation sur la cybercriminalité, afin de réprimer les cybercriminels et ceux qui vendent des logiciels illégaux. Avec tout ce que les économies et les collectivités ont à perdre, personne ne peut se permettre de laisser le piratage de logiciels sans contrôle.

MICROSOFT Côte d'Ivoire

Outils de protection du systéme d'information

En informatique, choisir un outil de protection dépend toujours du périmètre à sécuriser, de la valeur du patrimoine, des risques encourus et du budget disponible. Pendant que l'administrateur d'un système veille sur le parc informatique et logiciel d'une entreprise de plusieurs succursales, le simple usager ne sécurise que son seul ordinateur. L'approche, les outils et les coûts varieront selon la chaîne de valeurs produites, et la nature des biens à protéger. En somme, on ne sécurisera pas le serveur d'une banque commerciale comme un simple PC destiné à ne faire que de la bureautique. Il existe toute une panoplie d'outils de protection, propriétaires comme gratuits, allant des plus sophistiqués aux plus simples. Ceux répertoriés dans cet article à titre d'illustration ne sont pas exhaustifs.

Dossier réalisé par Kaboré BABA,
Chargé d'Etudes MENUP - Cabinet,
Expert en Sécurité des Systèmes d'Information
Certifié Microsoft, Chargé de TP à l'Université FHB

La boîte à outils de l'administrateur-système et réseau

Les pirates procèdent par un audit complet du système et du réseau ciblés en vue de recueillir des informations sur les vulnérabilités, les failles et les trous de sécurité ; l'objectif étant de les exploiter pour en tirer profit. En cas d'intrusion réussie, ils créent une backdoor (porte dérobée) dans le système pour en prendre totalement le contrôle à distance. Dans ce cas, en utilisant les mêmes outils pour auditer ses propres systèmes et réseaux, l'administrateur gagne une longueur d'avance sur les pirates.

Outils de détection de vulnérabilités

- **Retina:** cette solution payante qui détecte les vulnérabilités dans un environnement Windows est très prisée par les hackers. En plus de détecter les trous de sécurité, Retina fournit une liste «d'exploits» (programmes pour exploiter une vulnérabilité) avec un mode d'emploi simple et complet. Cet outil est extrêmement dangereux dans des mains inexpertes. Une version démo peut être téléchargée à cette adresse : https://www.beyondtrust.com/products/retina-network-security-scanner/

- **Microsoft Baseline Security Analyzer (MBSA):** outil gratuit de Microsoft, indispensable aux administrateurs, auditeurs de sécurité et autres professionnels de l'informatique, pour auditer et sécuriser les systèmes d'exploitation Windows. MBSA permet de détecter les failles et les anomalies de configuration de postes sous Windows, puis de les mettre à jour. La version française est téléchargeable à partir de ce lien : https://www.microsoft.com/fr-fr/download/confirmation.aspx?id=19892

- **LANguard:** cet outil propriétaire, autre application de prédilection des hackers, permet un audit total des différents systèmes d'exploitation et applications, pour en détecter les vulnérabilités et les failles. La version démo est disponible à l'adresse http://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard

- **Webcracker :** c'est un outil qui détecte les trous de sécurité en testant l'accès protégé des sites web et la robustesse des mots de passe.

- **Airsnort et Aircrack-ng:** ces deux outils permettent de monitorer les réseaux sans fil, de récupérer et craquer les clés WEP/WPA cryptées ainsi que les mots de passe. Ils sont disponibles aux adresses suivantes: http://airsnort.soft112.com/download.html et http://www.01net.com/outils/telecharger/windows/Utilitaire/optimiseurs_et_tests/fiches/tele124157.html

- **Nessus:** c'est un puissant et complet outil d'audit pour les distributions Linux / Unix pouvant réaliser plus de 1200 checkups de sécurité. Le reporting des informations sur les potentielles vulnérabilités se fait en formats HTML, XML, LaTeX et ASCII. A télécharger à l'adresse suivante. http://www.nessus.org/download/

- **Nmap:** cet outil pour Linux / Unix, dont la fonctionnalité principale est l'exploration et l'audit des réseaux et systèmes, est l'un des plus utilisés par les hackers. Disponible à l'adresse suivante : https://nmap.org/

Outils de surveillance du réseau

L'une des principales tâches de l'administrateur réseau consiste à contrôler les flux d'informations circulant entre le réseau interne et l'environnement externe de sorte à pouvoir les bloquer ou les autoriser.

