LA RÉFÉRENCE DU NUMÉRIQUE EN AFRIQUE
cio mag .com
N69 I AVRIL - MAI - JUIN 2021

Cybersécurité et télétravail, les risques augmentés ?

ÉTUDE CYBERSÉCURITÉ : 50 Twittos à suivre en Afrique

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

OLYMPIC®

BANKING SYSTEM

GREAT TEAMS FOR GREAT CHALLENGES!

olympicbankingsystem.com

eRI®

Édito

Mohamadou DIALLO
Fondateur et Directeur Général de CIO Mag

IA, Télétravail et Cybersécurité : des antidotes à la pandémie

En provoquant volontairement un débat d'experts, en amont de la parution de ce numéro consacré au triptyque *« IA, Télétravail et Cybersécurité »,* CIO Mag en a souligné l'importance. Et nous avons, dans le même temps, suscité l'intérêt de plusieurs centaines de lecteurs de notre magazine, si bien qu'ils ont participé à ce webinaire de haut niveau. Il est indéniable que ces trois tendances ont véritablement marqué l'année 2020. Et 2021 n'échappera pas à la montée en puissance de cette tri-force.

La bascule contrainte et précipitée vers le télétravail, du fait de la pandémie de Covid-19, nous permet d'entrevoir le côté positif du digital. Il va finir par faire gagner cinq bonnes années, en termes d'accélération, dans l'adoption des outils numériques. Mais, la question est de savoir s'il s'agit d'une redistribution des cartes ou d'un départ à zéro.

Dans tous les cas, pour l'Afrique, cette crise présente des opportunités certaines, qu'il faudra saisir.

Sans pour autant soulever le sempiternel débat sur l'opposition entre le déploiement des infrastructures physiques et celui des infrastructures digitales, on notera que cette crise est une opportunité pour l'Afrique. Elle lui offre l'occasion de se réinventer et surtout de prendre son destin en main.

Le continent a d'ores et déjà marqué, de façon inédite, l'exploit d'accélérer le déploiement des réseaux mobile face à l'absence des réseaux filaires. Il a également généralisé, en un temps record, l'adoption du Mobile Money comme alternative aux réseaux des banques traditionnelles, pour bancariser et favoriser l'inclusion financière. Et peut, bien sûr, réussir l'exploit de gagner les défis de l'E-santé, l'E-éducation, de l'agritech, de l'E-commerce ou encore de l'administration électronique, de façon à servir de laboratoire dans les nouveaux usages, pour le reste du monde.

Tenir compte des préalables

Plus que jamais, « l'abordabilité » des coûts d'accès demeure une question centrale dans l'inclusion du numérique en Afrique. Une approche plus réfléchie et plus volontariste dans les stratégies nationales devrait favoriser une politique plus ambitieuse en termes d'accès universel au haut débit. Une fois la question des accès résolue, on pourra aborder, de façon plus holistique, la question de l'accélération des usages. C'est une évidence pour l'Afrique.

Le continent, qui compte une population très jeune, pourra susciter des usages nouveaux, en rapport avec les problématiques locales. Les avancées de l'IA ont favorisé le passage de l'informatique transactionnelle au conversationnel. Elles promettent d'accélérer tous ces processus, mais cela passe obligatoirement par la formation et par l'acquisition des connaissances.

Enfin, le télétravail représente un changement de paradigme important en matière de cybersécurité. Aussi pratique et efficace qu'il puisse paraitre, il peut révéler des failles de sécurité. La population a besoin d'être sensibilisée aux diverses attaques : le ransomware, qui est comparé à une prise d'otage - en version numérique - avec un criminel anonyme ; le vol massif de données ; le piratage mobile, qui est devenu une pratique courante en Afrique.

Si nous voulons tirer les enseignements de cette pandémie, nous pouvons dire que l'Humanité a une formidable capacité de résilience et une grande capacité d'adaptation. Néanmoins, elle reste vulnérable aux changements soudains. Au moment où nous scrutons l'ère post-Covid et les plans de relance, nous pouvons affirmer avec certitude que le retour à la normal se conjuguera désormais - et de façon durable - avec le suffixe « télé ». Il conviendra de l'associer à toute activité socioéconomique. C'est une aubaine pour pallier le manque ou l'inexistence d'infrastructures physiques pour les pays en développement. Et quand les derniers seront les premiers, on pourra alors reparler de cette remise à zéro des compteurs pour un nouveau départ.

