LA RÉFÉRENCE DU NUMÉRIQUE EN AFRIQUE

ciomag.com

N°73 I MARS - AVRIL 2022

DATA & CYBER-RISQUES

Une réponse **africaine** trop timide ?

Rubrique agritech

Tendance, challenge et retour d'expériences

ZONE CFA AVION : 3000 FCFA - ZONE CFA SURFACE : 2000 FCFA - MAR : 55DH - FRANCE MÉTRO : 4,50€ - ESP : 4,50€ - CANADA : 8$ CAD

Édito

Mohamadou DIALLO
Fondateur et Directeur Général de Cio Mag

La cybersécurité, une guerre dans une guerre

Jamais, dans l'histoire contemporaine, le monde n'a fait face à autant de risques de cyberattaques commanditées par des États. A fortiori depuis l'invasion russe en Ukraine. Incontestablement, ces vagues de cyberattaques auront des répercussions sur nos organisations. Au-delà des récits d'affrontements sur de nombreux théâtres d'opérations, avec son lot déplorable de pertes en vie humaines et de populations déplacées, au-delà des nouvelles formes de trafic engendrées par les sanctions économiques, une autre forme de guerre fait son apparition. Une guerre moderne. C'est aussi ce qui se passe dans la finance digitale, notamment avec les cryptomonnaies.

Dans ce conflit, le recours à la cryptomonnaie est inédit. Et son succès repose sur le principe de monnaie décentralisée, fondée sur des échanges anonymes. Elle ne dépend d'aucune banque centrale et ne porte l'étendard d'aucun pays. De ce point de vue, le Bitcoin, qui est la plus importante des cryptomonnaies, n'est ni pro-ukrainien, ni pro-russe.

Et d'un camp à l'autre, son usage n'est pas le même. Pour le gouvernement ukrainien, il s'est caractérisé par un appel aux dons, qui a permis de collecter, en une semaine, plus de 50 millions de dollars en cryptomonnaie.

Du côté russe, son usage sera tout autre. Il consistera à contourner les sanctions économiques contre l'Etat, les banques privées et les oligarques, suite à leur bannissement du système international Swift de compensation interbancaire. Mais pas seulement. Il permettra de faire face à la dépréciation du rouble, qui a chuté jusqu'à 30 %. On note d'ores et déjà une ruée vers le Bitcoin, considéré comme une valeur refuge.

En conséquence, l'adoption de Bitcoin par les deux camps - ou dans les deux blocs (Est & Ouest) - pourrait accélérer l'acceptation des cryptomonnaies comme devises et leur intégration dans l'économie réelle. Et pour que cette adoption soit effective, il faut, au préalable, que les infrastructures de paiement reconnaissent et acceptent les paiements en Bitcoin, de façon à démocratiser les usages.

Et l'Afrique dans tout cela ?

L'Afrique ne peut rester en marge de cette situation, même si cette guerre semble lointaine. L'adoption d'une monnaie décentralisée pourrait favoriser rapidement et massivement l'inclusion financière de plusieurs millions d'Africains. Mais, les conséquences peuvent être importantes du fait de la fragilité et de la grande vulnérabilité des systèmes de protection des données critiques. C'est le thème de l'enquête, qui a été menée par nos équipes, dans ce numéro spécial. Et la plupart des acteurs interviewés ont mesuré l'importance des enjeux.

L'accroissement de la connectivité expose davantage à des vulnérabilités de toute sorte. Et pour vous permettre de suivre ces actualités au quotidien, la rédaction de Cio Mag a décidé de consacrer un cahier spécial, pour être au plus près de l'actualité de la cybersécurité et de ses enjeux au quotidien.

Bonne lecture.

SOMMAIRE

N°73 MARS - AVRIL 2022

ÉVÉNEMENT
Mobile World Congress : le futur à nos portes

AGRITECH
Quelles tendances pour demain ?

DATA ET RISQUES NUMÉRIQUES
Une cyberurgence africaine

cio mag.com — LA RÉFÉRENCE DU NUMÉRIQUE EN AFRIQUE

Cio Mag est édité par SAFREM Sarl

Directeur de publication :

Mohamadou DIALLO Mohamadou.diallo@cio-mag.com

Ont contribué à ce numéro

Mohamadou DIALLO :

Directeur de publication - Rédacteur en Chef.

Coordination de rédaction

Camille Dubruelh (France)

Rédaction :

Véronique Narame (France);

Anselme Akeko (Côte d'Ivoire); Aurore Bonny (Cameroun);

Michaël Tchokpodo (Bénin); Souleyman Tobias (Togo);

Enock Bulonza (RDC)

Représentations de Cio Mag :

Côte d'Ivoire : Anselme Akeko : anselme.Akeko@cio-mag.com
Tél: +225 08 56 47 26

Cameroun : Aurore BONNY : aurore@cio-mag.com

Sénégal : Abdoulaye DIALLO : abdoulaye33@hotmail.com

Tél : +221 77 595 50 02

Togo : Souleyman TOBIAS : tobias.carlos@cio-mag.com

Tel : +228 90 26 38 54

Bénin : Michaël TCHOKPODO : michael@cio-mag.com

Régie Publicitaire et Abonnements :

info@cio-mag.com

www.cio-mag.com/sabonner

Direction artistique : Cio Mag
Impression : Rotimpres, Aiguviva Espagne
N° Commission paritaire 1110 T89651 N Dépôt légal Juin 2013

L'AFRIQUE EN CHIFFRES

5,92 milliards $

Selon le cabinet Verified Market Research, le marché de la cybersécurité au Moyen-Orient et en Afrique, qui était évalué à 5,92 milliards de dollars en 2018, devrait atteindre 17,30 milliards de dollars d'ici à 2026.

5%

35% des investissements en cybersécurité sont dédiés à la sécurité des infrastructures IT. Et seulement 5% sont dédiés à la sécurité des données, à la détection des incidents, au suivi des menaces ou à la gestion des identités et des accès. (Source : Rapport Deloitte sur la cybersécurité 2021)

573 millions $

En 2016, la cybercriminalité a coûté 36 millions de dollars à l'économie kényane, 573 millions à l'économie sud-africaine et 500 millions à l'économie nigériane. (Source : Rapport Deloitte sur la cybersécurité 2021)

56%

En Afrique, les revenus générés par le contenu audiovisuel accessible en streaming et à la demande s'élèveront à 1,66 milliard de dollars en 2027, contre 476 millions de dollars en 2021. L'Afrique du Sud et le Nigeria représenteront ensemble 56 % du total. (Source : Rapport du cabinet américain Digital TV Research)

91%

Face à des problèmes de ransomwares, 71 % des responsables IT (sur les 1700 interrogés à travers le monde) ont pu restaurer 91 % ou plus de données affectées. 92 % d'entre eux n'ont subi aucune perte financière à cause des temps d'arrêt provoqués par les ransomwares. Et 85 % ont limité leur coût moyen de reprise d'activité à moins de 25 000 $. (Source : Rapport Veeam, Rétrospective sur les ransomwares en 2021)

Moins de 200.000 €

Selon une étude de Deloitte sur la maturité cybersécurité 2021 en Afrique francophone, 66% des entreprises investissent moins de 130 millions de FCFA (200.000 €) par an dans la cybersécurité.

Ils et elles ont dit ...

« L'inauguration de ce centre est une source de joie et de fierté légitime pour les Congolais et au-delà, pour la jeunesse africaine tout entière. Car, il constitue une véritable vitrine de l'Afrique décomplexée et émergente, telle que nous le voulons en termes de technologies innovantes, a l'instar de l'Intelligence artificielle. »

Léon Juste Ibombo, *Ministre congolais des Postes, des Télécommunications et de l'Economie numérique, lors du lancement du Centre africain de recherche intelligence artificielle (CARIA), le 24 février 2022.*

« La densité de la connectivité et la puissance de calcul déterminent la force de l'économie numérique, mais celle-ci doit également conserver sa vitalité dans la durée. Nous devons donc considérer un nouvel élément : la réduction des émissions de carbone . »

Guo Ping, *président tournant de Huawei, lors du MWC de Barcelone, le 1er mars 2022.*

« Plus le monde sera connecté, plus il sera sûr. Et il prendra davantage soin de la planète. Nous pensons qu' en utilisant les technologies mobiles, nous pouvons réduire les émissions de CO2 et de carbone de 11 gigatonnes, d' ici à 2030. »

Mats Granryd, *directeur général de la GSMA, lors du MWC de Barcelone, le 28 février 2022.*

« Les investissements dans l'écosystème africain des start-up se développent à un rythme incroyable. Selon l'Organisation de coopération et de développement économiques (OCDE), il existe aujourd'hui plus de 640 hubs technologiques actifs à travers toute l'Afrique. Et ils contribuent fortement à accélérer l'innovation et à créer de l'emploi, en particulier auprès des jeunes . »

Wael Elkabbany, *Directeur général de Microsoft Africa Transformation Office, en mars 2022.*

« Comme tous les domaines, le milieu des arts et de la culture doit être dynamique et doit toujours chercher à s'adapter aux différentes mutations sociales, sociologiques et économiques. Les créateurs de contenus doivent s'inscrire dans l'innovation, notamment celle de la transformation digitale . »

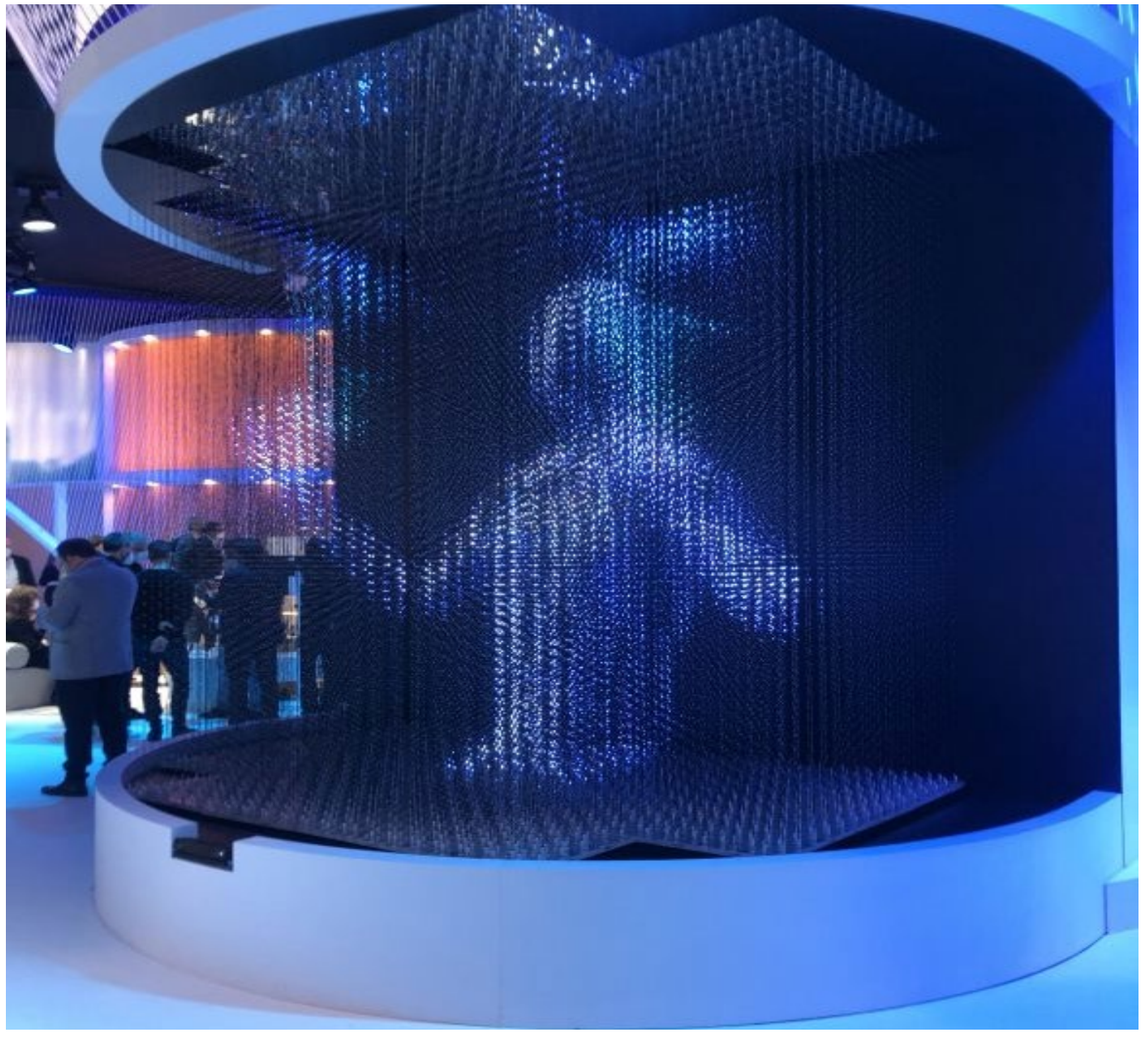
Patrick Achi, *Premier ministre ivoirien, à l'ouverture du Marché des Arts et du Spectacle d'Abidjan (MASA), le 5 mars 2022.*

ÉVÉNEMENT

Mobile World Congress : le futur à nos portes

Le MWC est le plus grand événement mondial consacré au mobile. Il s'est tenu du 28 février au 3 mars, à Barcelone, en Espagne. Exposants et public sont venus des quatre coins du globe pour échanger et observer les dernières technologies. Cette édition 2022, qui a fait la part belle à la 5G et aux questions environnementales, donne un aperçu du monde de demain. Si les Africains ont encore été absents parmi les entreprises leaders de la Tech Mobile, les représentants des institutions publiques ont fait le déplacement pour garder un œil sur les innovations et s'en inspirer pour construire un modèle de développement numérique adapté au continent. Reportage.

Camille Dubruelh



« La connectivité mobile a changé la façon dont nous vivons. Aujourd'hui, nous entrons dans l'ère de la 5G. Comment pouvons-nous construire un futur meilleur dans ce contexte ? ». C'est pour proposer et trouver des réponses à cette question, soulevée par la GSMA, que quelque 60 000 personnes, venues du monde entier, ont arpenté les immenses couloirs du MWC. Le plus gros salon mondial consacré au mobile, qui s'est tenu du 28 février au 3 mars, à Barcelone, était très attendu, après une édition 2021 réduite au minimum et une édition 2020 annulée, pour cause de crise sanitaire.

Sur des milliers de mètres carrés, plus de 1500 exposants, venus d'environ 180 pays, ont présenté leurs produits, leurs services et leurs innovations : applis, logiciels, mobiles, attractions de réalité augmentée, démonstrations d'habitats connectés ou encore solutions cloud.

Le village Huawei a sans doute été le plus impressionnant de tous. Le géant chinois est venu présenter sa nouvelle stratégie « Lighting up the future », comme une nouvelle page qui s'ouvre après deux ans de pandémie. *« Le MWC est une vitrine technologique et une plateforme de partage entre les clients du monde entier. Nous avons l'occasion de montrer et démontrer notre innovation, nos produits, nos solutions, mais aussi de partager les retours d'expériences »*, a confirmé Mounir Soussi, Vice-président Cloud & IA de Huawei Northern Africa.

Plus que les équipements, Huawei compte sur ses technologies, notamment en termes de Cloud, pour booster sa croissance et poursuivre sa stratégie de mondialisation. Grâce à cet investissement, le groupe espère remodeler ses théories fondamentales, autant que l'architecture et les logiciels qui sous-tendent à son industrie. Il escompte un accroissement de sa compétitivité à moyen et long terme et la durabilité, à plus long terme, de l'industrie des TIC, laquelle se doit d'être « green ».

« La densité de la connectivité et la puissance de calcul déterminent la force de l'économie numérique, mais celle-ci doit également conserver sa vitalité dans la durée. Nous devons donc considérer un nouvel élément : la réduction des émissions de carbone », a assuré Guo Ping, président tournant de Huawei. Le groupe adhère ainsi à la stratégie « *More Bits, Less Watts* », pour un monde technologiquement plus avancé, mais moins pollué. Car

Huawei en est convaincu, grâce à l'innovation, le secteur des TIC est en mesure d'aider d'autres industries à réduire leur propre empreinte carbone.

6G et monde virtuel

Les prévisions montrent que plus de 50 % du PIB mondial sera numérisé en 2022. Et le mobile sera sans aucun doute la pierre angulaire de ce développement. En 2022, le cloud est donc sur tous les agendas, tout comme la 5G. Ces technologies doivent servir à booster les compétitivités des pays. Mats Granryd, directeur général de la GSMA, a ainsi rappelé que les connexions 5G devraient atteindre 1 milliard d'ici à la fin de l'année. *« C'est un domaine de croissance transfrontalier, avec un grand nombre d'opportunités. Bien sûr, c'est un effort conjoint. Les gouvernements et les décideurs doivent être informés et doivent être encouragés à soutenir le développement rapide et la croissance durable de la 5G ».*

Parallèlement aux perspectives de la technologie de réseau, il a insisté sur les efforts continus à soutenir pour combler l'écart d'utilisation avec plus de 3 milliards de personnes n'utilisant pas le haut débit mobile. *« La bonne nouvelle, c'est que l'écart de couverture est en train de se réduire »*, a déclaré Mats Granryd.

De son côté, l'opérateur Orange a annoncé qu'il entend supprimer progressivement les réseaux 2G et 3G sur l'ensemble de son empreinte, entre 2025 et 2030. Ceci s'inscrivant dans le cadre des efforts visant à détourner le spectre vers la 4G et la 5G et à prioriser les investissements dans les technologies de réseau de nouvelle génération.

Au-delà de la 5G, au MWC, on regarde vers l'avenir et il est déjà question de la 6G. Jessica Rosenworcel, présidente de la Federal Communications Commission des États-Unis, a profité de son discours liminaire pour révéler que la prochaine vente aux enchères américaine du spectre à bande moyenne aura lieu en juillet 2022. Elle a souligné la nécessité de commencer à planifier, dès à présent, la 6G. *« Nous en sommes aux premiers jours. Mais, si nous avons appris quelque chose de notre expérience de déploiement de la 5G, c'est que le service sans fil est important pour la sécurité économique et nationale »*, a-t-elle fait remarquer.

L'Afrique observe pour construire son modèle

Quant aux Africains, les représentants des géants des télécoms sont venus en nombre à Barcelone, tout comme les régulateurs et les ministres des différents pays. Au cours de cet évènement, ils ont enchaîné les rencontres avec les partenaires et les réunions privées. *« Nous avons reçu des centaines de clients et de partenaires de l'Afrique. De très importantes délégations gouvernementales, d'entreprises, de régulateurs et d'opérateurs ont été présents à Barcelone pour discuter de leur projet de transformation digitale, de leurs projets cloud et de 5G »*, a assuré Mounir Soussi.

Alioune Ndiaye, CEO d'Orange Afrique, a arpenté les allées du MWC, tout comme les représentants de Sonatel, de MTN, d'Expresso Telecom ou de MPesa. Côté ministres, l'Ivoirien Roger Adom était présent, à l'instar de ses homologues chargés des TIC Cina Lawson (Togo), Aminata Kaba (Guinée) ou encore Désiré Cashmir Eberande Kolongele (RDC).

Lacina Koné, Directeur général de Smart Africa, a lui aussi fait le déplacement pour *« parler des sujets chauds avec les opérateurs »*. A savoir : le coût de l'internet, la taxation du mobile money et la question de l'identité numérique. Des préoccupations partagées avec la GSMA. *« Pour lancer le train de la transformation numérique, les opérateurs et le secteur public doivent connaître leurs clients, ce que nous appelons le KYC (Know Your Customer). Nous devons innover sur le modèle, afin de ne pas copier les autres, mais pour opérer un véritable saut de grenouille »,* a-t-il fait remarquer.

Pour le Bénin, Ouanilo Medegan Fagla, Directeur de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), a fait le déplacement pour voir les dernières technologies et solutions de son partenaire Huawei, qui pourront être implantées au pays. *« Nous prenons le train en retard par rapport aux autres, mais nous devons bien le prendre, en tenant compte de l'impact que nous pouvons avoir sur la planète »*, a-t-il rappelé. Il a ajouté que certains déploiements n'étaient pas encore prioritaires, à l'instar de la 5G. *« Nous devons d'abord œuvrer pour la couverture des zones blanches, la généralisation de la 3G et de la 4G, avant de penser à la 5G. Mais, il reste nécessaire pour nous d'entrer dans le jeu en même temps que tout le monde. Et de proposer ces nouvelles technologies sur certaines zones »*, a précisé le Directeur.

Mais, aux yeux du public, la présence africaine est restée peu visible. Les « sessions ministérielles », où sont intervenus les ministres, ont été interdites au public et aux médias. Du côté des stands, seules quelques start-up étaient présentes dans les allées, dont la sénégalaise LAfricaMobile, une plateforme de communication digitale. Ou encore l'agritech ghanéenne Esoko. Situées sur l'espace « 4 Years From Now » (4YFN), ces jeunes pousses ont été sélectionnées par Intracen, une agence conjointe de l'Organisation mondiale du commerce et de l'Organisation des Nations unies. Intracen assure, pour la 3ème année consécutive, une présence africaine au MWC, dans le cadre du projet NTF V, un programme d'appui à l'écosystème digital soutenu par les Pays-Bas.

« Nous avons co-sponsorisé leur présence à l'événement pour leur offrir une visibilité internationale et les appuyer à trouver et renforcer des partenariats et des clients », a expliqué Haifa Ben Salem, responsable du programme. Le MWC constitue en effet un tremplin pour ces start-up. A titre d'exemple, Malick Diouf, fondateur de LAfricaMobile, a eu une rencontre fructueuse avec l'ARTP, le régulateur sénégalais. *« Nous allons soutenir ce jeune talent. Des instructions ont été données aux services compétents pour décider de son accompagnement »*, a promis Abdoul Ly, le patron de l'ARTP.