Firewalls (pare-feu)

Les pare-feu de nouvelle génération sont à privilégier. Ces outils ont un mode opératoire qui intègre la détection et le blocage de nouvelles menaces. Leur souplesse autorise les activités des usagers (réseaux sociaux) qu'ils surveillent et protègent. Ils disposent également de mécanismes de détection d'intrusion avec des fonctionnalités plus avancées comme un IPS (Intrusion Prevention System) ainsi que des systèmes de signatures pour détecter malwares et schémas d'attaques. Les fournisseurs les plus en vue sur le marché de la sécurité informatique sont :

- **Check point** avec ses passerelles de sécurité, intégrant l'IPS, le contrôle applicatif, le filtrage d'URLs, l'anti-virus, l'anti-bot, la protection contre les attaques «zéro-day» (Sandblast), la prévention contre la perte de données (DLP : Data Loss Prevention), la mobilité grâce aux réseaux privés virtuels (VPN Virtual Private Network) hautement sécurisés;

- **Cisco** avec son Pare-feu Cisco ASA 5500-X ayant des caractéristiques similaires à celles des passerelles Cheick Point.

Outils contre les virus et les malwares (maliciels)

Les éditeurs d'antivirus proposent de plus en plus des packages comprenant un ensemble de solutions (firewalls, antimalwares, VPN) pour une protection optimale du système d'information.

- **Kaspersky Internet Security :** classé parmi les trois meilleurs antivirus en 2016, Kaspersky Internet Security est un pack complet qui prend en compte toutes les dimensions de la cybersécurité. Il adresse chacune des problématiques relatives à la sécurisation des fichiers, du courrier, du réseau Internet, de la messagerie instantanée, des applications, des transactions bancaires et du Cloud. Il est doté d'un pare-feu qui surveille le réseau, d'un anti-spam, d'un anti-phishing, d'un anti-bannière, d'un contrôle parental et d'un système de prévention d'intrusions. Difficile de trouver un outil plus complet avec une excellente proportion qualité-prix.
Beaucoup d'antivirus présentent des offres similaires tels que Bitdefender, Norton, McAfee Security, AVG, Panda, Eset, Nod 32, etc.

- **Persystent Suite :** C'est un puissant outil de restauration de système. Si un poste de travail de l'entreprise est victime d'un virus à partir d'un fichier infecté, Persystent Suite se charge de restaurer le système en quelques secondes et de le ramener au dernier état de bon fonctionnement, dans quelle que circonstance que ce soit. La technologie unique d'auto-récupération Persystent Suite offre la capacité de réduire la complexité du support aux utilisateurs, de diminuer sensiblement les dépenses liées aux opérations manuelles de reconstruction des systèmes. Elle peut même accomplir les tâches de récupération d'environnement, que le système soit connecté ou non au réseau. Disponible à cette adresse : http://www.cht-supply.com/utopic-software.html

Protection d'un ordinateur personnel

Il est absolument nécessaire d'installer un antivirus à jour. Opter pour une solution payante, mais à défaut, les fonctions basiques des antivirus gratuits offrent une protection minimale. Ajouter au dispositif un pare-feu et un antimalware donne une sécurité acceptable.

- **ZoneAlarm Mobile Security (https://www.zonealarm.com/fr/) :** cette solution gratuite de pare-feu est couplée à un antivirus qui protège les terminaux de toutes sortes de menaces. L'outil protège tout type de terminal (PC, portable, tablette, smartphone) contre le piratage informatique, les connexions Wi-Fi vulnérables et les applications malveillantes. ZoneAlarm Mobile Security signale l'existence de processus suspects, détecte les réseaux Wi-Fi dangereux, scanne l'appareil pour trouver les applications infectées ainsi que les mises à jour nuisibles et alerte des risques potentiels.