SOMMAIRE

N°69 AVRIL - MAI - JUIN 2021

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);
Zakaria Gallouch (Maroc); 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

Experts :
Marie de Fréminville, Présidente de Starboard Advisory
Jean-Michel Huet, Associé - Olivier Darondel, Senior manager
Marouane Znagui, Manager et Chloé Chevrand - Consultante - Bearing Point
Salah Baïna, Consultant en transformation digitale

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

Cybersécurité et télétravail :

50 twittos à suivre en Afrique

Une étude réalisée par SMART DATA POWER

L'AFRIQUE EN CHIFFRE INÉDIT

Ce sont des institutions, des entreprises, des associations et des personnalités. Elles débattent autour de la cybersécurité et du télétravail sur Twitter. Qui sont ces Twittos ? Où habitent-ils ? Quel est leur degré d'influence dans leurs communautés ? Une cinquantaine de profils activant sur le continent a été repéré, grâce à une recherche exclusive et originale menée avec notre partenaire Smart Data Power. Voici quelques clés de lecture pour comprendre cette étude documentée.

Souleyman Tobias

Innovation

C'est une première ! *« L'Afrique en Chiffres »* de ce nouveau numéro de CIO Mag est alimenté par une *« étude maison »*. Elle se concentre sur la Twittosphère et nous permet d'identifier les acteurs clés qui se démarquent par leurs intérêts pour les deux tendances de l'année : la cybersécurité et le télétravail.

Pour notre magazine IT, il s'agit de confirmer notre capacité à innover et à mettre en valeur les structures partenaires comme Smart Data Power.

50 Twittos, 3 nationalités

Pour Smart Data Power, il s'est agi de croiser les données collectées en conformité avec le Règlement général sur la protection des données personnelles (RGPD). Sur les questions de cybersécurité et de télétravail, 50 profils actifs sur Twitter émergent. Parmi eux, **61%** sont des entreprises et **14%** sont des universités, des instituts de recherches, des Think tank ou des laboratoires de recherches. Les associations ou les fédérations professionnelles représentent **11%** des profils. Les administrations et les institutions constituent pour leur part **8%** du taux d'influence et les associations, les ONG et les fondations **6%.**

Les trois pays de provenance de la plupart des influenceurs, qui débattent sur les deux thématiques, sont l'Afrique du Sud (avec 18 Twittos), le Nigéria (13) et le Kenya (8).

Une cybermenace localisée

Selon les données fournies, la cybermenace se concentre sur les trois pays africains qui regroupent le plus de Twittos, ce qui constitue une explication sur leur prise de parole active. Ces pays sont identifiés comme étant les plus exposés aux attaques de logiciels malveillants avec **10 millions** pour l'Afrique du Sud, **14 millions** au Kenya et **3,8 millions** au Nigéria.

Les chiffres avancés par Kaspersky sur le nombre de cyberattaques en Afrique (**28 millions**), entre janvier et août 2020, prouvent que la menace est bien réelle. Quel est alors le niveau d'exposition, par zone géographique, sur l'ensemble du continent ? En croisant les données avec celles du Cybersecurity Exposure Index (CEI-2020), il en ressort globalement que la vulnérabilité est souvent fonction du taux de connectivité des pays !

La sélection

Dans cette cyberétude, les acteurs considérés sont soit des professionnels de la cybersécurité, soit des personnes intéressées par le sujet. Grâce à sa capacité à rendre inteligible la masse de données dont regorge Twitter, Smart Data Power a su classer les Twittos repérés par leur zone d'influence. Les critères pris en considération sont : l'importance de la communauté de la cible, son utilisation récente du média social, ses tweets et retweets, la croissance de sa communauté et le taux d'attraction que génèrent ses publications. Ces critères ont permis de remonter les tops influenceurs des deux thématiques abordées.

Il ne s'agit donc pas d'une enquête exhaustive, mais orientée uniquement vers ceux qui ont une présence effective sur Twitter et qui traitent des deux sujets. Grâce à son savoir-faire et ses technologies modernes pour rendre lisible la Big Data, Smart Data Power nous permet de vous offrir une vue plus originale, plus intuitive et plus innovante des chiffres clés sur la cybersécurité et le télétravail. N'oubliez donc pas de scanner le code QR en page 10 pour accéder à l'intégralité de cette étude.

Bonne lecture !