Un MWC africain

L'Afrique du Nord a été, pour sa part, bien représentée au MWC. L'accélérateur Algeria Venture a bénéficié du soutien de Huawei pour exposer. Le Maroc a de son côté déployé un stand pour mettre en valeur sa nouvelle initiative : « Morocco Now ». *« C'est une première, c'est extraordinaire ! »,* s'est réjoui Hmad Chafiai, CEO de l'entreprise d'ingénierie télécoms Ingecys. *« Il serait impossible pour nous d'exposer seul, étant donné les coûts que cela représente. Or, c'est une belle opportunité. Les partenaires africains viennent voir nos solutions, tout comme les clients potentiels venus du Moyen-Orient, qui souhaitent orienter leurs activités vers l'Afrique et recherchent des partenaires »*. La Tunisie était aussi présente à travers ses incubateurs, notamment The Dot ou encore Novation City, son pôle de compétitivité.

Si la présence africaine reste timide, elle est pourtant prometteuse. D'autant que le continent dispose désormais de son propre congrès dédié au mobile, organisé sous la houlette de la GSMA : le Mobile World Congress Africa. Il se tiendra du 27 au 29 septembre 2022, à Kigali, au Rwanda. Une façon pour les pays du continent de se faire une place dans ce monde mobile globalisé.

Car, ainsi que l'a rappelé le président de la GSMA, *« tout se passe à une vitesse incroyable. D'énormes changements se produisent et d'autres sont à venir. Un nouveau monde immersif est presque arrivé, ce qui provoque des perturbations époustouflantes. Les nouvelles technologies redéfiniront notre façon de travailler et de vivre »*. Un mobile à la main et la tête dans les nuages, le monde est entré de plain-pied dans une virtualité bien réelle.

Les startups digitales africaines Beem, Lafricamobile, Looka et Esoko accompagnées par le projet Netherlands Trust Fund V (NTF V) au Mobile World Congress

METAVERS

Les entreprises entrent de plain-pied dans le virtuel

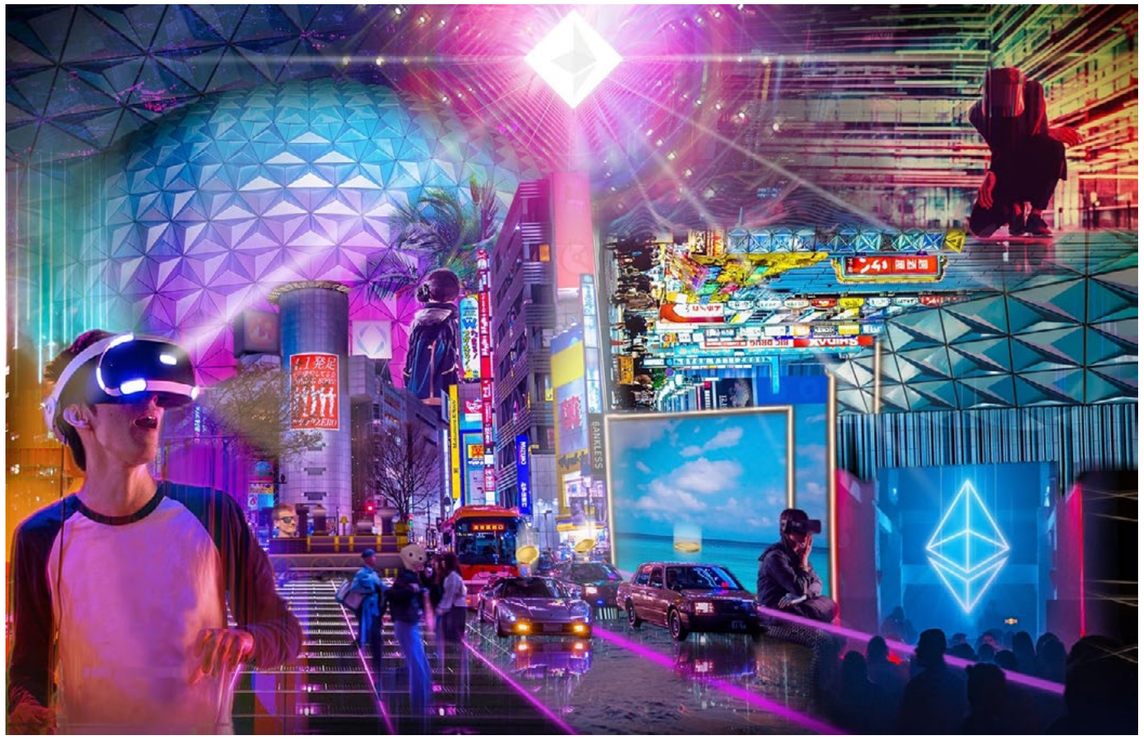
Après Meta, la liste des entreprises et des marques qui s'intéressent au Metavers s'allonge de jour en jour. Selon un rapport de Bloomberg Intelligence, ce nouvel univers révolutionne peu à peu le secteur du numérique et pourrait peser plus de 800 milliards de dollars d'ici à 2024. La révolution technologique présente plusieurs opportunités. D'abord en termes de diversification des sources de revenus et également pour la construction et la pérennisation de la notoriété des entreprises et des industries culturelles et créatives. Quant à l'Afrique, elle se fraie un chemin pour tirer parti du potentiel de cette technologie.

Enock Bulonza

Sur l'échiquier international, le Metavers s'impose déjà dans la sphère professionnelle. D'après Kevin Mukendi, consultant en Cybersécurité et membre de Internet Society Chapitre RDC, ce monde virtuel « *offre plusieurs opportunités. Il peut contribuer à la réduction du taux de chômage en Afrique, à la création de l'emploi et à la révolution de l'apprentissage en ligne. Grace à lui, les humains auront la possibilité de faire des choses impossibles dans le monde réel* », confie-t-il.

Les entreprises ont bien compris que le Metavers représente une belle opportunité. Certaines ont d'ores et déjà acheté des parcelles virtuelles dans ce nouvel univers et les personnes peuvent interagir entre elles, tout en exploitant des représentations virtuelles ou des avatars. D'autres ont lancé des plateformes virtuelles adaptées à leurs domaines d'interventions.

Parmi les entreprises les plus en vues figure Havas Group, qui dispose désormais d'une parcelle virtuelle dans un jeu vidéo.



Le groupe de conseil en communication a inauguré son premier Village virtuel, qu'il a appelé « le 69ème Havas Village ». Son objectif est d'aider les marques à se lancer avec succès dans cette nouvelle aventure virtuelle et de construire ensemble une image positive.

Et à la clé, une réputation riche de sens et un lien puissant avec les amoureux des jeux vidéo. Déjà, en 2021, le groupe a lancé Metavers by Havas. Cette offre de conseil, de création, de média et de commerce s'adresse aux marques qui voient dans le Metavers un nouvel espace de réponses à leurs enjeux de branding, de storytelling, d'expérience, de ciblage et de génération de revenus.

En janvier, Huawei et Beijing Shougang Park ont mis en ligne l'activité d'expérience Metaverse, qu'ils ont lancée conjointement. Cette plateforme virtuelle permet aux utilisateurs d'entrer directement dans un nouveau monde, en scannant un code QR dans le parc avec leurs Smartphones, afin de profiter des performances du groupe de robots Mojia et d'un spectacle de lumière virtuelle. Elle leur permet également de s'immerger dans une expérience en participant à des jeux de guerre.

Quant au fabricant d'appareils électroniques Samsung, il a lancé, en janvier, son emplacement Metavers, dénommé « Samsung 837X ». Alimenté par la blockchain, il offre aux utilisateurs la possibilité d'expérimenter tous les produits de la marque coréenne. Et leur permet de profiter de l'expérience immersive similaire avec des jetons non fongible (NFT), des jeux, des présentations de produits et des performances en direct.

L'industrie américaine de la mode Nike a pour sa part annoncé, en novembre 2021, le lancement de son Metavers « Nikeland » en 3D, sur la plateforme de jeu Roblox. Les utilisateurs s'exercent avec leurs avatars à différents jeux et les habillent avec les vêtements et des chaussures de la marque Nike.

Quid de l'Afrique ?

Toutes ces entreprises sont la preuve que le Metavers prend graduellement de l'ampleur. Mais qu'en est-il sur le continent africain ? Selon Kevin Mukendi, les industries culturelles et créatives africaines ne sont pas en reste, en dépit du manque de moyens et d'infrastructures.

« *Cette fois-ci, le continent ne se limitera plus à l'utilisation* », déclare-t-il. Le jeune expert en

cybersecurité indique que « *des start-up essayent déjà de se frayer un chemin pour tirer parti du potentiel de cette technologie, mais elles ont besoin d'importants financements pour se développer* ». A tire d'exemple, il cite la start-up algérienne Shédio, qui veut révolutionner le secteur du tourisme.

« *Elle en est encore à ses débuts, mais elle ambitionne d'offrir un service de tourisme digital avec la reconstitution 3D de sites culturels et historiques, et la création de musées interactifs* », précise-t-il.

La jeune pousse algérienne n'est pas la seule à s'activer pour intégrer l'espace virtuel dans son mode de travail. D'autres start-up font parler d'elles. C'est le cas d'Africarare, qui développe l'expérience de réalité virtuelle 3D. Sa plateforme virtuelle offre aux utilisateurs l'opportunité de créer leurs propres avatars uniques. Ils peuvent être échangés avec des skins uniques, tels que des chapeaux, des vestes et même des chaussures.

Cette année, la structure compte intégrer la pièce Ubuntu ($UBU) pour le payement des produits achetés sur sa plateforme. Avec cette politique, des terres pourront être achetées, échangées, conservées ou utilisées pour diverses expériences, telles que les expositions d'art, des jeux ou des expériences sociales. Cette stratégie aide Africarare a s'imposer sur le continent. Pour preuve, la société de télécommunication Mobile telephone networks (MTN Group) a acheté 144 parcelles de terrain numérique dans son Metavers.

Ajeverse est une autre industrie culturelle et créative africaine. Son ambition est de faire du continent un acteur de premier plan dans la révolution du Metavers et du jeton non fongible (NFT), grâce à sa plateforme virtuelle de gestion et de vente d'œuvres d'art, d'immobilier et d'espace publicitaire.

Le Metavers face aux attaques cyber

En dépit des opportunités, les craintes restent fortes sur la confidentialité et la sécurité des données dans le Metavers. « *Cette technologie est centrée sur les appareils numériques externes tels que les casques de réalité virtuelle. Mais, ces équipements peuvent facilement devenir la proie des pirates s'ils ne sont pas protégés* », fait remarquer le consultant en Cybersécurité. Il explique que « *les données capturées, via ces casques ou par l'un des autres appareils portables qui seront certainement introduits à l'avenir, peuvent être de nature très sensible. Les données peuvent facilement être transformées en menaces de chantage ou alimenter un complot d'ingénierie sociale d'un cybercriminel* », confie-t-il.

En outre, l'architecture du Metavers, construit grâce à la technologie blockchain, ne manque pas d'inquiéter. « *Bien que cette technologie soit sécurisée, elle n'est pas totalement à l'abri des vulnérabilités. De plus, le Metavers est décentralisé et ne dispose ni d'administrateur ni de modérateur désigné pour garder la charge ou le contrôle. Avec une telle absence d'autorité, il n'y aura aucun moyen possible de récupérer des avoirs volés ou obtenus illégalement* », conclut-il.

SPORT

Cryptomonnaie et réseaux sociaux pour le football africain

Le Cameroun, en Afrique Centrale, a accueilli, du 9 janvier au 6 février, la 33ème édition de la Coupe d'Afrique des nations. L'évènement a été sponsorisé par de nouveaux acteurs du domaine des technologies, tels que Binance, fournisseur mondial d'infrastructures de cryptomonnaie, ainsi que le réseau social chinois Tiktok. Deux participations aux ambitions révolutionnaires.

Aurore Bonny

Célébration de la Coupe d'Afrique des Nations par les joueurs de l'équipe nationale du Sénégal

Alors que plusieurs Etats africains ont marqué leur recul s'agissant de la cryptomonnaie et que d'autres s'y intéressent timidement, la participation d'un acteur aussi important que Binance, tout au long de cette compétition de football, a marqué les esprits et a suscité des interrogations. Pourquoi cet important réseau mondial a-t-il sponsorisé la plus grande compétition africaine de sport ?

Yi He, co-fondateur et CMO de la crypto entreprise, créée en 2017 et enregistrée aux Iles Caïmans, a indiqué que ce sponsoring *« corrobore la mission visant à généraliser la cryptographie à travers le continent »*. Parrain exclusif de la cryptomonnaie et de la blockchain de la CAN 2021, Binance traite déjà plus de 70 milliards de dollars en cryptomonnaie au quotidien. Et veut à présent *« faire en sorte que la cryptographie - et par là même Binance - soient davantage comprises et adoptées »*.

Croissance de la blockchain

Avec 1,2 milliard d'habitants et la prévalence de la technologie de la blockchain et de ses cas d'utilisation, Yi He considère que l'Afrique pourrait diriger l'avenir de cette industrie. Déjà, l'usage de la cryptographie est stimulé par la croissance des tradings, sous modèle pair-à-pair (P2P), mondialement dominé par le Kenya.

Et si le continent est la plus petite économie de cryptomonnaie mondiale, il n'en demeure pas moins la troisième région dont la croissance est la plus rapide.

Selon Chainalysis, le fournisseur de données dans le domaine, l'adoption de la cryptomonnaie a enregistré une croissance de plus de 1 200 % en valeur reçue, de juillet 2020 à juin 2021.

Avec un brassage de 105,6 milliards de dollars de cryptomonnaies, sur la même période, cette économie est *« l'une des plus dynamiques et des plus intéressantes, et elle dispose d'un potentiel de croissance important »*, indique la même source, dans un rapport sur la géographie de la monnaie numérique en 2021.

De son côté, la Confédération de football africaine (CAF) s'est dite prête à adopter la technologie basée sur la blockchain. Veron Mosengo-Omba, Secrétaire général de la CAF, est convaincu de son impact sur l'avenir du développement de ce sport en Afrique. Avec cette technologie, le football africain sera élevé à « un nouveau niveau ».

Des millions d'interractions

La compétition a d'ores et déjà atteint « des chiffres incroyables », sur les médias numériques, avec Tiktok, son sponsor « privilégié ». Selon un rapport publié par la CAF, *« la Coupe d'Afrique des Nations TotalEnergies Cameroun 2021 a établi de nouveaux records sur les pages de médias numériques et sociaux de la CAF, y compris sur les plateformes de nos partenaires, TikTok »*.

Pour preuve, le réseau social chinois enregistre 1,2 milliard de vues et sur Twitter, plus de 22 millions de visites de profils.

Quant aux réseaux sociaux de la CAN, ils comptent plus de 16 millions d'abonnés. Et avant la finale du tournoi, ils ont été visionnés 2,8 millions d'heures. Des millions d'interactions ont également eu lieu avec les canaux de médias sociaux de la CAN des différentes régions du monde.

Par ailleurs, avant la finale du tournoi, 400 000 commentaires ont été postés sur Facebook. Et plus de 28 millions d'interactions ont eu lieu, sur différents types de contenu. Sur le même réseau, plus de 50 millions de fans se sont manifestés en 35 jours. La page YouTube de la CAF a atteint 1 million d'abonnés et celle de YouTube CAFTV a enregistré 350 000 nouveaux abonnés en trois semaines.

« Ce sont des chiffres incroyables. Ils réaffirment simplement notre conviction que la Coupe d'Afrique des Nations TotalEnergies est un outil puissant et une plateforme qui a été sous-utilisée dans le passé. Nous créons un produit qui sera parmi les meilleurs au monde. Et il ne s'agit pas seulement de discours. Les résultats sont là pour le prouver », a déclaré le Secrétaire général de la CAF. De son point de vue, l'engagement des fans a été stimulé par *« un certain nombre de partenariats, y compris des nouveaux sponsors, comme TikTok »*.

Ce dernier a été mis à profit par la CAN TotalEnergies en tant que plateforme en Afrique. L'organisation considère que c'est *« un véhicule commercial solide et un important générateur de contenu »* sur le continent.

Avec ces chiffres, le réseau social chinois a saisi que la CAN est rapidement devenue un espace de référence pour tous les aficionados du football africain. En collaborant avec cet évènement sportif, TikTok a voulu accompagner les fans du ballon rond à célébrer ensemble les moments inoubliables du tournoi. Et continue d'incarner l'esprit et la passion des évènements sportifs emblématiques.

Loin de se limiter à la durée de la compétition, le partenariat de Tiktok s'étend tout au long de l'année. Il sera donc également présent à la TotalEnergies CAF Champions League 2022 et à la TotalEnergies CAF Women's Africa Cup of Nations 2022, au Maroc. Le sport possède une place importante au sein de la plateforme. Selon son promoteur, c'est l'une des thématiques préférées de la communauté, avec son milliard d'utilisateurs dans le monde.

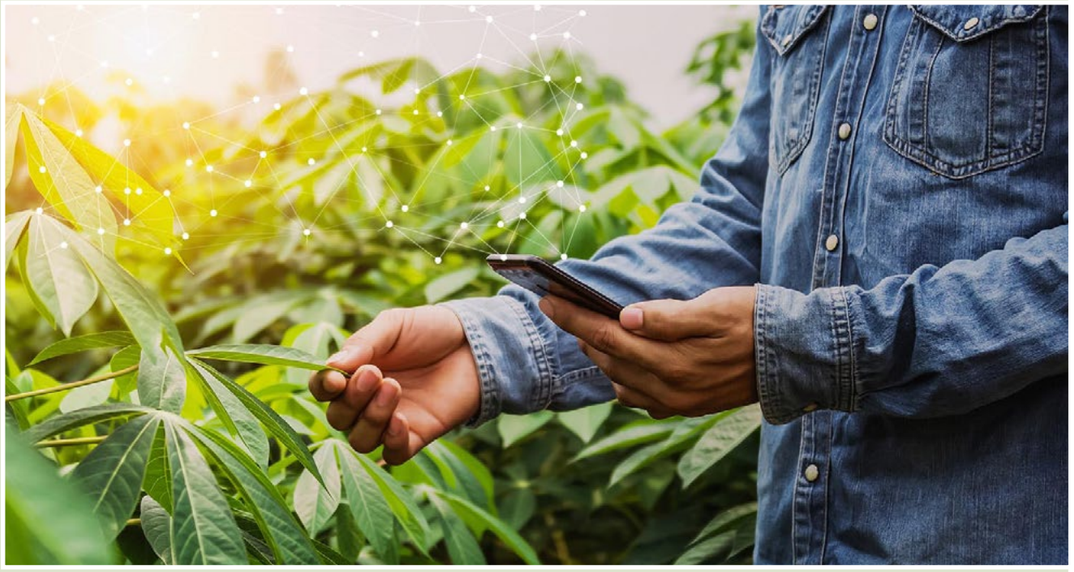
A travers cette alliance, la Confédération de football africaine veut être plus qu'une fédération sportive. La CAF veut *« continuer à être le plus grand producteur de divertissement footballistique, en Afrique, en offrant, aux fans du monde entier, des expériences de classe mondiale, tout au long de l'année »*.

AGRITECH

Quelles tendances pour demain ?

Avec environ 60% de populations essentiellement agricoles, l'Afrique dispose de plus de 60% des terres arables au monde. Cependant, elle n'est pas au rendez-vous pour optimiser sa production et reste encore l'un des continents les plus éprouvés par l'insuffisance alimentaire. Ce paradoxe est devenu un challenge pour son agriculture, qui a amorcé sa mutation grâce aux innovations technologiques.

Souleyman Tobias



Tous les segments de l'agriculture sont en pleine mutation sur le continent. Une agriculture de précision avec : des prévisions météorologiques, la gestion de l'eau et de l'engrais ; le contrôle et la sécurité des élevages ; la gestion de stock ou encore l'optimisation de la transformation agricole ! Ces innovations agricoles confèrent à l'Agritech africaine un dynamisme qui suscite l'espoir.

« Le développement de l'Agritech offre plus de promesses en Afrique que nulle part ailleurs », soutient Inoussa Maïga, Co-fondateur et directeur éditorial d'Agribusiness TV, une chaîne burkinabè dédiée à l'agriculture. Témoin privilégié des mutations du secteur agricole sur le continent et homme de terrain, il estime que même si l'Agritech africaine est *« très embryonnaire, elle est pleine de promesses, avec tout ce que cela implique comme changement socioéconomique »*.

Sur le continent, l'innovation technologique dans le secteur agricole doit changer la vie de millions de personne, analyse le directeur éditorial d'Agribusiness TV. Dans sa stratégie "Transformer l'Afrique", le NEPAD a déclaré que *« l'agriculture a son rôle à jouer dans la résolution de nos priorités continentales que sont l'éradication de la pauvreté et de la faim, la dynamisation du commerce intra-africain et des investissements, l'industrialisation rapide et la diversification économique, la gestion durable de nos ressources et de l'environnement, ainsi que la création d'emplois, la sécurité et la prospérité partagée »*.

Dans son document de *« Stratégie pour la transformation de l'agriculture africaine 2016-2025 »*, le Groupe de la Banque africaine de développement (BAD) a pour sa part relevé qu'*« en 2014, une proportion de plus de 60 % de la population d'Afrique vivait dans les zones rurales et comptait essentiellement sur l'agriculture comme moyen d'existence, tandis que les femmes représentaient au moins la moitié de la main-d'œuvre agricole »*. Akinwumi Adesina, Président de la Banque, estime que *« la transformation agricole contribuera à revitaliser les zones rurales, en transformant les zones de misère économique qu'elles sont aujourd'hui en zones de prospérité économique »*.