- **Avast antivirus (www.avast.com/fr) :** c'est un des meilleurs programmes antivirus gratuit pour PC, ainsi que pour mac, et un des plus populaires pour les utilisateurs de Windows. Il est totalement gratuit pour les particuliers à titre d'utilisation non-commerciale. Par ailleurs, Avast fournit l'ensemble des outils nécessaires de protection. Il comprend plusieurs boucliers de protection, c'est-à-dire l'analyse au moment du démarrage, une extension pour vérifier la fiabilité des sites internet, la protection contre les scripts et les logiciels malveillants, la protection en temps réel des fichiers et des e-mails. La protection est basée sur le Cloud et il possède une magnifique interface utilisateur.

- **Ad-Aware (www.lavasoft.com/free_download/trial/) :** cet antivirus gratuit demeure une solution très intéressante. Il offre une impressionnante panoplie d'outils de protection qui sont l'anti-rootkit, l'antispyware/Adware, la protection antivirus, les mises à jour automatiques, la protection en temps réel, la protection internet, la navigation sécurisée. Toutes ces options sont accessibles via son interface simple, facile et conviviale. Il est parfait pour les utilisateurs débutants qui apprécieront son design cohérent et simple. Il possède une grande variété de fonctionnalités qui peuvent être sélectionnées facilement à l'aide d'icônes claires.

A ces produits de sécurité gratuits et efficaces, on pourrait ajouter AVG, Avira, Panda Cloud Antivirus, Qihoo 360, Total Security, Comodo, etc. (http://comparatifantivirus.net/meilleur-antivirus-gratuit/).

Lorsque l'antivirus est seul, il faut lui adjoindre un firewall couplé d'un antispyware, et s'assurer qu'il n'y a aucun conflit de type « faux positif » entre les outils de sécurité installés.

- **Windows 10 Firewall Control**
  Le pare-feu intégré à Windows 10 permet d'empêcher les utilisateurs ou logiciels non autorisés (comme les vers) d'accéder à l'ordinateur depuis un réseau ou Internet. Par défaut, le pare-feu de Windows est activé. Néanmoins, certains réglages peuvent être nécessaires pour assurer une sécurité maximale suivant le point d'accès à Internet (maison, bureau, endroit public). Pour les utilisateurs avertis, une version avancée du pare-feu offre des réglages plus précis sur les logiciels accessibles depuis Internet, mais également sur ceux qui essaient de se connecter depuis l'ordinateur à Internet.

- **PC Tools Firewall Plus (http://www.pctools.com/)**
  Disponible gratuitement et en français, PC Tools Firewall Plus est un pare-feu personnel qui protège un ordinateur en empêchant les utilisateurs non autorisés de s'y connecter, que ce soit depuis un réseau ou via Internet. En effet, en surveillant les applications se connectant au réseau, Firewall Plus est capable de bloquer les chevaux de Troie, les portes dérobées, les enregistreurs de frappe et autres logiciels malveillants qui risquent d'endommager l'ordinateur et de voler des informations personnelles. PC Tools Firewall Plus est une technologie avancée qui s'adresse à tout le monde, pas uniquement aux experts. Une protection avancée contre les attaques et l'exploitation des failles est activée par défaut, mais les utilisateurs expérimentés peuvent créer leurs propres règles avancées de filtrage des paquets (IPv6 est pris en charge) afin de personnaliser la protection réseau.

- **Spybot Search & Destroy (Anty Spyware: https://www.safer-networking.org/fr/)**
  Le logiciel fait une recherche dans la base de registre et dans l'arborescence des fichiers des éléments considérés comme sensibles. La plupart de ceux-ci sont commentés ce qui facilite la prise de décision : «je supprime» ou «je garde». En plus de la détection des logiciels espions, Spybot - Search & Destroy nettoie également les chevaux de troie, les keyloggers, les cookies, les enregistreurs d'activité etc.