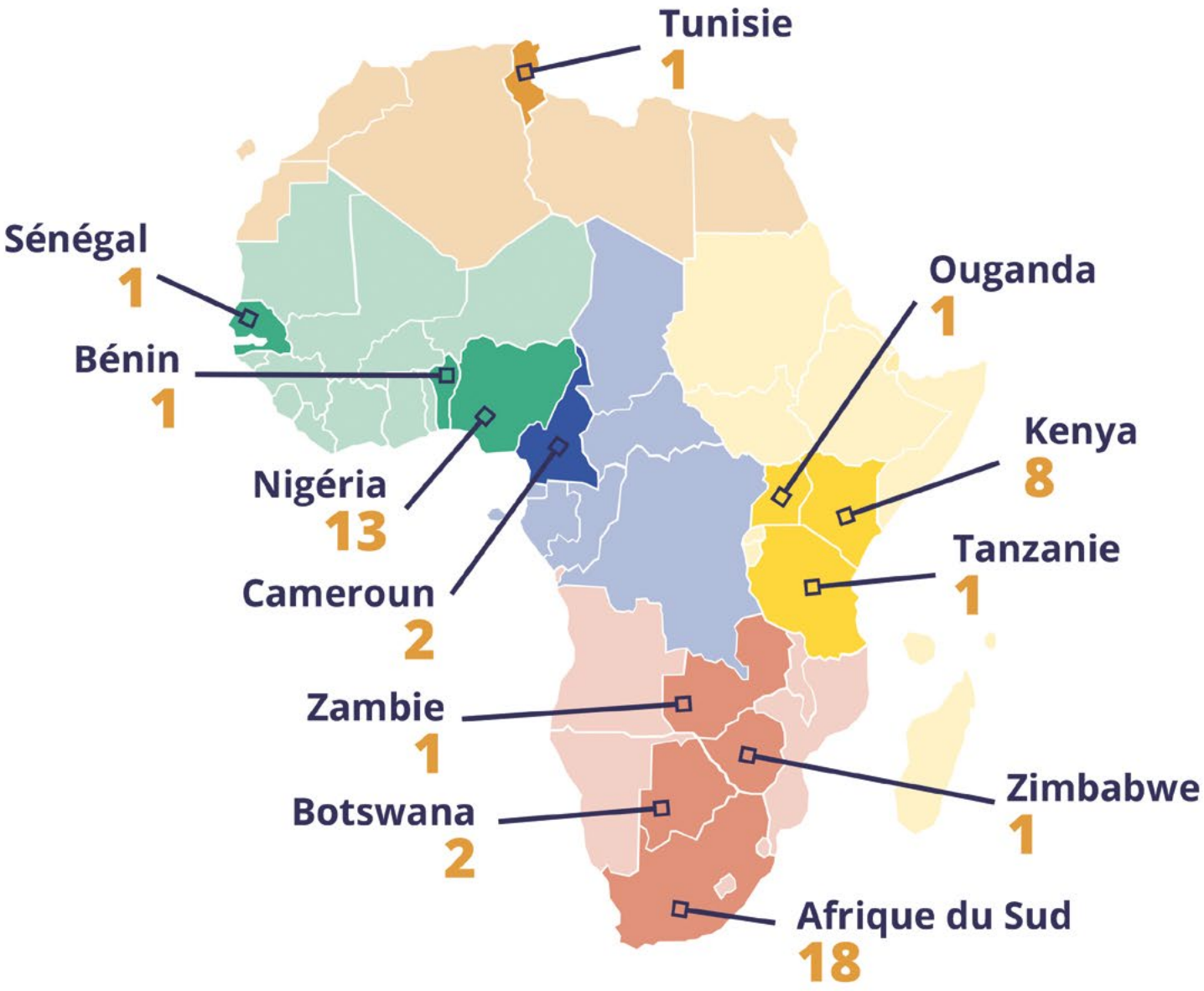
Les 50 twittos sélectionnés (de 1 à 25)