C'est désormais ce vœu que les acteurs de l'Agritech sont appelés à réaliser. A en croire Inoussa Maïga, ces acteurs sont sur la bonne voie. *« L'Agritech permettra d'accélérer le développement du secteur agricole rural. Avec des populations majoritairement rurales, si l'on arrive à accélérer leur développement, c'est le développement de tout le continent qu'on accélère »*, soutient-il.

Développer des solutions viables

Nourrir 1,5 milliard d'africains, d'ici à 2030 et 2 milliards d'ici à 2050 ! C'est le défi de l'agriculture africaine, selon les estimations du NEPAD. Le défi est de renforcer, entre autres, la capacité de production, la sécurité alimentaire et nutritionnelle, tout en préservant l'environnement et en faisant face aux défis climatiques.

C'est en cela que l'Agritech devient un levier important pour répondre aux attentes.

Inoussa Maïga estime que *« les solutions viables sont celles qui vont répondre aux besoins les plus basiques des acteurs »*. Peu importe la technologie, *« le plus important sera de répondre aux questions qui se posent »,* analyse-t-il. Dans un contexte africain souvent marqué par des conflits entre éleveurs et agriculteurs, Inoussa Maïga évoque un besoin récurrent : *« un éleveur nomade a besoin de savoir quel itinéraire emprunter pour éviter à ses animaux de détruire un champ ou encore de trouver des points d'eau »* !

Pour l'Agritech africaine, le sens de l'innovation consiste quelquefois à pourvoir à des besoins classiques, mais d'intérêt capital.

Sur le continent, les innovations se multiplient. Des solutions qui optimisent l'exploitation agricole. Le mapping des espaces cultivables avec des drones permet, par exemple, à des agriculteurs d'accroitre leur rendement en surveillant de près l'évolution des cultures.

Grâce à l'Intelligence artificielle ou avec d'autres technologies, l'analyse de données agricoles fournit des prévisions aux agriculteurs du continent,

Inoussa Maïga
Co-fondateur et directeur éditorial d'Agribusiness TV

qui sont souvent à la merci des climats et des intempéries. L'internet des objets (IoT) est au cœur de multiples solutions de gestion de l'eau et des stocks. Cet ensemble d'innovations technologiques transforme l'agriculture africaine.

Elle devient plus précise et plus performante, et obtient donc plus de rendements. Dans certains cas, ces rendements peuvent clairement être estimés par anticipation. L'agriculteur a ainsi la capacité d'anticiper la recherche de marché pour écouler son produit.

Sur le segment de la vente, les innovations technologiques ont suscité des solutions qui brisent les barrières. Des plateformes de vente directe (marketplaces), entre producteurs et consommateurs finaux, contribuent à éliminer les intermédiaires. Et les produits sont plus accessibles. Le producteur peut écouler plus facilement et plus rapidement son produit car le prix est plutôt accessible.

Que ce soit au Togo, au Bénin, au Burkina Faso ou encore au Niger, des solutions de transferts d'argent, via le mobile, permettent aux agriculteurs de disposer de fonds sécurisés pour l'achat des intrants comme les engrais. Des initiatives se sont multipliées en ce sens depuis 2019 et ont été accélérées par la pandémie de la Covid-19. Ainsi, les innovations digitales permettent aux acteurs de l'agriculture de contourner les obstacles.

Une adaptation plus sûre

Les défis de l'agriculture sont énormes en Afrique. Encore à l'étape rudimentaire dans bien des régions, l'agriculture doit faire face aux défis climatiques, à la production de masse, à la fertilité des sols et à la pérennisation même des exploitations. Avec les innovations technologiques agricoles, qui foisonnent partout sur le continent, l'adaptation de l'agriculture a un avenir prometteur. Ces innovations permettent de changer les habitudes, de la production à la consommation, en passant par la distribution.

L'écosystème Agritech africain est en pleine floraison. Inoussa Maïga espère davantage de soutien des gouvernants. De son point de vue, il faut une ouverture d'esprit pour comprendre les enjeux.

Et mettre en place un environnement adapté à l'innovation technologique agricole, de même qu'un financement, qui, pour l'heure, est encore tributaire des subventions étrangères. Une préoccupation dont la pertinence peut être retrouvée dans les actions du Groupe OCP : une exception marocaine pour soutenir une agriculture durable en Afrique.

MAROC

StartGate, un catalyseur pour l'émergence des start-up

Pour relever les défis de son industrie et de l'agriculture mondiale, le Groupe OCP est constamment à la recherche de nouvelles solutions. Et travaille à la mise en place d'un écosystème qui promeut l'innovation. Focus sur StartGate, un maillon clé de cet écosystème abrité par l'Université Mohammed 6 Polytechnique (UM6P). Interview de Sarrah Cherif D'ouezzan, StartGate Programs Lead et de Mohamed Lahmami, Community Builder StartGate

Souleyman Tobias

Sarrah Cherif D'ouezzan
Programs Lead, StartGate_UM6P

Mohamed Lahmami
Community Builder, StartGate_UM6P

Sarrah Cherif D'ouezzan
Programs Lead,
StartGate_UM6P

INTERVIEW

Cio Mag : StartGate est le bras opérationnel de l'UM6P pour promouvoir l'innovation, en collaboration avec le Groupe OCP. Quel est le rôle de cette composante ?

Sarrah Cherif D'ouezzan : StartGate est une des composantes de l'écosystème d'innovation construit par l'UM6P. StarGate est un campus de start-up. Il est rattaché à l'Université et regroupe un écosystème entrepreneurial international engagé à fournir une infrastructure et des ressources de classe mondiale.

L'objectif est de soutenir les entrepreneurs, qui lancent et font croître leur start-up. Des partenariats sont mis en place via des programmes pour accompagner les start-up dans leur lancement et leur développement.

Nos entrepreneurs bénéficient de partenariats gagnant-gagnant avec les différents acteurs de l'écosystème (entreprises, hubs d'innovation, investisseurs, administrations, experts, etc.). Ces partenariats permettent d'élargir, de mutualiser et de renforcer leur offre, mais aussi de favoriser l'accès à l'infrastructure et aux services de l'écosystème de connaissances et d'innovation de l'Université.

Par exemple, des plateformes d'expérimentation à taille réelle, des laboratoires d'analyses, des Fab Lab pour les besoins en prototypage ou encore à travers l'offre Cloud du Data Center pour le stockage de data.

StartGate réunit donc une offre de services dédiée aux entrepreneurs débutants ou chevronnés, de sorte à renforcer leur offre et leur notoriété. Et pour les accompagner dans leurs projets entrepreneuriaux.

Notre mission principale est de fournir toutes les clés de réussite nécessaires à ces entrepreneurs. Quelque 254 porteurs de projets, tous secteurs confondus, sont aujourd'hui accompagnés dans le cadre de StartGate.

Cio Mag : Comment StartGate identifie les projets qu'elle accompagne ?

Mohamed Lahmami : L'innovation et l'entreprenariat innovant, en particulier, sont encore embryonnaires au Maroc. StartGate est avant tout le catalyseur de l'émergence des start-up. StartGate fédère des programmes. Notre ambition est de créer une communauté, de générer du lien, de susciter de l'entraide et de donner aux porteurs d'idées un accès à l'écosystème d'entreprenariat innovant.

StartGate propose donc des programmes d'accompagnement qui sont autonomes et qui ont leur propre process de sélection, leurs propres exigences, leurs modes de financement, etc. Nous essayons de structurer les choses sans trop imposer aux programmes leur process.

Mohamed Lahmami
Community Builder,
StartGate_UM6P

INTERVIEW

L'idée, c'est de créer des modèles de fonctionnement avec des critères de base.

Nous aidons donc ces programmes, en fonction de leurs challenges, à trouver des start-up en fonction des défis qu'elles doivent relever. En termes de fonctionnement, nous publions tous les appels à candidature sur nos réseaux sociaux et notre site web.

Cio Mag : Pourquoi avoir notamment choisi d'accompagner les innovations AgriTech ?

Sarrah Cherif D'ouezzan : Il y a un contexte international à cela. Nous serons environ 10 milliards de personnes dans le monde, d'ici à 2050. Il y a un grand défi de sécurité alimentaire à relever. La vision d'OCP est de contribuer à l'essor d'une agriculture durable et la mission que se donne le Groupe est de nourrir le sol pour nourrir la planète ! Pour aider au développement d'une agriculture plus compétitive, mais aussi plus propre et plus soucieuse de l'environnement, la technologie est une des solutions, d'où l'intérêt pour le secteur de l'AgriTech.

Cio Mag : Quelles sont les perspectives pour StartGate en termes de programmes innovants ?

Sarrah Cherif D'ouezzan : La Covid-19 a montré qu'il fallait appuyer encore plus l'innovation et utiliser tous les mécanismes possibles. Il est question de travailler sur les différents types d'innovations, aussi bien celles qui vont améliorer l'existant, que celles qui vont être des innovations de rupture. La recherche et développement, les brevets et autres inventions devront être développés, tout en recherchant des start-up qui répondent aux challenges de demain.

STARTGATE

MOHAMMED VI POLYTECHNIC UNIVERSITY

START-UP

AgriEdge, actrice de la transformation agricole

Dans l'écosystème de l'innovation agricole au Maroc, AgriEdge a voix au chapitre. La start-up est en contact permanent avec le secteur et propose des solutions sur mesure aux agriculteurs. Du choix des cultures à leur mise sur le marché, en passant par la phase de suivi et de récoltes, AgriEdge imprime sa marque sur l'agriculture marocaine et bien au-delà. Focus sur une start-up africaine de l'Agritech présente sur toute la chaine de valeur agricole en Afrique.

Souleyman Tobias

Faissal Sehbaoui
Directeur général d'AgriEdge

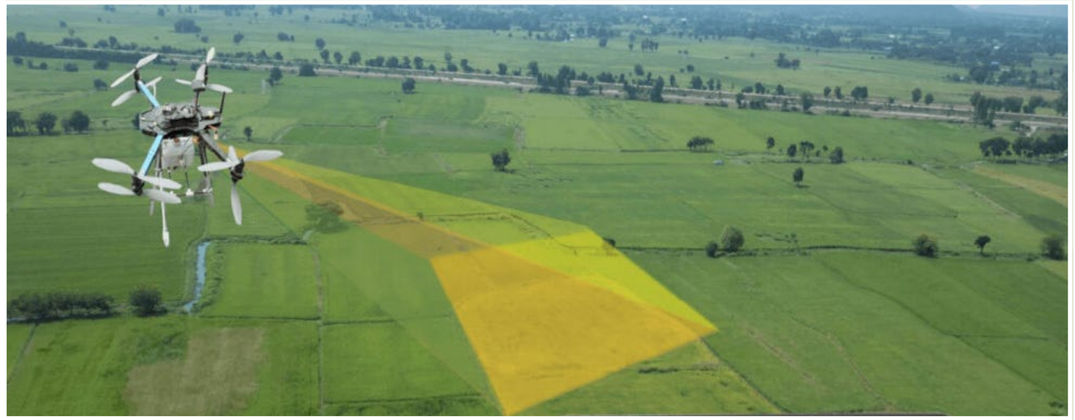
En 2017, AgriEdge s'est lancée à l'assaut du monde agricole, à la faveur d'un programme entrepreneurial du Groupe OCP. La jeune pousse avait un objectif précis : *« mettre la puissance du Big Data à la disposition des agriculteurs africains pour développer une agriculture de précision, résiliente et durable »*, confie Faissal Sehbaoui, directeur général d'AgriEdge. Cette ambition a permis à la start-up, devenue une société, d'entrer, dès 2018, en incubation à l'Université Mohammed 6 Polytechnique.

Grâce aux innovations technologiques, elle est entrée dans sa phase de maturité et s'est positionnée comme actrice clé de la transformation du secteur agricole au Maroc et en Afrique. Le challenge, pour AgriEdge, a été de prouver que l'agriculture africaine a besoin des solutions innovantes africaines. *« Une solution Agritech ne peut marcher convenablement en Afrique, sauf si on l'a développé sur le continent »*, soutient Faissal Sehbaoui. Et AgriEdge a pu compter sur l'environnement de l'UM6P, sur l'expertise de ses chercheurs et sur la qualité de ses laboratoires pour développer des services Agritech adaptés au contexte africain.

AgriEdge n'a donc pas perdu de vue les enjeux de son challenge. Elle a dû pour cela se résoudre à répondre *« aux défis techniques liés à la connectivité des parcelles et des cultures liées à l'utilisation du digital »*. Car, pour permettre aux agriculteurs de bénéficier de la puissance des données et aller vers une agriculture plus résiliente et plus durable, il a été nécessaire de changer de paradigme.

Simplicité et efficacité : des solutions sur mesure

Les solutions d'AgriEdge pourvoient à une large panoplie de besoins : la date optimale de semis, les besoins d'irrigation et la fertilisation ; l'estimation du rendement et la date optimale de la récole, etc. A l'heure actuelle, la jeune entreprise accompagne environ 24.000 agriculteurs au Maroc et au-delà de ses frontières. Et propose des solutions axées sur l'Intelligence artificielle, qui sont alimentées par des données agricoles. Agritech aide *« l'agriculteur à améliorer son processus décisionnel et à maximiser*



durablement sa performance globale », se félicite son directeur général. A ce jour, elle déploie des solutions d'optimisation agricole, parmi lesquelles AquaEdge, N-IndeX et CitrusYield.

Avec **AquaEdge**, Agritech propose un pilotage de précision de l'irrigation en utilisant des capteurs d'humidité et des images satellites. Cette solution permet 25% d'économie d'eau, affirme-t-on à AgriEdge. Co-developpée avec un grand groupe agro-industriel marocain, la **N-IndeX** renseigne pour sa part l'indice digital d'azote. Elle permet de *« rationaliser la fertilisation azotée de couverture de la culture de blé en se basant sur l'imagerie satellite »*, explique Faissal Sehbaoui. Des retours d'expérience, il note que *« cet indice a permis d'atteindre 21% d'économie d'azote, tout en réalisant 24% de rendement en grain supplémentaire »*. *« Ce gain double profite à l'agriculteur, qui améliore significativement sa recette »*. Enfin, le **CitrusYield** prédit le rendement des vergers d'agrumes (en particulier les clémentines), plusieurs mois avant la date de récolte. *« Une telle information est cruciale pour la planification des transactions d'export et la gestion rationnelle de la logistique de conditionnement et d'écoulement de la production »*, argumente AgriEdge. Il s'agit de *« permettre à l'agriculteur de disposer de plusieurs leviers pour gérer sa production »*.

Et de faire ainsi face aux aléas, comme la météo, dont les informations sont utiles pour les projections. Avec les solutions AgriEdge il est aussi possible d'optimiser les leviers sur lesquels l'agriculteur peut agir. A commencer par la quantité d'engrais à appliquer et par les besoins précis en eau d'une plante. Faissal Sehbaoui s'en explique. *« Les services Agritech proposés par AgriEdge dotent l'agriculteur d'outils simples. Il peut suivre ce qui se passe sur sa parcelle à distance et reçoit des conseils, sur son téléphone portable, sous des formats adaptés. Et également des alertes quand les conditions sont propices à l'apparition de maladies agricoles. Ou encore des prédictions sur sa production, avant la date de récolte, pour mieux préparer la partie vente et logistique. Tout cela contribue à l'amélioration de son expérience et à l'attractivité de l'agriculture pour les jeunes, qui sont très connectés et consomment beaucoup de digital »*.

Trois graines pour une Agritech performante

La recherche de solutions aux besoins du secteur agricole a conduit AgriEdge à développer d'autres approches, comme des programmes d'accompagnement du secteur. Faissal Sehbaoui en détaille trois :

- le programme **Filaha Innovation.** Il a comme objectif d'aider les jeunes porteurs d'idées en Agritech à les transformer en start-up. *« On est sur le point de boucler la deuxième édition, avec un total de plus de 300 candidatures reçues et de 24 start-up accompagnées »*, précise le directeur général d'AgriEdge,
- la **Caravane Agritech** pour la sensibilisation et la formation des petits agriculteurs et des jeunes en-

trepreneurs, dans les domaines des nouvelles technologies. Elle en est à son cinquième arrêt avec plus d'une soixantaine de participants à chaque étape,

- les **Agri Anlaytics Days**, premiers congrès scientifique international en leur genre organisés au Maroc ! Ils permettent d'inviter des experts nationaux et internationaux, ainsi que des agriculteurs, pour parler d'AgriTech. La troisième édition se prépare pour cette année, si les conditions sanitaires le permettent, précise l'entreprise.

A travers ces différents programmes, AgriEdge compte *« contribuer au développement de l'écosystème Agritech marocain afin de rapprocher, de la meilleure façon, les solutions technologiques de l'agriculteur »*. Dans son approche, AgriEdge adresse les besoins de tous les acteurs : des petits exploitants qui produisent exclusivement pour nourrir leurs familles, jusqu'aux grands groupes de production orientés vers le marché d'exportation.

Une transformation agricole en marche

Faissal Sehbaoui peut se féliciter de participer, avec ses solutions, à la mutation du secteur agricole sur le continent. Depuis son siège AgriEdge, observe comment l'Intelligence artificielle change les données agricoles au Maroc et au-delà. *« L'adoption de systèmes de l'IA permet aux exploitations agricoles de mieux utiliser leurs données et de produire plus avec moins de ressources. En effet, l'IA facilite la prise des décisions plus optimales, en recommandant la bonne chose/dose, au bon moment, au bon endroit »*, explique le directeur général d'AgriEdge.

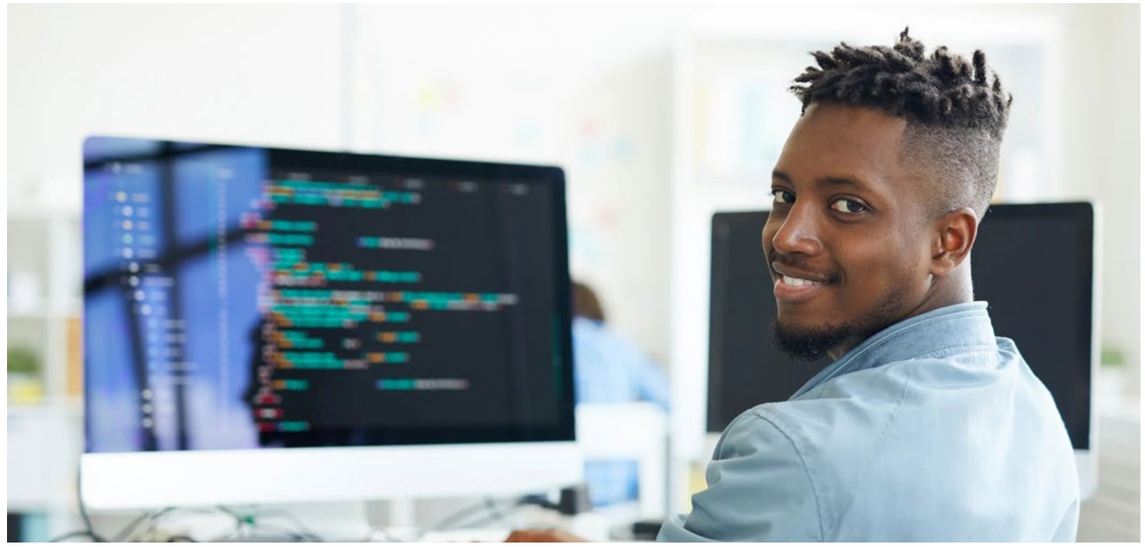
Aux delà de l'IA, l'ensemble des technologies que propose les innovations Agritech participe à transformer l'agriculture sur le continent. Ces outils technologiques sont présents sur toute la chaîne, observe le patron d'AgriEdge. *« Ces innovations mettent à la disposition des agriculteurs des conseils précis pour mieux produire, tout en utilisant moins de ressources. Et, in fine, un gain en temps de travail et en confort pour l'agriculteur, et plus d'efficacité, de productivité, avec, en sus, une marge bénéficiaire »*, conclut Faissal Sehbaoui.

Il note aussi, en ce qui concerne le Maroc, que les acteurs de l'agriculture adoptent, en fonction de leurs besoins, ces solutions locales adaptées à leurs réalités. Son entreprise joue un rôle de premier plan et va jusqu'à proposer des solutions gratuites, via des coopératives, à ceux dont les capacités financières ne permettent pas des choix de solutions pourtant nécessaires au développement de leurs activités agricoles.

DATA ET RISQUES NUMÉRIQUES
Une cyberurgence africaine

Avec la crise sanitaire, la digitalisation s'est accrue et l'Afrique et le reste du monde ont eu recours à de nouveaux usages numériques. Conséquence : le risque de cyberattaques a également augmenté. Les pays africains ont-ils pris la mesure de cette menace ? Comment s'arment-ils pour protéger les données des citoyens ? Et que font les entreprises pour faire face aux coûts colossaux engendrés par la cyber-criminalité ? État des lieux.

Camille Dubruelh



« Le niveau de protection en termes de cybersécurité sur le continent est quasi inexistant, pour ne pas dire nul ». Le constat, dressé par Clément Domingo, Co-Fondateur de l'ONG Hackers Sans Frontières (HSF), est sans appel.

La pandémie a sans aucun doute accéléré la digitalisation du continent, déjà en marche, en modifiant les habitudes des quelque 500 millions d'internautes. Aujourd'hui, on achète, on épargne, on se divertit, on discute et on travaille à travers les outils numériques, dans un environnement de plus en plus exposé aux cybermenaces.