De très bons logiciels anti-espion gratuits fonctionnent sur cette base. On peut citer, Spyware Terminator, SUPERAntiSpyware Free Edition, IObit Malware Fighter, AdwCleaner, Malwarebytes Anti-Malware, etc.

Une des faiblesses les plus courantes dans les communications consiste à émettre et à recevoir des informations en clair, c'est-à-dire faire circuler des données non chiffrées. Il suffit pour un pirate d'intercepter la communication à l'aide d'un renifleur (sniffer) et bonjour les dégâts. Crypter les communications et les données avec des outils adaptés permet de les sécuriser même en cas de vol ou de perte de l'ordinateur ou du dispositif de stockage. Le principe du chiffrement des données est le même pour tous les logiciels gratuits cités dans ce chapitre: créer un coffre-fort numérique, une sorte de « coffre-fort secret », sur l'ordinateur qui n'est visible que pour la personne qui connaît le mot de passe et l'emplacement du fichier sur l'ordinateur. Pas besoin d'avoir des connaissances techniques compliquées sur la cryptographie. Les outils suivants permettent de sécuriser totalement le contenu des ordinateurs et des disques durs externes: TrueCrypt, BoxCryptor, AxCrypt, BitLocker, VeraCrypt.

Quant au chiffrement des mails, un simple modules complémentaire, comme Mailvelope, sur le navigateur Firefox ou Chrome suffit pour crypter les e-mails afin que personne, en dehors évidemment de l'émetteur et du destinataire, ne puisse lire les messages émis.

C'est connu, les outils techniques à eux-seuls ne suffisent pas à sécuriser un système d'information qui, en réalité, présente une complexité multidimensionnelle. Les dimensions techniques, managériales et surtout humaines doivent être combinées pour atteindre une sécurité alignée sur les objectifs de l'entreprise.

Dans la chaîne de sécurité, le facteur humain est le maillon le plus faible car la sécurité implique des contraintes, des obligations et des principes à respecter strictement. C'est pourquoi former, informer et sensibiliser les usagers du système sur les risques qu'ils courent, les dangers qui les guettent et les méthodes malveillantes utilisées par les pirates, est la première étape à franchir en termes de sécurité informatique. Car à quoi servirait le plus puissant des outils de sécurité s'il n'est pas régulièrement mis à jour ? Que vaut une stratégie de sécurité avec des usagers ayant des mots de passe de types 12345678, azerty ou abcdefe, etc. ? Cela reviendrait à blinder la porte d'entrée d'une maison alors que les fenêtres sont grandement ouvertes.

La sécurité Informatique est à la fois une question d'utilisation d'outils adaptés, d'organisation et surtout de bon sens.

Défi de la sécurisation des usages mobiles et transactions Mobile Money

Leader dans les solutions de l'ère digitale, MTN est consciente que la cybersécurité est désormais une activité stratégique. Pour MTN, il est clair que la sécurité concerne tout le monde et que les attaques ne visent pas que les autres. La multiplication des usages (smartphones, tablettes, ordinateurs portable,…), les réseaux sociaux, le cloud computing et surtout la dématérialisation des moyens de paiement à travers l'introduction de la monnaie virtuelle (Mobile Money) sont autant d'alertes et de sources de menaces, non seulement pour les clients finaux, mais aussi pour les entreprises et tous les acteurs et partenaires.

- Quelles sont aujourd'hui les menaces réelles et latentes dans ce monde digital ?
- Quels sont les éléments déterminant la stratégie de sécurité de MTN Côte d'Ivoire ?
- Quelles sont les initiatives mises en œuvre par MTN-CI pour lutter contre la cybercriminalité ?

Les menaces réelles aujourd'hui

Les menaces sont de plusieurs ordres, partant des sources internes aux cibles les plus exposées telles que les clients finaux, les acteurs de Mobile Money :

- usage frauduleux des services data;
- divulgation d'informations sensibles des clients;
- usurpation des comptes des abonnés Ingénierie sociale : vol de crédit Mobile Money;
- authenticité de l'identité des abonnés Etc.