IDENTIFIANT TWITTER	NOM / PSEUDO	SCORE / 100	TYPOLOGIE TWITTOS	LOCALISATION	MÉTIER
@CA_Kenya	CA@20	86	Organisation	Kenya	Administration / Institution
@iLabAfrica	@iLabAfrica	85	Organisation	Kenya	Université / Institut / Labo de recherche / think tank
@BakeKenya	BAKE Kenya	84	Organisation	Kenya	Association / Fédération professionnelle
@JesseOguns	Jesse Block	83	Personne	Nigeria	Spécialiste cryptomonnaie
@UCTGSB	UCT Graduate School of Business	83	Organisation	Afrique du Sud	Université / Institut / Labo de recherche / think tank
@lawyershubkenya	Lawyers Hub Kenya	81	Organisation	Kenya	Association / Fédération professionnelle
@jeanfrancis	Jean-Francis AHANDA	79	Personne	Cameroun	Chef d'entreprise / Entrepreneur
@obs_senegal	Orange Business Services Sénégal	78	Organisation	Sénégal	Entreprise
@sasahost	Sasahost Limited	77	Organisation	Kenya	Entreprise
@RSM_za	RSM ZA	76	Organisation	Afrique du Sud	Entreprise
@nizarus	Nizar Kerkeni - @nizarus@mamot.fr	75	Personne	Tunisie	Fondateur d'association
@followlsstf	Lagos State Security	72	Organisation	Nigeria	Administration / Institution
@ZenzoLusengo	Zenzo L	70	Personne	Afrique du Sud	Chef d'entreprise / Entrepreneur
@OnDemandZA	Tarsus On Demand	70	Organisation	Afrique du Sud	Entreprise
@DanielMaithyaKE	Daniel Maithya	70	Personne	Kenya	Stratégiste digital
@Anssi_Bénin	ANSSI-Bénin	69	Organisation	Bénin	Administration / Institution
@Sabric	SABRIC	69	Organisation	Afrique du Sud	Entreprise
@Inlaks	Inlaks Nigeria	69	Organisation	Nigeria	Entreprise
@tommakau	Tom Makau	66	Personne	Kenya	Consultant
@jidaw	Jide Awe	66	Personne	Nigeria	Consultant
@IITPSA	IITPSA	63	Organisation	Afrique du Sud	Association / Fédération professionnelle
@Thoppy	TblaQ...	63	Organisation	Nigeria	Entreprise
@Adept_ICT	Adept ICT	62	Organisation	Afrique du Sud	Entreprise
@Oshosam	Samuel Osho	61	Personne	Nigeria	Consultant
@RSAWEB	RSAWEB	61	Organisation	Afrique du Sud	Entreprise

Les 50 twittos sélectionnés (de 26 à 50)

IDENTIFIANT TWITTER	NOM / PSEUDO	SCORE / 100	TYPOLOGIE TWITTOS	LOCALISATION	MÉTIER
@SwahiliDigital	Swahili Digital	61	Organisation	Tanzanie	Entreprise
@Isoc_Cameroon	ISOC Cameroon	60	Organisation	Cameroun	Association / ONG / Fondation
@DanielOpio_	Daniel Opio	60	Personne	Ouganda	Chef d'entreprise / Entrepreneur
@UCT_ICTS	ICTS at UCT	58	Organisation	Afrique du Sud	Université / Institut / Labo de recherche / think tank
@ispa_za	ISPA (South Africa)	55	Organisation	Afrique du Sud	Association / Fédération professionnelle
@LawTrustInfoSec	LAWtrust	55	Organisation	Afrique du Sud	Entreprise
@Questechie	John Onwuegbu	54	Personne	Nigeria	Blogger
@Pinki_licious	PINK PANTHER	54	Personne	Nigeria	Chef d'entreprise / Entrepreneur
@SignalAlliance	Signal Alliance	52	Organisation	Nigeria	Entreprise
@TSystemsSA	T-Systems SA	52	Organisation	Afrique du Sud	Entreprise
@despringsltd	Desprings	51	Organisation	Zimbabwe	Entreprise
@HostifyCo	Hostify.co.za	49	Organisation	Botswana	Entreprise
@ITIQBotswana	IT-IQ Botswana	49	Organisation	Botswana	Entreprise
@agrisols	Agrisol a Product of Sangana Africa	49	Organisation	Afrique du Sud	Entreprise
@Bonga_777	Bonga Ntombela	48	Personne	Nigeria	Chef d'entreprise / Entrepreneur
@robykenya	marlyk	47	Personne	Afrique du Sud	Étudiant
@WestechConnect	Westech - better than the rest	47	Organisation	Afrique du Sud	Entreprise
@ESET_EA	@ESET_EA	42	Organisation	Nigeria	Entreprise
@Schneider_NG	Schneider Electric Nigeria	42	Organisation	Zambie	Entreprise
@CyberZambia	Zambian Cyber Security Initiative Foundation	40	Organisation	Afrique du Sud	Association / ONG / Fondation
@GerritM_Olivier	Gerrit Olivier	39	Personne	Afrique du Sud	Chef d'entreprise / Entrepreneur
@dialanerdsa	Dial a Nerd	39	Organisation	Kenya	Entreprise
@igovafrica	iGov Africa	39	Organisation	Nigeria	Université / Institut / labo de recherche / think tank
@thehatchilab	thehatch Innovation Lab	37	Organisation	Nigeria	Université / Institut / Labo de recherche / think tank
@OneVaultSA	OneVault	33	Organisation	Afrique du Sud	Entreprise

Résultats par localisation



*nombre de représentants par pays

SMART DATA POWER

3 nationalités ressortent nettement parmi les profils sélectionnés : les Sud-Africains, les Nigérians et les Kenyans.