Quelques chiffres : l'éditeur de logiciels de cybersécurité Kaspersky indiquait que l'Afrique avait été la cible de 28 millions de cyberattaques, entre janvier et août 2020. Et dans une étude réalisée auprès de 211 grandes entreprises, basées dans onze pays d'Afrique francophone et réalisée en juin 2021, le cabinet de conseil Deloitte révèle que 40 % d'entre elles ont connu une augmentation du nombre d'incidents, depuis 2020. Ceci étant la conséquence immédiate du télétravail, auquel 92% des entreprises interrogées ont eu recours. *« De nombreuses entreprises sont victimes quotidiennement de piratages informatiques, d'espionnage industriel, ainsi que de vol de données et de propriété intellectuelles. L'Union africaine semble impuissante face à de nombreuses attaques informatiques ciblées depuis quelques mois. Le plus déplorable demeure l'absence totale de transparence, de traçabilité, de plaintes et de statistiques sur ces cyberattaques ! »*, déplore Clément Domingo. Selon une étude d'Interpol, 90 % des entreprises africaines n'utilisent pas les protocoles de cybersécurité nécessaires.

L'expert constate qu'en Afrique un tabou demeure autour des cyberattaques. L'omerta entoure ces pratiques, à cause du malaise engendré par le piratage. Les DSI risquent en effet de perdre leur poste en cas d'attaque... Selon le Centre d'études stratégiques de l'Afrique, 96% des attaques ne sont ainsi pas signalées ou restent irrésolues. *« La réalité, aujourd'hui en Afrique, c'est une absence totale de cadre juridique et de garde-fou concernant le cyberespace. En même temps, la priorité première des populations n'est pas le numérique, mais de se soigner, d'avoir accès à l'eau, à l'éclairage et de se nourrir ! »*, poursuit Clément Domingo.

Plus de 4 milliards de dollars de perte

Pourtant, le coût potentiel de la cybercriminalité est colossal. Dans le rapport « E-Conomy Africa 2020 », la Société financière internationale (SFI) et Google estiment que le numérique pourrait générer un revenu de 180 milliards de dollars pour l'économie africaine d'ici à 2025 et de 712 milliards, d'ici à 2050. Mais, la faible fiabilité des plateformes numériques africaines pourrait compromettre cette manne financière.

DOSSIER PROTECTION DES DONNÉES

Interpol a publié un rapport sur le sujet, en octobre 2021 et les conclusions sont irrévocables. Au cours de l'année 2020, dans certaines régions, les cyberattaques répertoriées ont plus que doublé. Une étude, réalisée par l'entreprise de cybersécurité kényane Serianu, a montré que la cybercriminalité a amputé le PIB africain de plus de 10 %, en 2021, avec un coût estimé à 4,12 milliards de dollars.

L'Afrique du Sud a même été classée, dans un rapport d'Accentur, au troisième rang mondial des victimes de la cybercriminalité, pour un coût annuel de 2,2 milliards de rands sud-africains.

Lorsqu'on évoque la cybersécurité, aujourd'hui, sur le continent, le parent pauvre des (trop) maigres investissements des entreprises et des Etats et sans aucun doute la protection des données personnelles. Selon le rapport Deloitte, si 35% des investissements cybersécurité sont actuellement dédiés à la sécurité des infrastructures IT dans les entreprises africaines interrogées, seulement 5% concernent la sécurité des données, la détection des incidents, le suivi des menaces ou encore la gestion des identités et des accès.

La protection des données, loin d'être une priorité

Tous les pays du continent sont-ils logés à la même enseigne ? Et le constat est-il aussi dramatique pour tout le monde ? Selon le Global Cybersecurity Index 2020 de l'Union internationale des télécommunications (UIT), seuls 23 Etats africains ont une stratégie nationale de cybersécurité ; 19 ont un centre d'alerte et de réponse aux cyberattaques (CERT) et 15 pays affichent un niveau de préparation de la cybersécurité supérieur à la moyenne mondiale. Quant à la protection des données, on ne compte que 29 pays africains qui ont une législation dédiée.

Jules Hervé Yimeumi, fondateur de la plateforme Africa Data Protection et juriste pour la protection des données au sein d'une société d'assurance, note certaines améliorations.

« Depuis ces cinq dernières années, plusieurs États africains ont adopté une législation relative à la protection des données, comme le Togo, le Rwanda ou le Kenya. Toutefois, la présence d'autorités de contrôle chargées de faire appliquer la loi est faible. A ce jour, sur 54 pays africains, 20 d'entre eux disposent d'une autorité de contrôle. Mais, elle ne dispose souvent que de très peu de moyens et de pouvoir de sanction ».

Une fois n'est pas coutume, ce sont donc les pays anglophones qui sont à la traîne dans le domaine. L'un des éléments d'explication est que la plupart des pays francophones font partie de l'Association francophone des Autorités de protection des données personnelles (AFAPDP). Créée en 2007, elle a pour objectif de partager l'expertise en matière de protection des données personnelles. Aujourd'hui, le Bénin, le Burkina Faso, le Cap-Vert, la Côte d'Ivoire, le Gabon, le Mali, le Maroc, Maurice, le Sénégal et la Tunisie sont membres de cette association.

Mais, malgré les avancées, le problème reste entier, car même pour les pays disposants de lois et d'organes de régulation, les sanctions restent rares. *« Il y a très peu de sanctions, même si certains pays, comme le Sénégal, commencent à punir ces entreprises »*, assure Hervé Yeumeni. La Commission de la protection des données du Sénégal à en effet déjà procédé à 27 sanctions, la plupart étant des mises en demeure (Sonatel, Attijariwafa Bank) ou des avertissements (Expresso pour l'envoi de SMS publicitaires ou Ceginus pour manquement à la législation sur les données à caractère personnel).

Une seule sanction financière a été prononcée. *« Le problème n'est pas la lourdeur de la sanction. Le principe même de la sanction est dissuasif et pédagogique »*, assure Awa Ndiaye, présidente de la CDP. En effet, un avis trimestriel est publié par la Commission, où les entreprises sont nommément citées. *« Personne n'a envie de s'y retrouver. Aussi, lorsqu'une société reçoit un avertissement ou une mise en demeure, elle nous contacte elle-même pour que nous l'aidions à se mettre en conformité avec la loi »*, poursuit la responsable, qui rappelle *« qu'il ne peut pas y avoir de développement digital sans confiance, sans sécurité et sans confidentialité des données »*.

De son côté, Jules Hervé Yimeumi précise que certaines législations ne sont pas assez avancées pour répondre aux enjeux numériques actuels. *« La plupart des pays africains ont des textes qui concernent les droits des personnes. On y voit, entre autres, les droits d'accès à nos données, à la ratification et à l'effacement. Aujourd' hui, dans les pays européens, on a rajouté de nouveaux droits, comme le droit à l'oubli ou encore le transfert de données d' une entreprise à une autre, ce qui n'existe pas en Afrique »*, détaille le juriste.

A quand un RGPD africain ?

Et ce n'est pas seulement au niveau national que le bât blesse. La Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel, qui date de 2014, n'a été signée et ratifiée que par un peu moins de la moitié des États du continent. Et elle nécessiterait une mise à jour pour faire face aux nouveaux enjeux du numérique. *« Un des enjeux à court et moyen terme serait de réexaminer la convention de Malabo. Et de pouvoir inclure une ou deux directives fortes, en plus, pour prendre en compte la protection des populations et avec elles, leurs données personnelles. Il est temps que l'Afrique dispose de son propre RGPD ! »*, assure Clément Domingo. « *Les GAMAM (Google, Amazon, META, Apple, Microsoft) et les multinationales ne peuvent plus se servir comme elles veulent en prenant en otage les données des citoyens africains »*. Pour Jules Hervé Yimeumi, *« il y a peut-être un problème de leadership, au sein de l'Union africaine, pour œuvrer à l'effectivité de la convention de Malabo. D'un autre côté, on a le Réseau africain des autorités de protection des données personnelles (RAPDP), dont le Maroc assure le Secrétariat Permanent, qui travaille à un projet d'harmonisation sur la protection des données en Afrique »*.

Les deux experts s'accordent sur un point : pour le moment, mieux vaut privilégier des réponses nationales. La priorité est que chaque État se dote d'une législation à jour face aux enjeux du numérique et d'une autorité de contrôle dotée d'un pouvoir de sanction. Un règlement régional pourrait suivre dans un second temps.

Awa Ndiaye, elle, plaide pour un modèle africain et une harmonisation des différentes pratiques et législations. Un processus qui est d'ailleurs en cours sous la houlette de l'alliance Smart Africa, précise-t-elle.

Formation et information

Pourquoi est-ce primordial aujourd'hui de protéger les données des citoyens et quels sont les risques ? Plus elles utilisent Internet, plus les populations sont menacées par le détournement de finalité des traitements de leurs données par les organismes. L'autre risque reste le ciblage. Il est très facile à mettre en place sur des sites internet grâce aux cookies, lesquels permettent de connaître les préférences des utilisateurs et de proposer des offres personnalisées, comme le fait par exemple Google. Et, sur le continent, les populations ne sont que très peu informées sur les risques liés à leurs données. *« On le voit très bien sur les réseaux sociaux. Il y a un gros travail de sensibilisation à faire chez les jeunes, dans les écoles. Il faut qu'ils comprennent ces enjeux dès le plus jeune âge. Il faut notamment leur expliquer que lorsque qu'ils s'inscrivent sur un réseau social et qu'ils partagent une photo, celle-ci ne leur appartiendra plus, mais sera celle du réseau social »*, alerte Jules Hervé Yimeumi.

« Les populations en Afrique sont livrées à elles-mêmes ! », martèle le cofondateur de HSF. *« On envoie nos concitoyens, nos familles, nos amis, nos enfants au casse-pipe. Si j'étais un attaquant, je me concentrerais sur ces cibles et je me ferais un pactole ! D'ailleurs je ne suis pas le premier à y avoir pensé. Dernièrement, dans l'actualité, on apprenait qu'une opération conjointement menée par Interpol et les autorités nigérianes avait démantelé un important groupe de cybercriminels au Nigéria »*.

Dans les pays africains, il n'existe pas de campagnes publicitaires et d'affichages pour expliquer tous ces enjeux, ni de sensibilisation aux heures de grandes écoutes. *« Il y a un grand retard à rattraper, mais ce n'est pas impossible. Concrètement, au sein de HSF, on prône la mise en place d'un permis cyber, comme on pourrait passer son code pour apprendre à conduire. Cela permettrait à la génération très connectée en Afrique (et qui contribue à hauteur de 70% des flux mondiaux sur les GAFAM) d'adopter peu à peu les bons cybers reflexes »*, propose Clément Domingo.

Au-delà de l'information des jeunes, sur le continent, il manque d'une part des infrastructures de stockage et d'autre part des profils humains spécialisés sur la cybersécurité. Cela se fait lourdement sentir et pose directement la question de la souveraineté numérique de l'Afrique. Aujourd'hui, les nombreux jeunes qui souhaitent travailler dans la cybersécurité poursuivent leurs études supérieures en Europe ou dans les pays anglo-saxons, faute de pouvoir effectuer leur cursus dans des centres d'excellence africains. Et le manque de cloud force les États à réclamer des dérogations pour stocker les données des citoyens sur d'autres continents.

Ces problématiques découlent, avant tout, d'un manque de volonté politique, alors que des partenariats pourraient être mis en place avec les entreprises privées, qui ont plus que jamais besoin de ces compétences. Mais, pour l'heure, le risque cyber est encore loin d'être une priorité. Pourtant, les infrastructures sont chaque jour menacées par des cyberattaques puissantes, qui pourraient faire dégringoler des économies entières. *« Le Monde s'est familiarisé avec la notion d'urgence écologique. Je pense qu'en Afrique, la notion d'urgence cyber va émerger. »*, conclut Clément Domingo.

Chiffres clés :

- L'Afrique a été la cible de 28 millions de cyberattaques entre janvier et août 2020.
- **90 %** des entreprises africaines n'utilisent pas les protocoles de cybersécurité nécessaires.
- **96%** des cyberattaques ne sont pas signalées ou restent irrésolues.
- La cybercriminalité a amputé le PIB africain de plus de **10 %** en 2021, avec un coût estimé à 4,12 milliards de dollars.
- **35%** des investissements cybersécurité sont dédiés à la sécurité des infrastructures IT dans les entreprises africaines interrogées.
- Seulement **5%** sont dédiés à la sécurité des données, la détection des incidents, le suivi des menaces ou encore la gestion des identités et des accès.
- Seuls 23 pays ont une stratégie nationale de cybersécurité ; 19 ont un centre d'alerte et de réponse aux cyberattaques (CERT) et 15 pays affichent un niveau de préparation de la cybersécurité supérieur à la moyenne mondiale.

DOSSIER PROTECTION DES DONNÉES

INTERVIEW

« Positionner le Togo comme moteur de l'intégration sous-régionale et de la coopération en cybersécurité »

C'est une première au Togo : du 23 au 24 mars, le pays accueil des chefs d'Etats, des décideurs et des experts, de divers horizons, autour des enjeux de la cybersécurité. Ce Sommet international, organisé en partenariat avec la Commission économiques des Nations-Unies pour l'Afrique (CEA), devrait permettre à l'Etat togolais de présenter son modèle de partenariat public-privé dans la cybersécurité. Dans cet entretien accordé à Cio mag, Gbota Gwaliba, Directeur général de l'Agence nationale de Cybersécurité (ANCy) et Simon Melchior, Directeur général de Cyber Defense Africa (CDA), expliquent la portée de l'événement pour le Togo.

Gbota Gwaliba
Directeur Général, Agence nationale de Cybersécurité (ANCy)

Simon Melchior
Directeur Général, Cyber Defense Africa (CDA)

Cio Mag : Le Togo organise le premier Sommet sur la cybersécurité, les 23 et 24 mars. Quels sont les objectifs de ces journées ?

Gbota Gwaliba : Les pays africains connaissent une explosion de l'utilisation d'Internet et des nouvelles technologies, ce qui expose les citoyens, les administrations et les entreprises aux risques de cybercriminalité. La cybersécurité est devenue un enjeu de sécurité et de souveraineté. Mais, nous constatons que les États africains ne mettent pas suffisamment les questions de cybersécurité au cœur de leur politique publique. Et la cybercriminalité transcende à présent les frontières physiques des États. C'est pourquoi il est important que les Chef d'États et de gouvernement s'entendent sur des mécanismes de coopération à tous les niveaux.

Les objectifs de ce premier Sommet de la cybersécurité au Togo sont donc multiples. Ils consistent à :

- Jeter les bases d'un cadre légal et réglementaire spécifique à la cybersécurité et à la lutte contre la cybercriminalité, à l'échelle africaine ;
- Réfléchir à des stratégies et des politiques de cybersécurité, qui soient adaptées aux réalités africaines, ainsi qu'à la lutte contre la cybercriminalité ;
- Encourager le développement des partenariats publics-privés dans la mise en place des écosystèmes de cybersécurité, de sorte à avoir des modèles économiques viables et efficaces ;
- Inciter les États africains à signer et à ratifier la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel – dite « Convention de Malabo » –, adoptée le 27 juin 2014. Cette convention est un instrument important dans la construction des mécanismes de coopération et de renforcement des capacités des État en matière de cybersécurité. A ce jour, seuls 11 pays - dont le Togo - l'ont ratifiée.
- Adopter la déclaration de Lomé, qui promeut la coopération entre les États africains et la mise en place de cadres opérationnels efficaces.

Cio Mag : Le renforcement du leadership du Togo, pour attirer les banques et les institutions financières, est une volonté exprimée par les autorités. Comment bâtir la confiance dans le numérique ? Quelle est la stratégie de votre pays en la matière ?

GG : La vision du Togo est de bâtir un environnement cyber sécuritaire pour offrir aux institutions financières, aux banques, aux potentiels investisseurs, mais aussi aux citoyens, un service de qualité optimal.

Pour qu'un utilisateur ait confiance dans les outils numériques, il faut que l'écosystème numérique du pays garantisse l'intégrité, la disponibilité, la confidentialité de ses données et des systèmes d'information.

Pour offrir un cyberespace, qui inspire confiance aux utilisateurs, le Togo a adopté une stratégie. Elle s'articule autour de cinq axes principaux :

- La sensibilisation de la société togolaise et le développement des compétences, via des partenariats avec les universités et les structures de formations ;
- La sécurisation de l'administration, des services essentiels et de l'économie numérique. Le Décret 2019-095/PR, relatif aux opérateurs de services essentiels, aux infrastructures essentielles et aux obligations y afférentes, décrit les principes généraux de protection des infrastructures essentielles. Il sera complété par des règles nationales de cybersécurité ;
- Le renforcement du système de réponse aux incidents de cybersécurité, avec la mise en place du CERT.tg ;
- La poursuite efficace des crimes et des délits de cybersécurité, par le renforcement des capacités des forces de l'ordre et des magistrats en investigation numérique et en répression de la cybercriminalité ;
- La régulation et l'amélioration continue des mesures de cybersécurité par l'ANCy.

Cio Mag : Pour l'heure, le Togo dispose-t-il de compétences locales suffisantes pour la cyberdéfense ? Comment les repérez-vous ?

Simon Melchior : La cybersécurité est un domaine très dynamique. Il est à la fois vaste en termes de différenciation sectorielle des attaques et pointu en matière de techniques d'attaque. La palette de compétences requise est également très large, que ce soit pour des auditeurs d'infrastructures et/ou d'applications, pour des spécialistes réseau, des pentesters ou pour des experts en criminalistique. Et pour les différents profils d'analystes, dont on a besoin, pour fournir un service complet. Il n'y a pas beaucoup de spécialistes et ils sont très demandés. Le défi, que nous relevons tous les jours au sein de Cyber Defense Africa, est de réunir toutes ces compétences, localement au Togo. Et de les former, de les motiver et de les garder. Mais, je suis heureux de vous dire que nous avons une excellente équipe, dont je suis très fier.

GG : La cybersécurité et la cyberdéfense sont des domaines transversaux. Ils nécessitent des compétences dans plusieurs secteurs : technique, juridique, communication, formations, etc.

Le Togo a la chance d'avoir l'un des systèmes éducatifs les plus performants de la sous-région. En plus, le pays dispose de structures de

Simon Melchior
Directeur Général, Cyber Defense Africa (CDA)

INTERVIEW

formation publiques et privées, tant nationales qu'internationales. Par conséquent, il existe un vivier de compétences togolaises, présent localement et à l'étranger. Notre challenge est d'adapter ces ressources aux problématiques de cybersécurité.

Pour repérer ces talents, l'ANCy a entamé des démarches, avec ces structures de formation. L'objectif est d'établir des partenariats pour les accompagner dans le renforcement de leurs capacités et de faciliter l'obtention de bourses et de formations des étudiants à l'étranger.

Cio Mag : Comment se passe la formation des locaux à la cybersécurité, en termes de compétences et de niveau de maturité des professionnels, au plan national et régional ?

SM : Il est assez facile de trouver des profils juniors, très motivés, mais, par définition, inexpérimentés. Il existe également pléthore de formations basiques et/ou théoriques en cybersécurité. Et elles sont plutôt accessibles localement. Pour nous différencier, nous nous focalisons sur l'identification de profils seniors et sur une formation à la fois poussée et pratique. Nous organisons des boots camps et des exercices de simulation d'attaques, dits cyber exe et capture the flag. Ils nous permettent de former nos collègues, de vérifier le suivi de nos process et la manière dont nous pouvons les améliorer de façon continue.

Un an après la création du Cert national, quel bilan en tirez-vous ?

SM : Aujourd'hui, je pense que nous avons fait du bon travail. Qu'il s'agisse de collaboration avec un certain nombre de ministères togolais ou avec les forces de l'ordre, le bilan est satisfaisant. Il l'est aussi en termes de sensibilisation et de collaboration avec d'autres CERT nationaux, européens, américains et africains. Cela dit, je pense que nous avons un défaut de notoriété, particulièrement auprès de la population et des PME togolaises. Or, le CERT national est là aussi pour eux. Et nous sommes bien opérationnels. Nos outils, notre personnel et nos procédures sont bien en place, mais nous n'avons pas assez communiqué auprès du public, dans son ensemble, sur le fait que nous sommes là pour lui fournir notre service. Nous comptons notamment sur un évènement d'envergure, à la fois national et international, comme le Sommet de la Cybersécurité, pour nous donner l'occasion de communiquer et de pallier ce défaut de notoriété.

Pour lutter contre les cybercriminels et les risques inhérents, un travail de sensibilisation des acteurs est fondamental. Où en-êtes-vous ?

GG : La formation et la sensibilisation des différents acteurs des administrations, des entreprises et du public, sur les enjeux de la cybersécurité, est l'une des missions dévolue à l'ANCy. Dès notre prise de fonction, nous avons lancé une campagne de sensibilisation. Elle s'est effectuée en collaboration avec Cyber Défense Africa, le bras opérationnel de l'ANCy. Et s'est adressée à certaines administrations, qui présentent de graves vulnérabilités en sécurité informatique.

Une autre campagne, dédiée aux opérateurs de services essentiels, en est cours. Elle a vocation à les accompagner et à renforcer la sécurité de leurs systèmes d'information. Et dans les prochaines semaines, une campagne de sensibilisation, cette fois-ci destinée au grand public, va démarrer.

Comment se positionne le Togo par rapport à ses pairs ouest-africains dans la gestion du cyberespace ?

GG : Nous avons l'ambition de positionner le Togo comme un des leaders en la matière et d'être le moteur de l'intégration sous-régionale et de la coopération en cybersécurité. Le cadre légal et réglementaire, que nous avons mis en place depuis 2018, contribue à cela, tout comme la création de l'ANCy et de CDA, qui est un modèle opérationnel basé sur un partenariat public privé.

Comme je l'ai dit précédemment, l'un des objectifs de ce sommet est le développement de la coopération continentale en matière de cybersécurité. Ce sommet est une occasion pour entamer des discussions et pour jeter les bases d'une coopération opérationnelle entre les différentes agences de cybersécurité en Afrique.