Les éléments de stratégie

La sécurité fait partie intégrante des activités et de l'organisation de MTN-CI. Avec le soutien et l'engagement du Groupe MTN et de la haute direction de MTN-CI, la sécurité est prise en compte au niveau de la stratégie et déclinée dans les différents plans opérationnels de sorte à s'assurer qu'elle est prise en compte dans les solutions offertes aux clients et aux entreprises. Par conséquent, les exigences de sécurité sont intégrées depuis la phase de conception des produits et services de MTN-CI :

- exigences légales et réglementaires Normes internationales et bonnes pratiques;
- exigences liées à la politique de sécurité interne à MTN Group, tant au niveau organisationnel qu'au niveau technique;
- pour la mise en place effective et efficace d'une politique de sécurité de l'information, MTN-CI a dédié une division en charge de la sécurité à tous les niveaux de l'entreprise, appuyée par des experts du Groupe MTN.

Le déploiement du système de gestion de la sécurité, ayant pour ambition d'inculquer une culture de la sécurité à tous les acteurs, implique aussi bien les agents de MTN-CI, ses partenaires directs de vente, que les fournisseurs et toutes les parties prenantes.

En plus des dispositions techniques prises au travers des 7 périmètres de la sécurité (sécurité des données, sécurité des applications, sécurité des équipements et serveurs, sécurité des terminaux mobiles, sécurité du réseau local, sécurité de l'accès physique, sécurité des opérations), le cadre de gestion de la sécurité de MTN-CI tire son efficacité de la cohérence de son programme de sensibilisation qui vise les employés, les partenaires, les fournisseurs ainsi que les clients finaux :

- les fournisseurs pour garantir que les services qui vont être délivrés aux clients intègrent un minimum de sécurité exigé par la politique de sécurité et les dispositions légales et règlementaires;
- les partenaires de vente surtout pour les sensibiliser afin de les rendre moins vulnérables;
- les clients pour réduire leur niveau de prévalence aux risques d'hameçonnage et d'ingénierie sociale.

Les initiatives mises en œuvre par MTN-CI

MTN-CI a perçu que le maillon le plus faible à adresser concerne la sensibilisation, la coordination et la coopération de tous les acteurs nationaux et internationaux dans le cadre de la lutte contre la cybercriminalité.

Ainsi, au niveau international, une équipe interne interagit avec CI-CERT piloté par l'ARTCI. Cette équipe traite les cas d'alertes et incidents d'attaques de cyber sécurité initiées depuis le réseau de MTN Côte d'Ivoire vers les ressources d'autres utilisateurs du monde.

Au niveau national, les initiatives suivantes sont prises :

- MTN-CI travaille en coordination avec l'ARTCI pour une mise en œuvre efficace de la protection des données à caractère personnel;
- MTN-CI met en œuvre la fixation des adresses IP des clients data de sorte à permettre la traçabilité des activités menées sur Internet;
- MTN-CI travaille avec les autorités judiciaires, la police et la gendarmerie en fournissant des données nécessaires pour la conduite des investigations et des enquêtes;
- MTN-CI a mis à disposition une adresse email sur son site web officiel afin de faciliter la remontée des cas de cybercriminalité;
- MTN-CI participe de manière active à la sensibilisation des populations à travers les journées d'actions citoyennes (21 jours d'actions citoyennes).

MTN Côte d'Ivoire

La sécurisation du paiement e-Banking, un changement de paradigme

Le besoin de mobilité grandissant, un accès des utilisateurs au réseau financier mondial par la technologie sans-fil : téléphones cellulaires, ordinateurs portables, etc. est devenu nécessaire. Les services bancaires offrent aux clients la possibilité de payer leurs factures et de transférer des fonds de compte à compte.

« La banque électronique », e-Banking ou Internet banking permet d'accèder aux services bancaires depuis une interface interactive, par exemple un navigateur web. Sa disponibilité permet l'accès aux comptes, d'effectuer des transactions ou d'obtenir des informations financières. La connexion se fait généralement par accès sécurisé. La banque électronique est un mode d'accès interactif à des banques ayant des agences bancaires, se distinguant de la banque directe qui est une banque sans guichet totalement en ligne.

Les institutions financières doivent adopter une interopérabilité des standards et des protocoles comme le Extensible Markup Language (XML) afin de faciliter les échanges de données entre divers utilisateurs. Les mécanismes de commerce électronique fournis sont les procédures de débits et crédits, la facturation, les chèques électroniques… gérés par l'Automated Clearing House (ACH). Puisque l'identification papier réduit la vitesse des transferts électronique, il a été mis en place les numéros d'identification personnels (PIN), associé à des infrastructures à clés publiques (PKI) et les cartes à puce. La syndication peut aider la représentation, la gestion et l'analyse de différents comptes à partir d'ID et mots de passe.

De la sécurité des transactions électroniques

En matière de transactions électroniques, la sécurité des transactions doit rester une préoccupation permanente. Les technologies pour la sécurisation des transactions électroniques visent à prévenir, détecter et limiter les attaques malveillantes à l'encontre des systèmes, des contenus, des services et des personnes.

Le changement de paradigme en matière de sécurisation du paiement e-Banking

La question qui est toujours posée est : « l'e-Banking est-il sécurisé ? ». En effet, le danger représenté par les tentatives de fraude sur Internet augmente. Le simple fait de se rendre sur un site internet comporte un risque. Ainsi, quiconque navigue sans protection sur Internet, consulte des e-mails suspects et visite des sites douteux, risque dans le cas le plus grave de voir son ordinateur infecté en quelques minutes par des virus, des vers, des chevaux de Troie ou par d'autres types de programme malveillants.
L'e-Banking nécessite donc de sécuriser le système au maximum. L'accent est mis particulièrement sur une gestion plus complexe des mots de passe des usagers, et à la limitation des accès aux ressources. Les normes de sécurité sont plus sévères et font l'objet de contrôles réguliers effectués par des experts en sécurité renommés et indépendants.

L'aspect juridique de la sécurité

La sécurité ne doit pas seulement être traitée d'un point de vue des systèmes informatiques des banques mais l'aspect juridique et légal est tout aussi important en cette matière. Face au développement des nombreuses possibilités qu'offre Internet, aux propositions de services en ligne et à l'accroissement du volume des transactions électroniques, et pour mieux sécuriser le cyberespace et les activités qui s'y déroulent, le gouvernement ivoirien a pris les devants en faisant adopter des lois pour encadrer tout cela sur le plan juridique et légal, dès 2013. Ce sont : la loi sur les transactions électroniques, la loi relative à la protection des données à caractère personnel, la loi sur la lutte contre la cybercriminalité.

Le comportement humain

Force est de reconnaître que pour la sécurité des systèmes informatiques et particulièrement des données, mêmes les technologies les plus pointues ne suffisent plus. En effet, selon certains spécialistes du domaine, un tiers des accidents de sécurité sont le fait de collaborateurs de l'entreprise. Ceci est bien résumé par le dicton qui dit que «*dans la chaîne de sécurité, le facteur humain est le maillon le plus faible*». La prise en compte de la dimension humaine en matière de sécurité apparaît donc comme un point essentiel que commencent à intégrer les entreprises et particulièrement celles évoluant dans le e-Banking.
Quelques règles simples mais utiles à l'attention des usagers des services de «e-Banking» :

Au-delà de tous les dispositifs de sécurité, et quel que soit le degré de leur complexité, il apparaît que le point faible de tout cela reste le comportement de l'usager lui-même pour une grande part. En matière de sécurité, des gestes simples contribuent à assurer une bonne sécurité de l'ensemble. Aussi, pour l'utilisateur de l'e-Banking l'observation de ces points suivants (non exhaustifs) contribue à lui épargner de désagréables surprises:

- utilisez un mot de passe sûr et ne le donnez jamais à quelqu'un d'autre;
- ne sauvegardez jamais vos données de connexion telles que le numéro de contrat, le mot de passe ou les codes complémentaires;
- saisissez à chaque fois l'URL de l'e-Banking manuellement dans votre navigateur et n'utilisez pas de liens à partir des favoris;
- soyez attentif lorsque vous utilisez l'e-Banking;
- vérifiez régulièrement les paiements, ordres permanents, relevés de compte, etc.;
- effectuez les mises à jour de vos navigateurs, logiciel de sécurité et système d'exploitation pour éviter les failles de sécurité;
- il n'est en aucun cas permis de saisir le numéro de contrat, le mot de passe ou le complément de mot de passe dans des boutiques en ligne;
- utilisez le bouton de Déconnexion de l'e-banking de manière systématique pour clore une session correctement.