Propos recueillis par Souleyman Tobias

ANALYSE

« Nous sommes les premiers protecteurs de nos données personnelles ! »

Depuis une dizaine d'années, l'Afrique a fait le pari de la protection des données. Qu'est-ce qui a présidé à cette prise de conscience ? Ce pari est-il aujourd'hui gagnant ? L'Ivoirien Léon Brandre, CEO du Groupe DPSE (Data Privacy Solution Expert), nous fournit un éclairage.

Léon Brandre
Directeur général du Groupe DPSE

Cio Mag : Depuis plus de dix ans, plusieurs pays africains ont marqué leur intérêt pour la protection des données en adhérant à l'Association francophone des autorités de protection des données personnelles (AFAPDP). Quel a été le déclic ?

Léon Brandre : C'est l'inéluctable montée de la technologie sur le continent qui a sonné l'alerte. L'Afrique s'est depuis longtemps positionnée comme un marché de choix pour le matériel des TIC. En 2012, les statistiques d'importations mondiales d'équipement TIC pointaient à 11,6% sur le continent pour les ordinateurs et les équipements périphériques, et à 27,7% pour les composants électroniques. Et c'est sans compter sur la grande vague de transformation digitale adoptée par les entreprises. A commencer par les sociétés de téléphonie mobile, qui se sont lancées dans la diversification de leurs offres et ont rivalisé de moyens technologiques.

Mais, l'utilisation des technologies va de pair avec le traitement automatisé des données personnelles et induit un risque de violation de la vie privée. C'est ce qui a poussé l'Afrique à s'engager sur la voie de la protection des données personnelles. Cela dit, il est bon de préciser que l'AFAPDP a été créée, en septembre 2007, à Montréal, avec l'appui de l'Organisation internationale de la francophonie. Parmi les 21 membres qui la composent, à ce jour, dix sont africains. En revanche, la détermination de l'Afrique remonte à 2010, quand a été signé l'Acte additionnel relatif à la protection des données à caractère personnel dans l'espace CEDEAO. Cet acte marquait déjà la volonté des pays membres à se mettre à niveau. Dans le même élan impulsé par la CEDEAO, le Réseau africain des autorités de protection des données personnelles (RAPDP) a été créé en 2016, au Burkina Faso.

Cio Mag : Ce dynamisme autour des données s'avère-t-il gagnant aujourd'hui ou faut-il souhaiter l'avènement d'un RGPD africain ?

L.B : Ce serait peut-être mettre la charrue avant les bœufs que de penser déjà à l'avènement d'un RGPD africain. En réalité, certains pays, comme le Sénégal, abattent un travail colossal. D'autres pays sont en revanche plus à la peine. Pour la première catégorie d'entre eux, l'amélioration du secteur de la protection des données personnelles est une quête permanente. Quant à la seconde, la gageure est de rechercher les causes profondes du manque de dynamisme de l'activité. Et le problème peut se situer à deux niveaux : alternatifs ou cumulatifs. Selon le cas, il s'agit du droit positif interne des pays africains en matière de données personnelles ou de l'implication de l'autorité de protection.

Cio Mag : Que préconisez-vous ?

L.B : Au vu de l'évolution technologique de la société et de l'environnement de la pratique de l'activité même de protection des données personnelles, il faut, de prime abord, penser au lifting profond de nos lois locales. Par exemple, il est temps d'ouvrir le débat sur les bases légales recevables en Côte d'Ivoire, en actualisant l'article 14 de la loi sur la protection des données à caractère personnel. Et aussi engager des discussions pour en finir avec les procédures administratives de déclarations et d'autorisations de traitement. Ceci de sorte à souscrire au principe « d'accountability », lequel repose sur la responsabilisation totale des entreprises.

Il faut ensuite revoir l'adaptation des autorités de protection dans nos pays. Nous parlons d'adaptation, surtout pour le modèle ivoirien, qui est, tenez-vous bien, un véritable cas d'école dans le monde entier !

Cio Mag : Quelle en est la cause ?

L.B : La Côte d'Ivoire est le seul pays au monde où l'autorité de protection n'a pas été créée, mais a été désignée. Le législateur ivoirien a décidé de confier les charges de l'autorité de protection à une autorité qui existe déjà : l'Autorité de régulation des télécommunications/TIC de Côte d'Ivoire (ARTCI). Elle se voit désignée par l'article 46 alinéa 1 de la loi de 2013.

Léon Brandre
Directeur général
du Groupe DPSE

INTERVIEW

Aujourd'hui, il faut analyser profondément la situation de l'ARTCI et déceler si cette autorité est bien placée, dans sa structure et son organisation, pour porter la casquette d'autorité de protection. Nous pensons que cette configuration n'est pas celle qui convient. Pour que la protection des données personnelles soit plus efficiente, une autorité doit être mise en place indépendamment de l'ARTCI.

Les autorités de protection doivent aussi booster leur engagement dans la sensibilisation et la vulgarisation de la discipline. Une fois ces contours revisités, nous pourrions alors aborder la question d'un éventuel RGPD africain. Par ailleurs, l'Afrique dispose aussi d'une convention sur la cybercriminalité et la protection des données à caractère personnel. Elle a été adoptée le 27 juin 2014, à Malabo. Plusieurs pays l'ont ratifiée. Cependant, le bilan n'est toujours pas reluisant. Les pays africains qui n'ont pas encore ratifié cette convention gagneraient à le faire.

Cio Mag : Le citoyen lambda a-t-il conscience de ses droits ? De quels moyens dispose-t-il pour les exercer ?

L.B : On ne cessera de le dire, les premiers protecteurs de nos données personnelles, c'est nous même ! Cependant, le citoyen lambda n'a en général pas conscience de ses droits en la matière. Le premier moyen pour lui d'exercer un contrôle sur ses données est de se former et de s'informer sur le sujet.

Il existe plusieurs moyens juridiques de veiller sur ses données. Nous pouvons en citer quelques-uns : **le droit à l'information**, qui oblige le responsable de traitement à informer l'utilisateur préalablement à la mise en œuvre d'un traitement de données ; **le droit d'accès** qui permet de demander d'accéder aux données et de vérifier comment elles sont traitées ; **le droit de modification** pour la mise à jour ou la modification, par le responsable de traitement, des données des usagers ; **le droit à la suppression** pour supprimer purement et simplement ses données personnelles. Le citoyen lambda, que nous appelons dans notre jargon la personne concernée, doit savoir comment exercer concrètement ses droits.

Cio Mag : Que fait le Groupe DPSE pour favoriser cette prise de conscience ?

L.B : Nous publions fréquemment des articles sur notre portail web. Ils informent les personnes concernées et les responsables de traitement. Nous organisons également des afterwork en présentiel, lesquels vont désormais se transformer en webinaires, avec des rencontres physiques, au fil de l'eau, dont nous maintiendrons la gratuité. Le Groupe DPSE est vraiment satisfait de ses actions. Elles se poursuivent à présent avec l'édition de la première bande dessinée de sensibilisation sur les données personnelles.

Cio Mag : Compte-tenu de l'explosion des moyens de collecte d'informations, ce combat n'est-il pas perdu d'avance ?

L.B : Non, nous pensons que ce combat n'est pas perdu d'avance. A l'instar des pays européens, qui ne font qu'adapter leurs lois à l'évolution de la technologie, nous, Africains, n'avons pas intérêt à baisser les bras ! Les actions juridiques menées font contrepoids à cette machine contemporaine qu'est la technologie. Qu'adviendrait-il si nous baissions totalement les bras ? C'est donc le moment, surtout pour nous, Africains, de poser des bases très solides pour nous protéger et pour protéger les générations futures. L'inaction, face au traitement à grande échelle des données à caractère personnel, serait une véritable catastrophe !

Cio Mag : S'agissant des entreprises qui traitent des données, quelles sont leurs obligations ?

L.B : Les entreprises responsables de traitement doivent obligatoirement prévoir des procédures pour que la personne concernée exerce librement ses droits. Et le moyen le plus sûr pour y parvenir, c'est qu'elles s'inscrivent dans une démarche de mise en conformité à la loi relative aux données personnelles de leurs pays respectifs. Il n'y a que l'implémentation de cette démarche qualité qui respecte les principes directeurs de la loi. Et les standards internationaux vont leur permettre de rassurer leur personnel, leurs partenaires et usagers, mais aussi de garder un avantage concurrentiel certain sur le marché.

Le Groupe DPSE assure, à ses partenaires, ce travail d'accompagnement et d'assistance pour l'implémentation de la conformité réelle dans les entreprises. A ce titre, nous tenons à rappeler aux entreprises africaines que la conformité ne se limite pas au remplissage de formulaires et à l'obtention d'autorisations délivrées par leurs autorités de protection. La conformité réelle, c'est l'implémentation de toutes les procédures en tenant compte des mesures juridiques, organisationnelles et techniques, qui assurent la sécurisation de la vie privée.

Cio Mag : Quel est votre analyse sur la prolifération des cyberattaques sur les données personnelles ?

L.B : Actuellement, les données personnelles sont le nouvel or noir. Les cibles principales de ces attaques sont les entreprises. En Afrique tliés à la cybersécurité sont occasionnés par l'hameçonnage et les logiciels malveillants.

Selon une étude de Deloitte sur la maturité cybersécurité 2021 en Afrique francophone, ces deux types d'attaques constituent, à eux seuls, 78% des préjudices subis par les entreprises. Ces attaques viennent nous rappeler l'importance, pour les entreprises, d'investir fortement dans la sécurisation de leur cyberespace.

Malheureusement, la réaction des entreprises n'est pas à la hauteur des risques de cyberattaques auxquels elles font face. La même étude de Deloitte souligne très clairement que les budgets dédiés à la cybersécurité restent insuffisants. En effet, 66% des entreprises investissent moins de 130 millions de FCFA (200.000 €) par an. Les menaces liées à la cybersécurité devraient pourtant les faire réagir. Il est vital, pour leur business, que les entreprises s'engagent sur la voie de la conformité. La protection des données personnelles et la lutte contre la cybercriminalité sont deux faces d'une même pièce. Pour preuve, la convention de Malabo lie ces deux domaines, avec d'une part la cybersécurité et d'autre part la protection des données à caractère personnel. Tous les pays africains devraient donc se doter d'une loi sur la cybercriminalité et/ou ratifier la convention de Malabo pour assurer, à leurs concitoyens, un minimum de sécurité et de sérénité sur Internet.

Cio Mag : En conclusion, pourquoi la protection des données est-elle si problématique pour les Etats, les entreprises et les citoyens ?

L.B : C'est principalement dû à la mauvaise compréhension du sujet par les entreprises et les citoyens, qui sont pourtant des acteurs à part entière de ce secteur. Nous constatons aussi un certain flou, notamment dans les lois relatives à la protection des données personnelles de certains pays africains.

Les Etats ne sont, en outre, pas suffisamment informés et impliqués dans le développement de la discipline. C'est peut-être la raison pour laquelle peu d'Etats africains ont ratifié la convention de Malabo. En définitive, dans chaque pays africain, des cadres d'échanges doivent être créés entre les autorités de protection et tous les autres acteurs du secteur pour une meilleure compréhension de la discipline. Et pour l'établissement de référentiels solides et adaptés à nos différentes sociétés.

Propos recueillis par Anselme Akeko

DROIT DES DONNÉES

Une bande dessinée rappelle les obligations des entreprises

Parce que les entreprises n'ont pas toujours conscience de leurs obligations vis-à-vis de la loi, une bande dessinée vient d'être publiée pour le leur rappeler.

Anselme AKEKO

L'objectif de la bande dessinée, publiée par le Groupe ivoirien Data Privacy Solution Expert (DPSE), est de sensibiliser la population sur le caractère confidentiel d'un certain nombre d'informations contenues dans des documents papiers retrouvés sur la place publique. Leur cible ? Les organismes publics et privés, autant que la « personne concernée », c'est à dire le citoyen lambda, dans le jargon des spécialistes de la protection des données à caractère personnel.

Cette BD s'intitule *« La protection des données personnelles ; le CV refoulé, réceptacle des bananes Alloco »*. Elle relate les conditions dans lesquelles une femme, nommée Anna, découvre que le papier qui a emballé ses aliments est son propre curriculum vitae (CV). Consciente de ses droits, elle se rend dans cette entreprise pour réparer ce préjudice.

Respect des obligations

A l'instar des dossiers médicaux ou bancaires, le CV contient une mine d'informations, qui peut permettre d'identifier une personne, de savoir où elle réside et quelle activité elle mène. Il n'est donc pas normal qu'un document de cette nature se retrouve dans la rue, martèle Léon Brandre, directeur général du Groupe DPSE.

Et quand il se décide à publier cette BD, c'est pour rappeler aux entreprises le respect des obligations qui encadrent la gestion des informations ou des données qu'elles sont amenées à collecter. Faute de quoi, toute personne concernée par ces informations peut saisir la justice, si elle estime que ses droits ont été bafoués, affirme l'expert en management et protection des données à caractère personnel.

Publireportage

INNOVATION

« Progress Protected aide à l'adoption et à la transition vers un monde numérique protégé »

Leader européen en matière d'édition de solutions de sécurité, ESET développe des produits pour la protection des données, la sécurité cloud et la protection endpoint. L'entreprise, qui s'est engagée pour le progrès, mise sur la protection de l'innovation et invente « Progress protected. » Une avancée dont parle fièrement Benoît Grunemwald, directeur associé ESET France & Afrique francophone, qui cumule une vingtaine d'années d'expériences au sein du groupe. Interview.

Benoît Grunemwald
Directeur associé ESET France & Afrique francophone

Cio Mag : Quel constat faites-vous sur les cyber-risques dans le monde et en Afrique ?

Benoît Grunemwald : La transformation numérique est en marche chez les particuliers et dans les entreprises. Il y a une avancée particulière en Afrique, notamment par rapport au paiement mobile et à une utilisation très nomade centrée sur le Smartphone. A contrario, la protection du Smartphone est sous-estimée dans les sociétés, comparativement à l'ordinateur. Ce qui est très dommageable pour une organisation très portée sur le Smartphone, surtout en raison des informations cruciales contenues dans ces appareils. Les cyber-risques dans le monde et en Afrique demeurent les mêmes : les données sensibles et l'argent.

Pour les particuliers, il peut s'agir d'une escroquerie au moyen de paiement. Les jeunes générations sont quant à elles exposées à l'addiction aux réseaux sociaux et à la perte de contrôle sur leur vie numérique. Ces dangers et leur fusion avec ceux de la vie réelle se retrouvent dans le monde numérique. Dans les entreprises, on note une perte de productivité, voire un arrêt de production.

Ces termes sont souvent assimilés au secteur industriel, mais concerne toutes les entreprises. Les Etats font également face à des risques de déstabilisation, d'ingérence, de fakenews ou de cyber-espionnage.

Pour son développement, le monde connait un progrès humain et technologique assez fulgurant. Quelles sont les failles de sécurité que laisse entrevoir ce processus ?

B.G : Le premier risque est la sécurité des données. Dans cette course à la technologie, on invente de nouveaux outils et des suivis d'activité. A lui seul, le Smartphone regroupe énormément de fonctionnalités génératrices de données. On lui confie et il produit beaucoup de données, dont il faut assurer la protection de l'intégrité, la disponibilité et la confidentialité. C'est un paramètre que l'on souhaite porter à la connaissance de tous ceux qui utilisent les technologies et de ceux qui innovent.

Tout ceci est très bénéfique pour nos sociétés, mais il ne faut pas oublier que ces données, parfois personnelles, peuvent être détournées ou utilisées à des fins moins bienveillantes que celles prévues au départ. La problématique n'est pas de savoir si les dispositifs antiviraux existent pour les téléphones, mais s'ils sont adoptés. C'est là que se trouve notre combat, celui de sensibiliser et de faire adopter, dans cette nouvelle technologie, la protection et les comportements qui vont de pair.

Fidèle à son positionnement de premier éditeur européen de solutions de sécurité, ESET innove en créant le concept Progress Protected. Pourquoi avoir suscité la réflexion sur le sujet ?

B.G : Il nous semblait important d'élargir le débat de la protection en ne le restreignant pas seulement à l'antivirus, même s'il y a un concept de protection de l'innovation et de la technologie d'ordre universel. Cette notion reprend l'ensemble des cyber-risques précédemment annoncés : la protection des plus jeunes, de l'innovation, de l'industrie, etc. C'est ce qui se cache derrière Progress

Benoît Grunemwald
Directeur associé
ESET France & Afrique francophone

INTERVIEW

Protected, une innovation qui aide à l'adoption et à la transition vers le monde numérique qu'il faut protéger.

Pour nous, c'est une modification dans nos sociétés. Nous avons connu des inventions très importantes comme la machine à vapeur, mais, rétrospectivement, elle est sans commune mesure avec l'invention de la connectivité et le monde numérique dans lequel nous sommes. Ces technologies impactent beaucoup plus nos sociétés que la machine à vapeur.

Quels sont vos offres de logiciels et de services de cybersécurité pour soutenir cette avancée ? Et quelle est la cible de cette nouvelle signature futuriste ?

B.G : Cela passe par deux volets. Le premier consiste à protéger un maximum de technologies passées, actuelles et futures. Le passé fait référence aux industries qui utilisent encore des systèmes obsolètes, lesquels doivent néanmoins être protégés, à l'instar des Smartphones. Il faut aussi protéger le futur, à travers toutes les nouvelles technologies qui vont émerger : les cryptomonnaies, les NFT, etc. Enfin, il convient de protéger la société dans son ensemble, soit par des logiciels, soit par l'expertise humaine, les conseils et la sensibilisation. Cette nouvelle signature futuriste a une cible mondiale et universelle. On se rend compte que la technologie touche, de manière directe ou indirecte, l'intégralité de nos sociétés. On se doit donc de ne rien oublier dans l'accompagnement de l'utilisateur dans sa vie numérique.

Quelles sont les règles d'une vie numérique éthique pour les internautes, les entreprises et les gouvernements africains ?

B.G : Il est important de noter qu'il n'existe pas de sécurité à 100%. La sécurité est un chemin à mener, sur lequel il faut avancer avec tous les acteurs de la spirale numérique. Au final, tout le monde est un acteur du numérique. Et pour que la vie sur le net soit éthique, il faut prendre en compte le Privacy by design. Je fais référence à tous ceux qui partagent ces valeurs, notamment les acteurs de la régulation européenne sur la donnée personnelle, qui incluent la notion de Privacy by design ou de Security by design. Le maître-mot pour tout acteur du numérique, c'est de réfléchir à sa propre sécurité et de faire en sorte que l'usage du numérique soit une valeur ajoutée pour tout le monde, sans en détourner les bénéfices dans son propre intérêt.

Propos recueillis par : Michaël Tchokpodo

Benoît Grunemwald travaille pour la société ESET en France et en Afrique depuis plus de 17 ans. A la base, il a une formation technique en électronique mais s'est rapidement tourné vers la cybersécurité. Aujourd'hui, il fait le lien entre la recherche, la découverte des menaces, leur analyse auprès des gouvernements, des associations et toute entité intéressée par sa cyberprotection. ESET est une entreprise européenne, qui a plus de 30 années d'existence. Sa mission est d'assurer la protection des organisations, de protéger et de sensibiliser au monde numérique.

FORMATION

L'ESMT, une réponse sous-régionale pour parer aux urgences

Le besoin de protection des systèmes d'information ne laisse aucun choix à l'improvisation. Les risques d'incidents informatiques provoqués par des attaques sont au cœur des stratégies de digitalisation de l'Afrique. Mais, pour un continent dont la numérisation s'accélère, tout porte à croire qu'il y a encore d'énormes défis à relever pour répondre aux enjeux de la sécurité.

Souleyman Tobias

Adamou Moussa Saley
Directeur général de l'ESMT

A l'instar des data centers, qui sont de plus en plus usités, l'Afrique a pris conscience de la nécessité de former ses propres ressources humaines pour la défense des systèmes d'informations. Les cyber-menaces n'épargnent pas le continent, que ce soient les infrastructures publiques ou privées. Et la majorité de l'expertise continue d'être exportée. Mais, peut-être plus pour longtemps ? C'est en tout cas ce que l'on serait tenté de croire lorsqu'on suit les discours politiques sur les stratégies nationales de cybersécurité. Progressivement, le continent se dote en effet des mécanismes nécessaires pour assurer une sécurité informatique optimale via des équipes de réponses (CERT), des autorités de protection des données, des lois sur la cybersécurité…. Seulement, les compétences locales sont encore loin de répondre à la demande. Face à l'urgence, des initiatives communautaires voient le jour.

Une école pour répondre aux défis de la transformation digitale

L'Ecole supérieure multinationale des télécommunications (ESMT) se positionne aujourd'hui comme un mécanisme sous-régional pour répondre aux défis inhérents à la transformation digitale du continent. Créée en 1981, l'ESMT s'adapte à la mutation numérique sur le continent. *« Une étude sur les besoins de formation a été menée au Sénégal pour identifier toutes les compétences requises dans le domaine du numérique »*, confie Adamou Moussa Saley, Directeur général de l'ESMT.

Les résultats de cette étude ont amené l'école à proposer des programmes de formation, dont la cybersécurité. Pour doter les Etats, les entreprises et les autres entités, de ressources qualifiées, l'ESMT dispense des formations de courtes et longues durées, selon les besoins et les parcours. Le but est de *« traduire en programme de formation tous les besoins identifiés »*, explique Adamou Moussa Saley.