Lorsque les fondamentaux en termes de cybersécurité ou de sécurité des systèmes d'information sont mis en œuvre, d'une manière générale, l'e-Banking offre une flexibilité et une meilleure gestion des comptes. Un des atouts majeurs est la disponibilité 24h sur 24h, 7 jours sur 7 des services bancaires à la clientèle et de fait, les clients n'ont plus besoin de se rendre dans une banque, ni de faire la queue pour effectuer les opérations, au contraire, elles sont réalisées instantanément, à ceci vient s'ajouter le fait que le client a le sentiment de contrôler la gestion de son compte.

Ainsi, les contraintes liées aux heures et aux jours d'ouverture des agences bancaires sont annihilées par le fait même. Le client a donc la possibilité d'effectuer rapidement et aisément des opérations bancaires depuis son domicile ou son bureau, et de partout dans le monde à n'importe quelle heure, pour peu qu'il dispose d'une connexion Internet.

CONTAYON Eric
Conseiller Technique
Ministère de l'Economie Numérique et de la Poste

4e Congrès de l'UPU en 2020

Le lobbying de Bruno Koné et Mabri Toikeusse auprès des ambassadeurs

Les autorités ivoiriennes ont annoncé récemment la candidature de la Côte d'Ivoire à l'organisation du Congrès mondial de l'Union Postale Universelle (UPU) en 2020. Selon le porte-parole du gouvernement, Bruno Koné, qui intervenait lors d'une rencontre avec le corps diplomatique accrédité en Côte d'Ivoire, le pays reste le seul Africain dans la course après le retrait de la Tunisie et de l'Ethiopie.
«La Côte d'Ivoire est la candidate unique de l'Afrique pour l'organisation de cet événement mondial. Les pays africains ont fait bloc derrière notre pays», a-t-il noté. De son avis, la Côte d'Ivoire a de fortes chances d'être désignée au cours du prochain congrés mondial de l'UPU à Istanbul pour organiser cet événement.
«Si l'organisation nous revient, ce serait une première en Afrique depuis 1932», a fait remarquer Bruno Koné. Pour sa part, le ministre ivoirien des Affaires étrangères, Albert Toikeusse Mabri, a souligné que l'organisation du congrès en terre ivoirienne sera une belle victoire pour la diplomatie du pays. Lors d'une rencontre officielle de l'UPU tenue à Genève , le Premier ministre ivoirien, Daniel Kablan Duncan, a exprimé la volonté de la Côte d'Ivoire de demeurer parmi les acteurs du changement *«dans ce monde en constant mouvement»* et de contribuer à la construction de la Poste du futur.
«La Côte d'Ivoire, après les deux rendez-vous manqués, le Congrès mondial de l'UPU en 2004 et la Conférence stratégique de l'UPU en 2014, serait très heureuse et honorée d'accueillir le congrès mondial de l'UPU en 2020», avait-il souligné. Pour faire face aux nouveaux enjeux du marché concurrentiel, la Poste ivoirienne a engagé la diversification de ses activités, en accordant une place de choix à l'utilisation des technologies de l'information et de la communication. Au cours d'une récente rencontre à Abidjan, des responsables de l'UPU avaient exprimé l'engagement de l'institution à apporter un appui à la dynamisation de la Poste ivoirienne. Le Congrès de l'UPU constitue l'un des plus grands événements dans le monde. L'UPU regroupe 192 Etats.