Pour mener cette mission, l'ESMT s'est entourée de tous les acteurs de l'écosystème de la sous-région. Opérateurs télécoms, régulateurs, start-up, institutions publiques… tous sont impliqués dans l'anticipation des besoins. *« En ce qui concerne la formation initiale, nous proposons des modules de sécurité et de cybersécurité, dans les différents programmes que nous dispensons, notamment les programmes de Licence professionnelle Réseaux et Télécoms (Sécurité système et réseau) et de Licence professionnelle en Télécommunications et Informatique avec une spécialité en administration et sécurité réseau (ASR). Cette spécialité, qui est orientée dans la gestion de la sécurité des systèmes et réseaux, dote nos étudiants des compétences clés pour répondre aux attaques et garantir la sécurité des systèmes et des plateformes de services. Nous disposons aussi de programmes de Masters (BAC +5) dédiés »*, témoigne Moussa Saley.

Des talents pour le continent

Même s'ils ne sont pas forcément formés sur le continent, les talents africains en cybersécurité existent. Seulement, leur environnement ne les incite pas suffisamment à rester. Alors, les pouvoirs publiques et les entreprises sont appelés à proposer à ces experts - souvent des repats - des mécanismes incitatifs pour qu'ils mettent leur expertise au profit du continent.

A l'ESMT, la stratégie mise en place consiste à valoriser les talents formés auprès des partenaires publics et privés. L'écosystème du continent sera en effet perdant s'il laisse partir les talents formés sur place. Pour le DG de l'ESMT, *« il revient aux entreprises africaines de se doter des politiques de fidélisation des ressources humaines et des talents. Et de créer le cadre de leur épanouissement et surtout de mettre en place des plans de carrière »*. A défaut, les talents locaux partiront vers d'autres horizons. Et pour cause. *« Derrière la sécurité, se cache aussi des enjeux business. Toute entreprise a pour défi de se mettre à l'abri des cyberattaques. Même les Etats, aujourd'hui, ne sont pas épargnés par la menace. C'est pourquoi un expert en cybersécurité, doté de compétences pointues, est recherché partout dans le monde. Il n'est pas exclu de voir s'expatrier les talents africains, qui ont été formés par nos soins, au sein de nos laboratoires à Dakar, dans une entreprises à Londres, à Dubaï, à New York ou dans la Silicon Valley. C'est le cas des cryptologues »*, fait observer Moussa Saley.

« La sensibilisation et la formation sont le pare-feu idéal contre les cyberattaques », expliquait, dans une récente tribune, Eric Heddeland, VP EMEA chez Barracuda Networks. Le Directeur général de l'ESMT ajoute que la formation d'un expert en cybersécurité, avec des compétences pointues, coûte cher. D'où l'impératif de retenir les talents locaux. Ce à quoi travaille l'école sous-régionale. Elle tient les meilleurs étudiants experts en cybersécurité à la disposition des Etats et des grands groupes, comme la Banque mondiale, la SONATEL, FREE Sénégal et d'autres opérateurs dans les pays membres.

Sensibiliser les acteurs aux enjeux

L'humain reste le maillon le plus faible du chainon de la cybersécurité. Garantir une meilleure sécurité des infrastructures et des systèmes d'information nécessite de sensibiliser tous les acteurs aux enjeux. Ce n'est donc plus la seule affaire des DSI.

A l'ESMT, la problématique de la formation de masse est déjà abordée. La bonne connaissance des sujets de cyber attaque, par les chefs d'entreprises, les collaborateurs et les décideurs, accentuera l'efficacité des solutions mises en place par les experts pour la cyberdéfense et la protection. *« Au regard du caractère transverse de la cybersécurité, nous souhaiterions organiser des formations de haut rang destinées aux dirigeants d'entreprises. L'idée est de sensibiliser, d'accompagner et de doter de compétences pointues les chefs d'entreprises, pour leurs prises de décisions »*, annonce le Directeur général de l'école sous-régionale.

L'ESMT, qui est un centre d'excellence de l'UIT, répond ainsi progressivement au défi de la formation en cybersécurité sur le continent. A côté de cette initiative inter-Etats (Bénin, Burkina Faso, Mali, Mauritanie, Niger, Sénégal, Togo et Guinée), d'autres initiatives privées naissent sur le continent. Des universités et des instituts privés proposent de former des talents. Ces centres de formations, qui sont généralement tenus par des consortiums étrangers ou par des experts africains formés dans de grandes universités, ont de beaux jours devant eux tant la demande va crescendo. Et si on ajoute la dématérialisation des formations, qui permet de se former à distance, tout porte à croire que l'expertise locale pourra progressivement répondre au besoin du marché africain de la cybersécurité.

ENTREPRISE

Kaspersky, « un acteur majeur » de la cybersécurité en Afrique

Fort de ses 25 ans d'existence, l'éditeur de solutions de cybersécurité Kaspersky s'impose en Afrique depuis plus de 15 ans. Parmi ses clients, des entreprises de différents secteurs d'activités et des administrations publiques, qu'il célèbre en appuyant l'évolution de la cybersécurité sur le continent.

Aurore Bonny

Pour accompagner la montée en compétences techniques en matière de cybersécurité ou pour fournir les solutions technologiques les plus à la pointe, Kaspersky et son réseau de partenaires se déploient sur le continent africain depuis plus de 15 ans et les régions de l'Afrique de l'Ouest et du Centre sont directement gérées par une équipe dédiée, rattachée à Kaspersky France, depuis 2018. Son équipe travaille auprès de clients composés d'entreprises ou de particuliers de divers secteurs d'activité, mais également avec des administrations publiques.

Kaspersky assure la protection des systèmes avec l'objectif *« d'implanter une dynamique vers l'instauration de nouvelles technologies plus à la pointe et adaptées à la réalité de la menace »*. Hervé Iro Mondouho, Territory Channel Manager sur l'Afrique de l'Ouest et du Centre, au sein de cette entreprise, explique que les clients peuvent notamment se prémunir contre les attaques lancées via la compromission de logiciels légitimes. Selon son manager Pascal Naudin, Head of B2B Sales sur le continent africain, il est également question *« de renforcer la cyber-hygiène, afin que les utilisateurs deviennent un maillon fort dans la chaine de protection des systèmes d'information et des actifs de l'entreprises »*.

Dans la poursuite de ces aspirations, l'éditeur a un regard d'expert sur l'état général de la cybersécurité des entreprises africaines. Dans le rapport Interpol 2021 sur l'évaluation des cybers menaces dans la région, et dont

Kaspersky est partenaire, il est rapporté que 90 % des entreprises africaines n'utilisent pas les protocoles de cybersécurité nécessaires. Il constate également un manque de sensibilisation du personnel sur la cybersécurité, notant que de nombreuses entreprises ne disposent pas de politique ou de stratégie pour amener le personnel à comprendre les enjeux de la cybersécurité, tout comme l'impact d'une cyberattaque sur le plan financier et sur la réputation de l'entreprise.

Toutefois, Kaspersky constate que les gouvernements des différents Etats Africains font des efforts. Ils concernent la mise en place de lois sur la cybercrimalité et sur la protection des données à caractère personnel, l'élaboration de stratégies nationales de cybersécurité et de structures telles que les CERT nationaux.

« L'obligation des entreprises dans le secteur bancaire et des télécommunications à être en conformité vis-à-vis de certaines réglementations, telles que la norme PCI DSS pour les banques, les a poussées à effectuer d'importants investissements pour mettre à niveau leur système d'information, de sorte à se prémunir contre les cyberattaques », soulignent les experts. De leur point de vue, il y a d'énormes efforts à faire pour maintenir la confidentialité et l'intégrité des données, ainsi que la disponibilité des services, dans certains secteurs tels que les établissements de santé, l'industrie, etc.

L'approche humaine privilégiée

Face à ces lacunes, Kaspersky se positionne en tant qu'expert, avec des équipes de recherche et développement qui travaillent en continuité vers l'adaptation des technologies à la réalité des menaces. *« Notre équipe de chercheurs est également active dans la recherche, notamment celle des groupes malveillants les plus sophistiqués. Elle fournit à nos clients une vision en temps réel de la menace, pour qu'ils puissent l'analyser, la comprendre et s'en prémunir »*, atteste Pascal Naudin.

D'après Hervé Iro Mondouho, les outils de Kaspersky détectent plus de 380 000 nouveaux échantillons de malware par jour, que les solutions du groupe sont en mesure de bloquer. *« Nos partenaires nous reconnaissent comme un acteur majeur. Nous avons reçu, depuis plusieurs années consécutives, les meilleures notes au Gartner Peers Insight. »* Son collègue poursuit en confirmant que Kaspersky privilégie une approche humaine et de proximité, et que ses acteurs sont présents sur le terrain, dans les différents pays de la région africaine. L'éditeur d'antivirus travaille avec un canal de distribution bien structuré, apte à couvrir les besoins de toutes tailles et les divers projets des clients.

Dans cette lancée, Kaspersky peut compter sur Aitek, son distributeur historique en Afrique de l'ouest et en Afrique centrale. Il constitue un centre ATC (Authorize Training Center), lequel contribue à la formation des partenaires et des clients finaux sur les technologies de Kaspersky. Redda Ben Geloune, son promoteur, assure que ce distributeur est à valeur ajoutée. Sa vision est de devenir la première licorne ivoirienne à utiliser le levier offert par la convergence des nouvelles technologies, pour résoudre les grands challenges de l'Afrique. *« Notre mission est d'impacter positivement notre continent en aidant nos partenaires à créer des entreprises qui gagnent et en se positionnant comme un allié incontournable, dont l'expertise, le professionnalisme et la proximité sont reconnus par tous »,* scande-t-il.

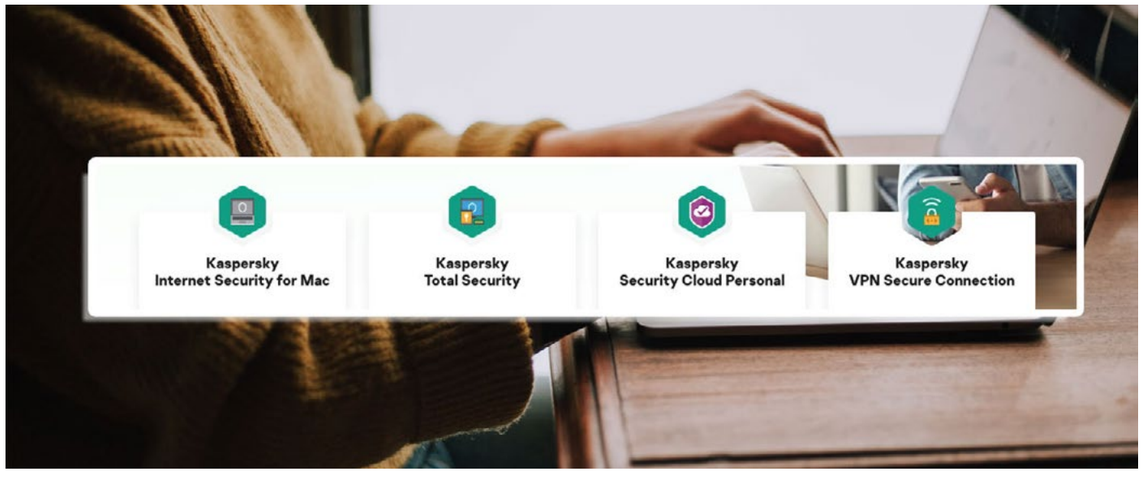
Aitek est déployé en Côte d'Ivoire, au Sénégal, au Burkina Faso, au Mali, avec des représentations commerciales au Ghana, au Cameroun, en France et aux Emirats Arabes Unis. Son catalogue est composé de 17 constructeurs HW et d'éditeurs de logiciels tels que Kaspersky, Microsoft, HP, DELL, Lenovo, Canon, Epson, etc. Et à son actif, 2000 revendeurs positionnés dans plus de 20 pays.

Partenariat gagnant-gagnant

Avec 20 années d'existence, Aitek est une marque reconnue non seulement par les revendeurs, mais également par les grands comptes. Son équipe est composée de plus d'une centaine de collaborateurs, qui bénéficient d'une maitrise parfaite des spécificités du continent et de la topologie de son marché. Ce statut permet aux fournisseurs de construire une activité pérenne, tout en adressant les opportunités latentes qui regorgent sur un marché en plein essor. L'entreprise a signé son contrat de distribution régional avec Kaspersky en 2008, à l'époque où le continent africain était directement géré par le siège à Moscou. *« Ensemble, nous avons posé les jalons d'une collaboration gagnant-gagnant. Année après année, nous avons progressivement réussi à faire de Kaspersky une marque reconnue dans nos pays pour la fiabilité de ses solutions, ainsi que pour la consistance de son approche commerciale, dans le respect de ses partenaires et des spécificités locales »*, rapporte Redda Ben Geloune. Et d'ajouter que le partenariat, qui se poursuit actuellement, a permis d'améliorer le temps de réponse et a réduit les barrières liées à la langue lors des visites conjointes. Son entreprise, dont la cybersécurité est l'un des piliers, apprécie l'importance des investissements locaux, ainsi que la formation des partenaires, de sorte à garantir l'exécution à long terme, tel que le perçoit Kaspersky.

Redda Ben Geloune apprécie également le fait que la vision, l'humain et l'amour profond pour l'Afrique soient au cœur de la politique de son éditeur partenaire. Ensemble, ils planifient le KNEXT Africa, un évènement qui a lieu le 16 mars, en Côte d'Ivoire. Et sera la clé de voûte d'une année à venir chargée de projets en matière de cybersécurité. *« Ce rendez-vous résonne par-delà nos frontières. Il alerte non seulement nos partenaires de la cartographie des risques, mais leur présente aussi l'artillerie de solutions que nous pouvons mettre à leur disposition, de sorte que l'Afrique bénéficie des mêmes défenses que les autres continents »*, conclut le dirigeant d'Aitek.

Kaspersky participe également cette année au Cyber Africa Forum, qui se tiendra en Côte d'Ivoire en mai, sans oublier plusieurs autres évènements, qui célèbreront ses 25 années d'existence.



CYBERMENACES
Quels sont les pays africains les plus vulnérables ?

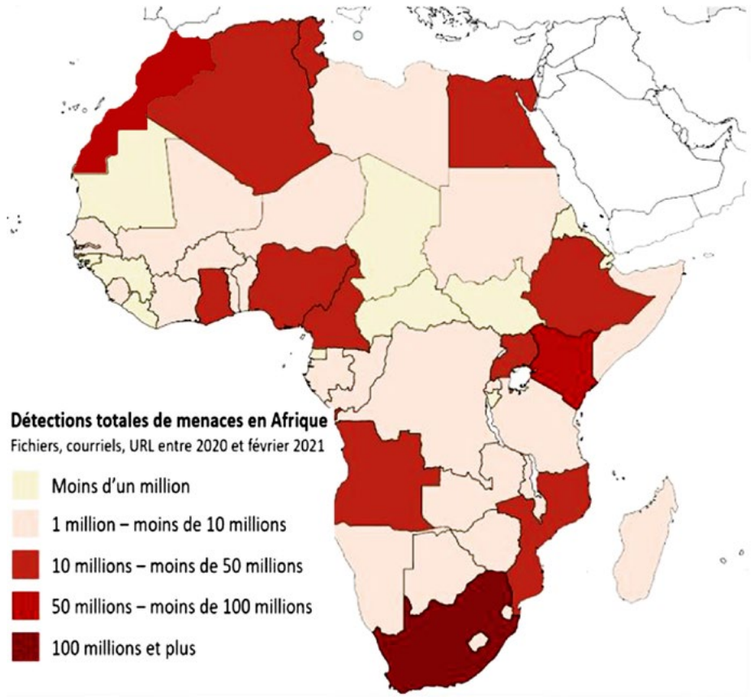
L'Afrique n'est pas épargnée par les cybermenaces. En 2020, le continent a enregistré une hausse soutenue de 238 % des cyberattaques. Dans son rapport intitulé « Evaluation 2021 des cybermenaces en Afrique », Interpol révèle qu'elles visent ses infrastructures essentielles et ses plateformes bancaires en ligne. Quels sont les pays les plus touchés par le phénomène ? Analyse.

Enock Bulonza

La pandémie de Covid-19 a accéléré l'essor de l'écosystème de la cybercriminalité, avec une fracture numérique persistante et des vulnérabilités de cybersécurité croissantes en Afrique. D'après Interpol, 90 % des entreprises africaines n'utilisent pas les protocoles de cybersécurité nécessaires.

Trend Micro, un partenaire d'Interpol, a enregistré des millions de détections de menaces en Afrique, entre janvier 2020 et février 2021. Ces attaques concernent : les courriels (679 millions de détections), les fichiers (8,2 millions de détections) et le web (14,3 millions de détections).

Ces attaques ont été principalement signalées en Afrique du Sud et au Botswana. Ainsi, en Afrique du Sud, Life Healthcare Group, une organisation qui gère 66 établissements de santé, a été victime d'une cyberattaque grave et durable. Plus spécifiquement, l'Afrique du Sud a enregistré, au total, 230 millions de détections de menaces, contre 72 millions au Kenya et 71 millions au Maroc. En Afrique du Sud, 219 millions de détections ont concerné des menaces liées aux courriels. Ce pays a également affiché le taux le plus élevé de tentatives ciblées de rançongiciels et d'escroqueries aux faux ordres de virement (FOVI).



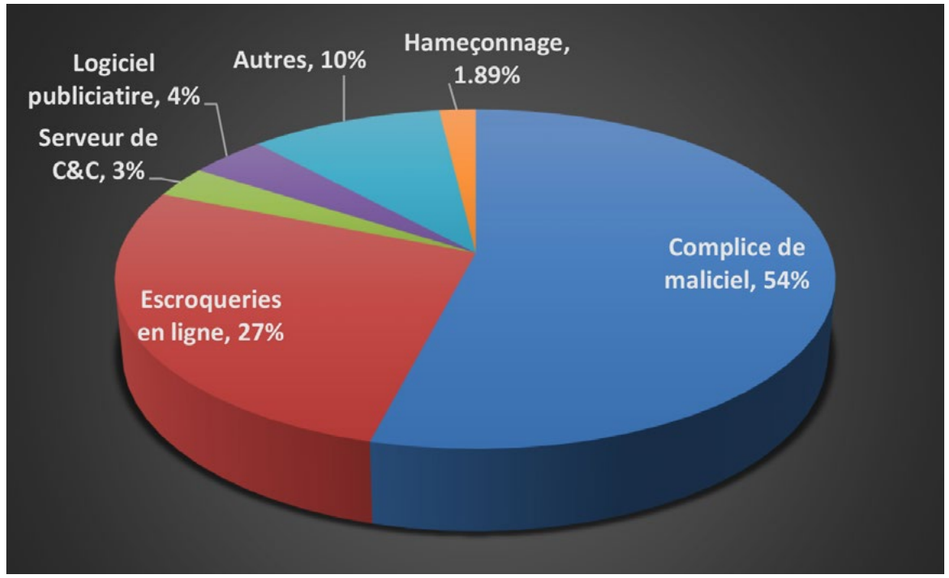
Détection globale des cybermenaces en Afrique à l'aide des capteurs de Trend Micro

Escroquerie en ligne : l'Afrique du Sud, la grande perdante

Dans son rapport, Interpol note que l'escroquerie en ligne représente la cybermenace la plus fréquemment signalée et la plus pressante en Afrique du Sud. Cette menace cible et exploite les peurs, les insécurités et les vulnérabilités des victimes. Elle recourt au hameçonnage, aux campagnes d'envoi massif de messages électroniques et à l'ingénierie sociale.

Selon les preuves recueillies par le South African Banking Risk Information Centre (SABRIC), *« les pertes brutes dues à la fraude, sur les cartes émises en Afrique du Sud, ont augmenté de 20,5 %, entre 2018 et 2019 ».*

La fraude au paiement à distance est à l'origine de ces pertes, tout comme les attaques de maliciels contre les banques, lesquelles placent le pays juste derrière la Russie. Toutefois, ce chiffre ne tient pas compte des tentatives d'hameçonnage liées à la COVID-19, ni des répercussions financières, émotionnelles et mentales pour les victimes. Les données volées, dans le cadre des escroqueries aux cartes de crédit, sont vendues aux enchères au plus offrant ou mises en vente sur des forums.



Détection des principales menaces en ligne en Afrique pour le seul mois de mai 2021

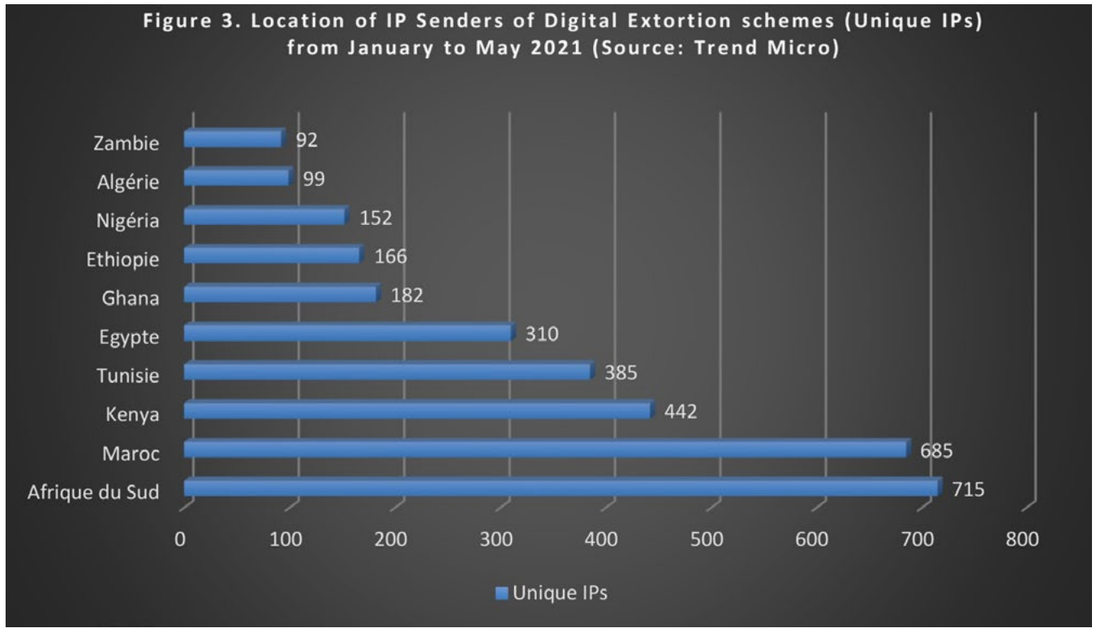
Hameçonnage et sextorsion

Pour son rapport 2019 sur l'Afrique, KnowBe4 a interrogé plus de 800 personnes en Afrique du Sud, au Kenya, au Nigéria, au Ghana, en Égypte, au Maroc, à Maurice et au Botswana. Et de son étude, il ressort que l'hameçonnage est l'une des principales cybermenaces subies par le continent. 28,14 % des personnes interrogées ont indiqué avoir déjà cliqué sur un courriel d'hameçonnage, 27,71 % ont déjà été victime d'une escroquerie et 19 % ont contribué à faire circuler un courriel non sollicité ou un canular.

Kaspersky, l'un des partenaires privés d'Interpol, a détecté près de deux millions de tentatives d'hameçonnage en Afrique du Sud, au Kenya, en Égypte, au Nigéria, au Rwanda et en Éthiopie, pour la seule année 2020.

L'extorsion en ligne, avec chantage et sextorsion, a été signalée comme l'une des cybermenaces les plus prééminentes en Afrique. Les acteurs des menaces emploient soit de fausses allégations, soit des preuves de données ou de fichiers à caractère personnel volés, pour forcer les victimes à payer une rançon, afin de

les récupérer ou d'éviter leur publication en ligne. Plus spécifiquement, les acteurs des menaces de sextorsion utilisent l'hameçonnage et le chantage sur de nombreuses plateformes pour obtenir de l'argent de leurs victimes, en alléguant avoir obtenu des images sexuelles compromettantes.



Localisation des IP des expéditeurs de courriels d'extorsion en ligne (IP uniques) entre janvier et mai 2021

La Namibie vulnérable face au réseau de machines zombies

Un botnet, ou réseau de machines zombies, est un réseau d'ordinateurs et de dispositifs piratés et infectés par un robot malveillant, contrôlé à distance par un pirate informatique. Ce réseau peut être utilisé pour envoyer des courriels non sollicités ou pour lancer des attaques par déni de service distribué (DDoS). Il peut être loué à d'autres cybermalfaiteurs. Les botnets peuvent aussi servir de point d'entrée pour les attaques par rançongiciel. Toute machine pouvant se connecter à Internet peut être compromise et transformée en machine zombie : ordinateurs, appareils mobiles, équipements de l'infrastructure Internet comme les routeurs réseau. Et, de plus en plus, les appareils IoT (Internet des objets), comme les appareils domestiques connectés.

A en croire Trend Micro, on détecte, en moyenne en Afrique, 3 900 victimes de botnets par mois, pour un total d'environ 50 000 détections. Différents acteurs africains de la menace déploient des campagnes de courriels non sollicités, en y joignant des chevaux de Troie voleurs comme Emotet, Lokibot, Agent Tesla, Fareit, etc. De manière assez surprenante, la Namibie a présenté le taux de détections le plus élevé pour Emotet, même s'il s'est résorbé après les efforts mondiaux menés plus tôt dans l'année pour désorganiser le botnet Emotet.

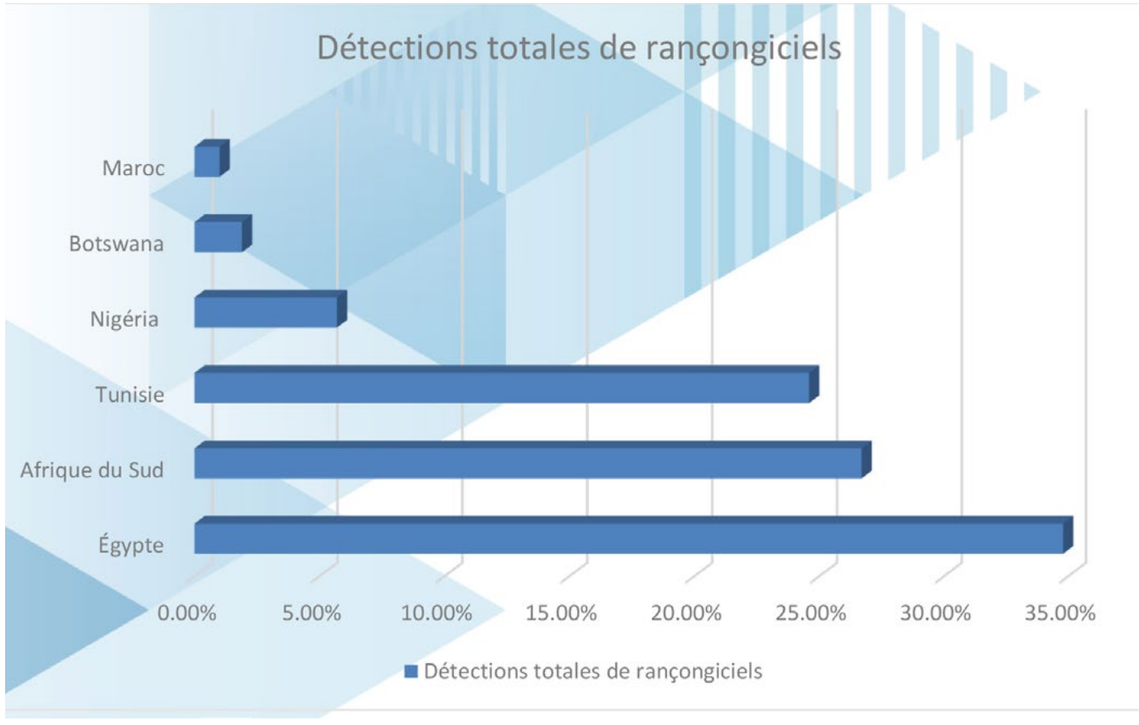
Rançongiciel : Egypte et Tunisie sont les premières victimes

Un rançongiciel est un logiciel malveillant. Il crypte les données de la victime ou verrouille ses systèmes, désorganisant les opérations des organisations victimes, en rendant leurs données et leurs systèmes inaccessibles.

Les opérateurs des rançongiciels demandent ensuite une rançon, habituellement en cybermonnaie, pour des raisons d'anonymat, en échange du décryptage des données.

Selon les études de Kaspersky, plus de 1,5 million de détections de rançongiciel ont été recensées en 2020. Au cours du premier trimestre 2021, l'Égypte, l'Afrique du Sud et la Tunisie ont été les pays les plus touchés de toute la région. Et l'Égypte a subi, à elle seule, près de 35 % des détections de rançongiciels en Afrique.

Au cours du premier trimestre 2021, l'Afrique du Sud a été le pays le plus fortement touché par les rançongiciels ciblés. Ils sont issus d'un large éventail de familles comme les rançongiciels Crysis, Nefilim, Ryuk, Clop et Conti. L'Égypte a été le deuxième pays le plus touché, avec un profil similaire dans les détections de rançongiciels ciblés. La Tunisie se place en troisième position et a été principalement ciblée par les rançongiciels Egregor (avant son démantèlement en février 2021), Ryuk et Sekhmet.



Détections de rançongiciels en Afrique en mars 2021

Notons que le rapport *« Evaluation 2021 des cybermenaces en Afrique »* d'Interpol s'appuie sur les données de ses pays membres en Afrique.
Sur les 55 pays membres que compte la région, 22 ont répondu à l'enquête et ont fait part de leurs perspectives nationales sur les cybermenaces. Interpol a également obtenu des données pertinentes de ses partenaires privés, notamment Group-IB, Kaspersky, Palo Alto Networks et Trend Micro.

FOCUS

« En matière de cybersécurité, il est primordial de travailler sur des stratégies d'alliances »

La cybercriminalité atteint des records. On estime désormais à 6000 milliards de dollars par an le coût des cyberattaques pour l'économie mondiale. Une tendance qui devrait se poursuivre et même s'aggraver, dans les prochaines années et qui touche tous les secteurs d'activités. Les cyberattaques menacent aussi bien les particuliers que les institutions publiques et les entreprises privées. Emmanuel Cheriet, Directeur Maghreb et Afrique de l'Ouest Orange Cyberdefense, dresse, pour Cio Mag, un panorama des nouvelles tendances en matière de cyber-risques et les moyens d'y faire face.

Emmanuel Cheriet
Directeur Maghreb et Afrique
de l'Ouest Orange Cyberdefense

Cio Mag : L'année 2021 a connu une progression de la menace cyber, tant en qualité qu'en volume d'attaques. Allons-nous observer de nouvelles « tendances » de cybercrimes en 2022 ?

Emmanuel Cheriet : Sur les aspects qualitatifs, nous observons une amélioration et une professionnalisation des hackers. Désormais, ils ciblent de manière plus précise pour avoir un effet maximum et combinent des effets en conjuguant différents types d'attaques.

Ils restent peu atteignables, malgré les efforts des autorités publiques. Tous ces éléments sont des preuves de l'élévation de la maturité de la filière « hack to cash ». En termes de tendances, nous observons une recrudescence des attaques via Malwares (logiciels malveillants) et notamment de type Ransomware. Pour preuve, en 2020, les incidents de type Anomalies réseaux et applications étaient en pole position. Or, en 2021, les incidents liés au réseau ont chuté et proportionnellement, les Malwares ont presque doublé. Nous estimons que cette tendance risque de se confirmer en 2022.

Cio Mag : En termes de vulnérabilité et de cyberattaques, quelles sont les spécificités africaines ?

E.C : De manière générale, l'Afrique subit les mêmes typologies d'attaques que les autres continents. Il y a cependant un déficit de déclaration d'incidents, lequel tend à minimiser les statistiques. Par ailleurs, sur le continent, les attaques sur les environnements de Mobile Money sont plus répandues.

Ces services étant beaucoup plus développés qu'ailleurs, cela génère automatiquement plus de fraudes. Nous observons aussi une moins bonne couverture du risque cyber et suivi/traitement des vulnérabilités par les entreprises africaines, comparativement à des entreprises européennes.

Cio Mag : La situation géopolitique en Afrique de l'Ouest, avec les coups d'États dans plusieurs pays, engendre-t-elle des risques cybersécuritaires accrus ?

E.C : Les instabilités politiques ou les conflits peuvent engendrer une recrudescence des attaques. Le cyberespace est un instrument extrêmement puissant dans les rivalités de pouvoir entre groupes et minorités, entre forces politiques, religieuses et économiques, au niveau local ou mondial.

Il peut être utilisé par des cybercriminels pour s'enrichir ou par des groupes et des États agissant dans le cadre de conflits politiques, de combats militaires, de guerre économique, de renseignement ou de politique d'influence diplomatique et culturelle.

Nous avons aussi observé, ces dernières années, des campagnes de déstabilisation liées à de la désinformation, notamment via les réseaux sociaux. Aujourd'hui, la déstabilisation d'un pays n'est plus uniquement militaire, mais aussi cyber. Le cyberespace devient à la fois un théâtre d'affrontements et aussi une arme importante dans les conflits géopolitiques.

Cio Mag : L'avènement de la téléphonie mobile (et bientôt de la 5G ?) nécessite-elle de mettre en place de nouvelles formes de protection ? Lesquelles ?

E.C : La protection des mobiles est très largement sous-estimée par les utilisateurs et les entreprises, alors que nos smartphones hébergent la plupart de nos données (emails, messages, contacts, documents, etc.) Aujourd'hui, le mobile redéfinit les frontières au profit des attaquants. Il y a de plus en plus d'appareils, donc plus de façon d'entrer. Et plus de fonctionnalités, donc plus de surface d'attaque. Plus de données pro/perso, donc plus d'intérêt des pirates. Et enfin, ces appareils sont plus proches de l'utilisateur, ce qui induit une fausse sensation de sécurité. Donc, oui, il est nécessaire de mettre en place de nouvelles formes de protection.

Des logiciels d'éditeurs de sécurité peuvent être installés sur les mobiles. Ils permettent de détecter les différentes menaces (applications, réseaux, vulnérabilités des OS, phishing), de gérer la politique de sécurité mobile et de visualiser des attaques ou des vulnérabilités en cours. Orange Cyberdefense propose ce type de services, notamment via notre offre « Mobile Threat Protection ».

Concernant la 5G, elle apporte plus de connectivité et donc un accès à plus de fonctionnalités pour les utilisateurs, ce qui va augmenter l'intérêt et la surface d'attaque des pirates.

Cependant, la 5G n'apporte pas de faiblesse directe. C'est l'augmentation des usages générés qui fait croitre les attaques et donc la nécessité de protéger les Mobiles.

Cio Mag : Comment les États africains peuvent-il rester maîtres de leur souveraineté numérique, sachant qu'ils utilisent des outils cyber provenant de partenaires privés extérieurs ?

E.C : Tous les États ont sur la table le sujet de la souveraineté des données. Mais, pour être totalement souverain, il faut être capable de fournir l'ensemble des services, pays par pays. Or, un grand nombre de pays n'a pas la taille critique (en termes de potentiel business) ou la maturité et les compétences pour couvrir l'ensemble de ces services.

L'approche et la réflexion peuvent être régionales pour gagner en taille et en capacité. A l'instar de l'Europe, qui pousse les entreprises à privilégier des services européens, estimant être dans une zone de confiance, de partenariat et d'alliance (souveraineté européenne).

Aujourd'hui, la plupart des services cloud sont proposés par des sociétés privées et notamment américaines. Il va être difficile pour les autres nations de rattraper le retard et de se passer de ces services. L'alternative sera peut-être de réfléchir à localiser ces services cloud sur le continent, en mutualisant les besoins de plusieurs pays. Ou en créant des zones de confiances (pour atteindre une taille critique) et en mettant en place des partenariats avec ces acteurs pour les obliger à localiser les données en Afrique et ainsi garantir

INTERVIEW

Emmanuel Cheriet
Directeur Maghreb et Afrique de l'Ouest Orange Cyberdefense

une confidentialité de ces dernières.
En matière de cybersécurité, il est primordial de travailler sur des stratégies d'alliances pour être plus forts face aux risques, en intégrant l'ensemble des acteurs (Etats, acteurs spécialisées, législateurs, providers, etc.).

Cio Mag : Quelles solutions proposez-vous pour aider les institutions publiques et les entreprises privées à protéger leurs données ?

E.C : Orange Cyberdefense propose une gamme complète de services et de solutions qui couvrent l'ensemble des problématiques de cybersécurité. Il est tout d'abord primordial de connaitre ses actifs et leurs vulnérabilités en réalisant des audits réguliers (tests d'intrusions réalisés par nos hackers éthiques). Ensuite, il est nécessaire de mettre en place des systèmes de protection et de contrôle. Et, bien entendu, nous proposons aussi des services permettant d'améliorer la détection et la réaction face aux incidents de sécurité (via nos CyberSOC, Microscoc, Exercices de crise Cyber, etc.).

Concernant le service MicroSOC, il permet de protéger efficacement les postes de travail et les serveurs en identifiant les menaces le plus rapidement possible et en les bloquant. Il y remédie via des plans d'actions et des investigations poussées. Nous proposons un service complet alliant solutions technologiques de premier ordre (EDR, XDR), expertise des analystes d'Orange Cyberdefense, couplée à notre connaissance de la menace via nos bases de Threat Intelligence. Avec l'ensemble de ces services, les entreprises augmentent drastiquement et rapidement leur niveau de détection et de protection en couvrant les risques les plus importants (notamment les Malwares/Ransomwares).

Cio Mag : Aujourd'hui, Orange Cyberdefense est la branche d'Orange qui permet au groupe de s'assurer une croissance. Quelles sont les perspectives d'évolution ?

E.C : Il est vrai qu'Orange Cyberdefense connait un succès continu depuis son lancement. Il enregistre 800 millions de chiffre d'affaires en 2021. Nous sommes confiants sur notre capacité à confirmer notre croissance dans les années à venir. Pour accompagner ce développement, nous travaillons sur deux axes : la croissance organique en accélérant l'embauche des experts (nous ciblons par exemple 600 recrutements cette année) et en conquérant de nouveaux clients et marchés. Nous étudions également toutes les opportunités de croissance externes pour renforcer nos positions ou ouvrir de nouveaux marchés. Notre ambition est d'être un leader européen, avec une forte empreinte internationale, afin de suivre nos clients dans le monde entier.

Propos recueillis par Camille Dubruelh

Emmanuel Cheriet évolue depuis plus de 16 ans dans le secteur IT et la Cybersécurité. Depuis 2016, il a d'abord été Directeur commercial Grands comptes France chez Orange Cyberdefense et est à présent Directeur Maghreb et Afrique de l'Ouest Orange Cyberdefense, en charge de la construction et du développement des activités en Afrique.

Emmanuel Cheriet a lancé cette activité au Maroc, en 2018, avec l'ambition de positionner Orange Cyberdefense comme un leader de la cybersécurité sur le continent.

PANORAMA

Quelles sont les principales atteintes aux données personnelles ?

Un certain nombre d'attaques défient la sureté des données en ligne. Les experts attestent, à l'unanimité, qu'elles sont toujours d'actualité et même en développement. Et les gangsters du net profitent de la fragilité de leurs proies.

Aurore Bonny

« Il existe trois attaques principales, qui sont indirectes et peuvent être considérées comme des vulnérabilités pouvant conduire à la fuite de données personnelles », note Didier Simba, expert en cybersécurité et président et fondateur du Club d'experts de la sécurité de l'information en Afrique (CESIA). En tête de liste, l'arnaque en ligne incluant l'hameçonnage ou le phising. Il s'agit d'un système d'escroquerie - en ligne ou via un mail - très répandu, qui annonce un gain matériel, une perte ou toute autre chose. Et qui inclue un lien ou un document à ouvrir, lequel sert d'appât de données personnels lorsque la victime y accède. *« Cette attaque est prolixe sur les réseaux sociaux. Les gens sont intéressés par des messages et des propositions de jeux ou par des cadeaux et des crédits de communication à gagner, mais ils ne se rendent pas compte de l'action qui suit en arrière-plan »*.

Selon l'Organisation internationale de police criminelle (Interpol), l'escroquerie en ligne est la cyber invasion la plus signalée dans la région africaine et la plus urgente. Elle exploite les craintes, les insécurités et les vulnérabilités des victimes par le biais du phishing, du publipostage et de l'ingénierie sociale. Pour Kaspersky, ces menaces *« sont particulièrement proéminentes et pressantes »*. Avec le phishing, les fraudeurs visent l'accès aux renseignements personnels dans le but de perpétrer une usurpation d'identité ou pour collecter les données personnelles qui ont une grande de valeur pour les cybercriminels. La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance - banque, administration, etc. - afin de lui soutirer des renseignements personnels.

Dans la série des cyber extorsion s'ajoutent les Ransomware ou logiciels de rançon. Ils prennent en otage les informations des victimes et demandent en échange une somme d'argent. Ils leur laissent le choix entre payer la rançon, supprimer l'application malveillante ou redémarrer l'appareil selon les mesures sécuritaires rapportées par les experts. Ce type de logiciel *« a fait des*

ravages en Afrique durant ces dernières années », admet Didier Simba.

Dans son rapport sur les cybercrimes en Afrique, publié en octobre 2021, Interpol rapporte que plus d'1,5 million de détections de rançongiciel ont été recensées en 2020. Au cours du premier trimestre 2021, l'Égypte, l'Afrique du Sud et la Tunisie ont été les pays les plus touchés de toute la région. Et le pays des Pharaons a subi, à lui seul, près de 35 % des détections de ransomware sur le continent.

En début d'année 2022, Kaspersky a observé *« une attaque massive de ransomware sur l'Afrique de l'Ouest »*. Selon les responsables du groupe - notamment Herve Iro Mondouho, Territory channel manager sur l'Afrique de l'ouest et du centre, ainsi que son collaborateur Pascal Naudin, Head of B2B sales dans la région africaine -, les menaces qui ciblent en particulier le secteur public sont à craindre car une bonne part est dans un processus de digitalisation des services administratifs.

« Le secteur industriel est aussi particulièrement exposé, car l'impact financier qu'implique l'arrêt d'une chaine de production est très important et les cybercriminels le savent. Enfin, les banques et les télécommunications sont aussi particulièrement ciblées dans la région et les attaques sont en permanente augmentation », ont indiqué les deux experts à Cio Mag. Interpol range également cette cyber extorsion parmi les cybers outrages les plus en vogue sur le continent.

Défaut d'applications

Pour Interpol, l'évolution vers une société numérique, même si elle n'est pas nouvelle, a néanmoins créé de nouveaux vecteurs d'attaques, qui permettent aux criminels de dissimuler leur identité et de cibler de nouvelles victimes. *« La menace des ransomwares se développe sur le continent africain. Selon les allégations, plus de 61 % des entreprises de cette région ont été touchées par des ransomwares, au cours de la seule année 2020. Ces attaques ont visé les infrastructures critiques de certains pays africains, notamment les secteurs de la santé et de la mer ».*

Les infrastructures et la construction des applications ont constitué des failles, qui ont exposé les données personnelles des internautes, comme a pu l'observer Didier Simba, lors de la crise sanitaire mondiale liée au Coronavirus.