L'Afrique soutient la candidature de la Côte d'Ivoire

Les ministres africains en charge de la Poste, réunis les 22 et 23 juillet 2016 à Yaoundé au Cameroun, ont décidé, par l'adoption d'une résolution, de s'unir autour de la candidature de la Côte d'Ivoire pour l'organisation du Congrès de l'Union Postale Universelle (UPU) 2020. C'était dans le cadre de la 9ème Conférence des Plénipotentiaires de l'Union Panafricaine des Postes (UPAP). Représentant la Côte d'Ivoire, le Ministre de l'Economie Numérique et de la Poste, Porte-parole du gouvernement, Bruno Nabagné KONÉ, a dit sa satisfaction et traduit la gratitude du gouvernement ivoirien aux Etats membres de l'organisation pour leur soutien à la candidature de son pays. *«Nous l'avons clairement dit, l'organisation de ce Congrès de l'UPU est un événement qui concerne toute l'Afrique. Et nous sommes heureux de voir le soutien de toutes les 5 régions postales du continent»*, a-t-il dit.
La Côte d'Ivoire a été reconduite au Conseil d'Administration de l'UPAP, l'organisation postale africaine.

Poste de Côte d'Ivoire

Isaac Gnamba Yao succède à Konaté Mamadou

La cérémonie de passation des charges entre le DG sortant de la Poste de Côte d'Ivoire, Konaté Mamadou, et le nouveau responsable de ladite institution, Isaac Gnamba Yao, s'est déroulée le jeudi 28 juillet 2016 dans les locaux de la direction en présence du PCA, Denis Kah Zion, et des représentants du ministère de la Poste et de la primature.
Denis Kah Zion a félicité Konaté Mamadou pour sa nomination au titre de conseiller du Conseil de Régulation à l'ARTCI et l'a remercié pour son dévouement à faire de la Poste de Côte d'Ivoire un outil moderne au service du développement.
Pour sa part, Konaté Mamadou a témoigné sa gratitude à l'ensemble du personnel qui l'a aidé dans sa tâche durant son mandat .
Quant à Isaac Gnamba Yao, le nouveau DG, il a remercié le ministre pour son soutien depuis son entrée à la Poste et a promis de redoubler d'ardeur pour être à la hauteur de la mission à lui confiée.

Régulation/ARTCI

Deux nouveaux membres du Conseil de régulation prêtent serment

Le Président de la République a nommé par décret trois nouveaux membres de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire (ARTCI). Deux membres - Paul Kangah et Mamadou Konaté - ont prêté serment devant la Cour d'Appel d'Abidjan-Plateau. Les deux se sont engagés à remplir leur mission avec rigueur, loyauté et intégrité conformément aux lois et réglements en vigueur. Ces nouveaux membres remplacent Demba Diop, André Braud Mensah et Pierre Lamine en fin de mandat, pour un exercice de six ans au sein de l'instance de régulation du secteur des télécommunications ivoiriennes.

Prix du meilleur partenaire Microsoft

INOVA réédite l'exploit

En 2015, la société d'ingénierie et de service numérique INOVA se voyait décerné l'Awards pour la Côte d'Ivoire du *''Microsoft Partner of the Year 2015''* à Orlando aux Etats Unis lors de la conférence mondiale des partenaires Microsoft. Elle avait aussi remporté l'Awards du *'' Microsoft Innovative Technology for Good Citizenship Partner of the Year'' pour la zone Afrique de l'Ouest, de l'Est et du Centre.Cette année, INOVA réédite l'exploit en remportant une fois de plus l'Awards du ''Microsoft Partner of the Year 2016''* pour la Côte d'Ivoire et celui du ''Windows Partner and Devices'' pour la zone Afrique de l'Ouest, de l'Est et du Centre. Pour M. Patrick M'Bengue, DG de INOVA *«Ces différents prix récompensent tous les efforts consentis pour que les clients puissent accéder à des applications de qualité, des formations de pointe et des services IT avec la plus grande expertise»*.

ACTUAL-IT

LE MAGAZINE D'INFORMATION
DE L'ÉCONOMIE NUMÉRIQUE