« Avec la crise sanitaire, nombreux sont ceux qui se sont précipités sur la construction de solution numériques comme les applications et les sites internet, sans réellement se préoccuper de l'aspect sécuritaire. Ces vulnérabilités sont appelées injections du langage de requête structuré (SQL). La technique d'injection de code est utilisée pour modifier ou récupérer des données dans des bases de données. Les attaquants l'utilise pour introduire des programmes malveillants ou d'autres virus, qui accèdent aux bases de données attaquées ». L'expert remarque que ces attaques sont plus répandues en Afrique et qu'elles ont la particularité de s'intéresser aux bases de données.

Ettiene Van Der Watt, directeur régional pour le Moyen-Orient et l'Afrique de la société de vidéosurveillance Axis Communications – cité par le site sud-africian TechMetro – prédit pour sa part qu'il sera très difficile de prévenir les escroqueries numériques en 2022. En cause, le développement du deepfake, un procédé qui permet aux cyberbandits d'altérer des images et des vidéos. De son point de vue, il s'agit d'un défi auquel de multiples secteurs doivent faire face en travaillant pour lutter contre.

Outre les escroqueries en ligne, la compromission des e-mails professionnels (BEC) a été identifiée par Interpol comme une préoccupation et une menace importante pour la région. *« Les entreprises et les organisations qui dépendent fortement des transactions par virement sont vulnérables à cette menace en Afrique. La pandémie de COVID-19 a contribué à l'augmentation de ce type de cybercriminalité »*, précise l'organisation.

Interpol cite aussi les attaques par Botnets. Ces réseaux de machines compromises sont utilisés comme outil pour automatiser des campagnes à grande échelle, telles que les attaques DDoS, le phishing, la distribution de logiciels malveillants et autres. *« Le nombre de détections de victimes de botnets, en Afrique, était d'environ 50 000, avec une moyenne mensuelle de 3 900 détections »*, en 2021. Et *« de nombreux cas d'attaques DDoS contre des infrastructures critiques ont été très médiatisés, au cours des cinq dernières années ».*

Interpol estime qu'il est crucial de mettre en place un cadre de cybersécurité solide, à l'heure où la faiblesse des réseaux et de la sécurité rend les pays africains particulièrement vulnérables. Des pays qui manquent de politiques et de normes de cybersécurité, exposant ainsi les services en ligne à des risques majeurs.

CYBERMENACE

« Lorsque vos données personnelles sont volées, tout peut arriver... »

L'accroissement des usages numériques génère autant de données à protéger. La diversité des profils fait varier l'échelle des menaces dont il faut se prémunir. Mais, quels sont les risques en cas de récupération des données ? Et comment en faire une bonne gestion ? .

Michaël Tchokpodo

En 2019, seuls 28 % d'Africains utilisaient Internet et les acheteurs en ligne étaient encore relativement peu nombreux. Ils devraient atteindre 39,5 %, selon les estimations de Statitica et de l'Union internationale des télécommunications (UIT). Mais, la crise de Covid-19 a rapidement augmenté l'attrait des internautes pour les solutions numériques, en même temps que le volume des données échangées.

En 2020, que ce soit via Zoom et WhatsApp ou via Facebook, Instagram ou TikTok, les données échangées par minute ont été impressionnantes. Selon le média tech clubic.com, sur Facebook, quelques 147 000 photos ont été publiées et 150 000 messages partagés. Plus de 208 000 personnes ont participé aux réunions Zoom et près de 42 millions de messages ont été échangés sur WhatsApp. Et chaque minute, plus de 2 700 téléchargements ont été effectués sur TikTok. Ces chiffres sont en nette progression.

Les internautes échangent des informations, du son et des images d'une personne physique identifiée ou identifiable. *« Si, par le passé, la catégorie des données personnelles était considérée comme étroite et définie, la réglementation moderne en matière de protection de la vie privée élargit le champ. Sont inclus les données des ménages, les données pseudonymisées, les adresses IP, les identifiants des appareils, etc. »*, précise Enza Iannopollo, analyste principal chez Forrester, un cabinet d'études et de conseils qui accompagne les responsables métiers et les leaders technologiques.

Vulnérabilité des données

A l'instar du pétrole dans l'industrie contemporaine et de l'or parmi les métaux, les données sont des ressources vitales pour le monde numérique. Et plus le monde des TIC devient transversal, plus la valeur de la donnée supplante toutes les autres parce qu'elle regroupe l'ensemble des informations dont la divulgation peut nuire à l'existence de la victime. Les données sont-elles de facto exposées ou accessibles ? *« Lorsqu'on est connecté, certaines données telles que les adresses IP, les données de navigation, l'historique de connexion, les données de localisation... sont accessibles et collectées par les équipementiers, les Fournisseurs d'accès internet (FAI), les GAFAM et autres »*, répond Yvon Détchénou, président de l'Autorité de protection des données personnelles (APDP) au Bénin.

Pour Roland Aïkpé, ingénieur en cybersécurité à l'Agence nationale de la sécurité des systèmes d'information (ANSSI) au Bénin, les informations généralement accessibles au public sont les noms et prénoms, les photos et les vidéos publiées, etc. Par contre, nuance-t-il, les données renseignées lors de la création d'un compte, sur une banque en ligne, par exemple, ne sont pas accessibles au public. Dans ce cas, il revient à l'entreprise de prendre les dispositions nécessaires pour les protéger. *« Les bannières de cookies et les avis de consentement, par exemple, donnent aux utilisateurs le choix de partager ou non leurs données »*, précise Enza Iannopollo. Mieux, *« ils aident les utilisateurs à comprendre quelles données un site web tente de collecter et pourquoi. Nos données suggèrent également que les individus du monde entier utilisent de plus en plus des technologies, telles que «do not track me» ou des extensions de navigateur similaires. Ceci pour empêcher les sites web et les applications de collecter leurs données personnelles. »*

Risques de vol de données

Internet étant à l'image d'un open space, les risques de vol ou de récupération des données personnelles sont permanents. Et toutes les données sont utiles. Elles servent parfois à cerner la personnalité d'un internaute,

ses goûts, ses choix ou ses besoins. Créer un compte sur les réseaux sociaux nécessite des données personnelles. Et chaque internaute a un compte sur plusieurs réseaux à la fois, sans compter les adresses emails. Ceux-ci s'exposent déjà, en plus des faits de piratage qui surviennent chaque année chez les géants tels que Facebook, Google, Yahoo, et qui les rendent plus vulnérables. *« Lorsque vos données personnelles sont volées, tout peut arriver »,* prévient l'analyste principal de Forrester.

Chez les internautes, le vol de données peut mener à l'usurpation d'identité, le chantage, le spamming, l'hameçonnage, l'anxiété et le risque réputationnel. *« Ce qu'il faut craindre, c'est la capacité des systèmes à identifier des déterminants de la personne qui peuvent se retourner contre elle »*, avertit Yvon Détchénou. Enza Iannopollo renchérit : *« L'utilisation abusive des données ne produit toutefois pas toujours du vol. Lorsqu'une entreprise utilise vos données personnelles d'une manière inattendue ou sans que vous ne le sachiez, il s'agit d'une mauvaise utilisation de vos informations. Et, malheureusement, ces données peuvent être utilisées pour nous manipuler de manière subtile, sans même que nous nous en rendions compte. »*

Pour les entreprises, la fuite des données peut engendrer des risques économiques, une atteinte à la notoriété, une baisse du chiffre d'affaires ou une perte financière. Dans le cas des gouvernements, il est souvent question de cyber espionnage. L'autre façon subtile de collecter les données personnelles passe par l'acceptation, à l'aveuglette, des conditions d'utilisation lors de la création d'une adresse email ou des cookies pour accéder à un site web. Diverses sortes de cookies [de cession, techniques, publicitaires ou de navigation] permettent au propriétaire de site web de connaître les habitudes des internautes en termes de publicité et de diffusion d'informations.

Quid de la réglementation ?

Selon la Conférence des Nations-Unies pour le commerce et le développement (CNUCED), 128 des 194 pays du monde ont mis en place une législation pour assurer la protection des données et de la vie privée.

En Afrique, seulement 33 pays sur 54 ont adopté une loi sur la protection des données des consommateurs. Et seuls 18 pays du continent ont une autorité de contrôle. Si beaucoup considèrent le Règlement général européen sur la protection des données (RGPD) comme une norme mondiale en matière de protection de la vie privée, de nombreux autres pays ont élaboré leur propre réglementation en matière de protection de la vie privée.

A l'instar de l'Afrique du Sud, avec la loi sur la protection des informations personnelles (POPIA). Et du Bénin, avec la loi n°2017 du 20 avril 2018, portant code du numérique, qui met en place les dispositions nécessaires pour protéger la vie numérique de la population.

En outre, *« il faut une certaine participation de l'internaute dans la protection de ses données personnelles. Quand on possède des données sensibles, il faut mettre des couches supplémentaires de sécurité, comme un mot de passe. Il faut tout le temps verrouiller son téléphone pour qu'en cas de perte, personne ne puisse accéder à ses informations »*, conseille Roland Aïkpé.

Hormis la réglementation, la souveraineté des données permet une meilleure protection de leur gestion. Comme le rappelle Enza Iannopollo, *« toute organisation qui utilise des services en nuage doit s'assurer qu'elle sait où ses données sont effectivement stockées et/ou traitées. En fonction des flux de données et des pays qu'ils traversent, les entreprises doivent tenir compte des exigences spécifiques en matière de confidentialité et de gouvernement concernant l'accès aux données, leur protection, etc. »*

La plupart des organisations ou des Etats africains hébergent leurs données à l'étranger. La tendance change, ces dernières années, avec la construction de datacenters nationaux, avec le choix des équipements, les stratégies de gestion des équipements et des données, et la soumission aux lois du pays. *« Cela protège la propriété intellectuelle et renforce la confiance numérique »*, renchérit l'ingénieur de l'ANSSI. Néanmoins, l'illusion que cela procure d'être derrière son smartphone ou son ordinateur, ou la méconnaissance des règles de protection et de sécurité des données, continuent de faire de certains internautes, des proies faciles.

DOSSIER PROTECTION DES DONNÉES

INTERNATIONAL

Le Luxembourg s'engage pour la cybersécurité en Afrique

L'année 2022 marque l'arrivée du régulateur luxembourgeois à la tête du réseau francophone de la régulation des télécommunications FRATEL. Cet évènement invite Cio Mag à se pencher sur les actions en matière de cybersécurité de ce petit pays européen. Outre son engagement au sein de FRATEL, le Luxembourg multiplie les projets de coopération avec le continent africain pour relever les défis en matière de cybersécurité. Notre magazine donne la parole à Luc Tapella, directeur de l'Institut luxembourgeois de régulation.

Cio Mag : Fratel a choisi de discuter des thèmes de la résilience et de la sécurité des réseaux dans son plan d'action 2022. Quelles sont les raisons qui ont guidé ce choix ?

Luc Tapella : Fratel est un réseau qui réunit une cinquantaine de pays membres francophone. Fratel aborde cette année les thèmes de la résilience et de la sécurité des réseaux. La résilience s'est imposée comme un sujet d'intérêt commun, dans le contexte de la pandémie de Covid-19. La crise sanitaire a entrainé une forte hausse de la demande de connectivité du fait des changements majeurs dans l'utilisation des services, en particulier le télétravail et l'enseignement à distance. Le sujet de la cybersécurité s'est imposé dans un contexte de digitalisation croissante et d'explosion de la quantité de données. Il parait important pour Fratel d'échanger sur les bonnes pratiques à adopter et sur les différentes manières d'appréhender et de concevoir des méthodes de sécurité des réseaux. Pour discuter de ces thèmes, un séminaire, consacré aux défis pour la sécurité des réseaux de nouvelle

génération, aura lieu les 23 et 24 mai. Il sera accueilli par l'autorité de régulation de la poste et des télécommunications du Congo.

Les grands enjeux liés à la cybersécurité seront évoqués, ainsi que les diverses obligations des opérateurs en la matière et les mesures pour réduire les risques. L'objectif de ces échanges est également d'aborder les enjeux de sécurité liés à l'évolution technique et les architectures réseaux. En effet, de nouvelles problématiques apparaissent avec les nouvelles technologies comme la 5G, la virtualisation des réseaux et l'émergence de nouveaux acteurs.

Le séminaire constituera également une occasion, pour les autorités membres de Fratel, de mieux appréhender ces innovations sous l'angle de la sécurité. En outre, les aspects liés aux nouvelles menaces contre les réseaux pourront être discutés. Il sera question d'échanger sur les différentes formes de réduction des risques liés aux menaces telles que les attaques malveillantes ou sur la dépendance vis-à-vis des fournisseurs. Le séminaire sera également l'occasion de présenter différentes approches liées à la sécurité des réseaux en matière de contrôle et de prévention.

Cio Mag : Depuis 2021, le Luxembourg s'est engagé à mobiliser davantage les partenariats et les initiatives innovantes du domaine des TIC, dans le cadre de sa politique de coopération en Afrique. La cybersécurité est un des axes d'action en la matière. Pourriez-vous présenter quelques initiatives pour les lecteurs de Cio Mag ?

L. T : La stratégie du Luxembourg en matière de cybersécurité prévoit un engagement proactif en termes de coopération au niveau mondial. Dans le domaine spécifique de la coopération au développement, les initiatives du gouvernement luxembourgeois s'alignent sur les objectifs de la Commission européenne. Et consistent à faire du Digital4Developpement (D4D) une priorité des partenariats internationaux. Un des axes d'action concerne la cybersécurité, notamment en Afrique subsaharienne, une zone dans laquelle le Luxembourg est engagé depuis de nombreuses années. Ensemble, avec ses pays partenaires (que sont le Sénégal, le Niger, le Burkina Faso, le Mali et le Cap Vert), mais aussi avec d'autres pays comme le Rwanda ou le Bénin, nous visons à encourager l'intégration et la capitalisation des outils numériques par les acteurs de l'aide au développement et de l'action humanitaire. Et également le transfert de connaissances. Les synergies entre deux domaines d'expertises spécifiques du Luxembourg – à savoir le traitement et la sauvegarde de données sécurisées et celui de la finance inclusive et innovante - sont activement recherchées et promues pour renforcer les capacités locales.

Par exemple, le Luxembourg s'est engagé, en 2020, dans un partenariat entre des universités du Burkina Faso et du Sénégal avec le Centre interdisciplinaire de sécurité, fiabilité et confiance (*Interdisciplinary Centre for Security, Reliability and Trust*, SnT) de l'université du Luxembourg.

Cet ambitieux projet de formation, intitulé Luxways, propose des formations en cybersécurité au sein du SnT. La collaboration se matérialise à travers des supervisions conjointes de thèses entre les universités partenaires, ainsi que par la formation de stagiaires/ingénieurs, dans le cadre de courts séjours de recherche au Luxembourg. Le programme comporte également des écoles d'été, ainsi que des formations et des publications conjointes. Le projet vise à renforcer le capital humain en matière de cybersécurité des pays d'Afrique de l'ouest. Une étude est actuellement en cours pour étudier la possibilité d'une implantation du SnT en Afrique de l'ouest.

L'accompagnement de la transformation numérique en Afrique est également un pilier de l'action du *D4D Hub Africa* entre l'Union africaine et l'Union européenne (UA-UE), laquelle est opérationnelle depuis 2021. C'est une plateforme multi-acteurs, qui aspire à mettre en place des partenariats stratégiques et

Luc Tapella
Directeur de l'Institut luxembourgeois de régulation

INTERVIEW

à stimuler les investissements conjoints entre l'Europe et les pays partenaires africains. Dans ce cadre, le Luxembourg préside le groupe de travail en charge de la cybersécurité.

Le Luxembourg promeut également des partenariats public/privé dans le cadre de la coopération, notamment dans le secteur des TIC et de la cybersécurité. Ainsi, un groupement d'intérêt économique GIE Cyber4Dev a été créé en septembre 2020. Il est composé de « Security Made in Lëtzebuerg g.i.e » et « Excellium Services S.A », deux des principaux acteurs de la cybersécurité au Luxembourg. Le GIE s'associe de manière flexible avec d'autres acteurs clés, sur des projets spécifiques dans le domaine de la cybersécurité.

À titre d'exemple, Cyber4Dev met en œuvre le projet *Africa Cybersecurity Ressource Centers (ACRC) for Financial inclusion*, avec le C3, SnT et Suricate Solutions. Et grâce à un financement de la Banque africaine de développement (BAD). Le projet ACRC vise à assurer le développement rapide des systèmes financiers numériques et à ainsi accroître l'inclusion financière sur le continent. Il cherche à renforcer la cyber-résilience du système financier à travers la création de centres de ressources et de réponse aux cyberattaques en Afrique subsaharienne, afin de sécuriser le secteur de la finance inclusive.

Cio Mag : Quelle est la spécificité du Luxembourg en matière de cybersécurité ?

Luc Tapella : L'ILR est l'autorité nationale compétente. C'est le point de contact unique qui veille à ce que les opérateurs des services essentiels gèrent la sécurité de leurs réseaux et de leurs systèmes d'information. Actuellement, l'ILR travaille à faire évoluer une plateforme d'analyse et de gestion des risques SERIMA, en collaboration avec le *Luxembourg institute of science and technology*. Cette plateforme a pour objectif de permettre aux opérateurs de procéder à des analyses de risques. Ils disposent également d'une méthodologie commune pour effectuer des analyses de risque et pour déclarer des incidents en fonction des régulations en vigueur. Cet outil peut être utile à toute autorité nationale dans le domaine de la cybersécurité. C'est cette expérience luxembourgeoise de gestion des risques que nous souhaitons partager lors du prochain séminaire de Fratel.

Propos recueillis par Mohamadou Diallo

FORMATION

Le numérique pour l'éducation et la formation professionnelle

Le numérique permet de gagner en efficacité dans l'enseignement supérieur. Premièrement,la digitalisation de cet enseignement permet un meilleur pilotage des politiques publiques du secteur et une réponse agile aux attentes du marché du travail local, grâce à la récolte de données de qualité : suivi d'indicateurs de performance ; « Tracer studies » (études sur l'insertion des alumni dans le marché du travail) ; gestion de l'enregistrement des élèves, professeurs, diplômes ; diffusion d'informations ; identification des besoins…. Des suivis automatisés de l'insertion des diplômés et de leurs parcours professionnels auraient également l'avantage de fournir aux élèves des exemples très concrets des débouchés et niveaux de rémunération de chaque formation, voire de rencontrer aisément les employeurs, ce qui faciliterait et accélèrerait considérablement leur orientation.

Deuxièmement, il est possible d'étendre l'enseignement et la formation, tout en améliorant leur qualité, grâce au digital. En particulier, dans le contexte de pénurie d'enseignants, le digital pourrait permettre de fournir rapidement une éducation de masse, aux standards de qualité vérifiables. Introduire le numérique dans la formation professionnelle et l'enseignement supérieur serait un puissant levier d'inclusion sociale et de genre. Sur le continent africain, dont le marché du travail est largement informel et où les femmes ont la plus forte proportion d'entrepreneures au monde, utiliser le digital pour former à l'entrepreneuriat à moindre coût est d'ailleurs particulièrement pertinent. Démocratiser l'accès aux équipements et infrastructures de base est un préalable indispensable à la digitalisation de la formation professionnelle Les potentialités du numérique ne pourront être pleinement exploitées qu'à condition d'accompagner ces moyens matériels d'une pédagogie appropriée, grâce à laquelle les enseignants comme les élèves puissent tirer le meilleur parti des ressources digitales dont ils disposent. Quant aux outils eux-mêmes, les plateformes d'apprentissage en ligne ou e-learning, la gamification, l'apprentissage sur mobile ou encore les ressources éducatives libres sont autant d'instruments susceptibles de servir la formation par le digital et ils sont nombreux.

Comment les acteurs publics et privés peuvent-ils améliorer la compétitivité et l'attractivité de la formation professionnelle et supérieure ?

En premier lieu, se doter d'une stratégie nationale ambitieuse en matière et concevoir puis mettre en œuvre des politiques publiques dédiées incombe aux pouvoirs publics :

- Mobiliser des financements
- Définir et appliquer les normes de qualité des certifications et des établissements
- Faciliter la coordination interministérielle et entre administrations
- Développer des institutions spécialisées dans la formation supérieure aux « métiers du digital ».
- Assurer un suivi étroit de l'efficience des projets réalisés et une mesure d'impact précise

Les directions des établissements peuvent aussi contribuer grandement à la revitalisation du secteur, grâce au partage de ressources en ligne, à la diffusion des meilleures pratiques pédagogiques, à la signature de conventions d'échanges et de partenariats à l'intérieur du pays et à l'étranger, à la création de communautés d'alumni soudées et suivies régulièrement… Quant au secteur privé, sa mobilisation est une condition sine qua non du succès de toute stratégie nationale de formation professionnelle, à la fois pour aider les acteurs publics à cibler les besoins du marché de l'emploi, pour contribuer à définir les différents niveaux de maîtrise des compétences attendues de la part les étudiants, et pour former lui-même des salariés, via des programmes conçus au sein de l'entreprise ou en finançant pour ses employés le passage de certifications reconnues.

Jean-Michel Huet, associé BearingPoint

Un engagement pour l'égalité numérique en Afrique

Orange Digital Center

Un espace gratuit d'accompagnement des jeunes consacré à l'innovation :

- formations pratiques sur les technologies innovantes
- ateliers de prototypage numérique
- incubation technologique
- accélération de start-up à l'international

Les Orange Digital Centers sont présents en Tunisie, au Sénégal, au Cameroun, en Ethiopie, au Mali, en Côte d'Ivoire, en Jordanie, au Maroc, en Egypte, en Sierra Leone, au Burkina Faso, à Madagascar, en Guinée Conakry, au Libéria et prochainement en République Démocratique du Congo, au Botswana, en République Centrafricaine et en Guinée Bissau.

orange™

Vous rapprocher de l'essentiel