Près de la moitié des twittos sélectionnés vivent au sud de l'Afrique, majoritairement en Afrique du Sud.

SCAN ME

Télécharger l'enquête

Retrouvez l'intégralité de notre étude en scannant le QR code ci-contre

SANTÉ

Les centres hospitaliers, nouvelles cibles des cyberattaques

En Europe comme aux Etats-Unis, les établissements hospitaliers sont pris pour cible. L'accès à Internet et au système informatique est coupé ; les postes de travail et les appareils sont déconnectés du réseau, etc. Les hôpitaux risquent la paralysie de leur système de santé et la vie des patients est en jeu à cause de la recrudescence des cybermenaces. L'Afrique est-elle préparée pour faire face à cette nouvelle forme d'attaque ?

Michaël Tchokpodo

« Selon le rapport de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), Ryuk aurait été responsable de 75% des attaques sur le secteur de la santé dans le monde, en octobre 2020 ». L'information est relayée par Frédéric Lemaire, Directeur France de Cohesity, une entreprise privée californienne des technologies de l'information. Il explique que ce ransomware très lucratif serait, selon le FBI, le plus rentable. Il aurait généré environ 61 millions de dollars (plus de 30 milliards de francs CFA), entre février 2018 et octobre 2019.

Philippe Trouchaud, chargé de la cybersécurité chez PWC, l'un des principaux cabinets de conseil au monde, estime que *« les cyberattaques contre les hôpitaux ont bondi de 500% depuis l'arrivée de la Covid-19. »* Entre mars et avril 2020, une vingtaine de cyberattaques ont été identifiées. Il s'agit plus fréquemment d'une stratégie de ransomware menée via un email de phishing, lequel permet aux cyberattaquants de prendre en otage les données personnelles des patients en les cryptant. Ils parviennent ainsi à bloquer l'accès au système informatique de l'hôpital en réclamant une contrepartie pécuniaire.

Une « cible facile »

La cible hospitalière est davantage privilégiée par les cybercriminels, qui trouvent en la Covid-19 une opportunité pour rançonner des hôpitaux. Cette faille s'est créée du fait de la digitalisation du processus de prise en charge des patients et des traitements administrés. Et les hôpitaux ne sont pas les seuls concernés. Tout le système sanitaire est exposé, à l'instar des laboratoires pharmaceutiques, des cliniques privées, des centres de rééducation, etc.

« Les établissements hospitaliers constituent une cible très facile parce qu'ils ne sont pas protégés et qu'ils ne sont pas suffisamment matures en matière de cybersécurité. S'ils sont aujourd'hui victimes de cybermenaces, c'est juste un concours de circonstance. La pandémie de Coronavirus a en effet mis la santé en lumière. Or, les DSI des centres hospitaliers, qui étaient sous pression, avaient bien d'autres préoccupations que de mettre à jour leur logiciel, de vérifier des failles ou de se concentrer sur la sécurité », justifie Mohammed El Bouzidi, directeur du pôle Système d'information du groupe Akdital Holding.

Ce groupe de santé privé au Maroc est leader dans son domaine. A son actif, sept cliniques et hôpitaux privés, dont l'Hôpital privé Casablanca Ain Sebaa.

Les conséquences de ces cyberattaques sont souvent sans appel. L'arrêt des serveurs entraîne le ralentissement des activités, la désorganisation et la déprogrammation. Des risques évidents liés à la qualité du diagnostic sont à craindre, tout comme ceux inhérents à la santé du patient, sans compter l'impact financier. Le pire est arrivé en Allemagne, où une patiente a succombé au cours d'un rançongiciel, alors qu'elle devait subir une opération chirurgicale.

Prévenir les cyberattaques

En Afrique, la défaillance d'un plateau technique et le manque d'informations sanitaires sont à l'origine des déficiences liées au système de santé. Les populations succombent sous l'effet des épidémies, mais surtout des maladies endémiques, tel le paludisme.

Même si le continent a entamé une ère de digitalisation, les disparités et la fracture numérique entravent sa généralisation. Et la cybersécurité reste, dans la plupart des cas, le maillon faible des politiques de transformation numérique.

Mais, bien qu'étant moins outillée, l'Afrique ne sera pas pour autant exemptée de cette nouvelle forme de cyberattaque.

« Les DSI doivent se former sur ces risques et mettre en place un Plan de continuité d'activité (PCA), qui consiste à travailler en mode dégradé (back-up), pour éviter tout arrêt brusque de l'activité. On n'est jamais à l'abri d'une cyberattaque, mais si on s'est préparé, on en subit moins les conséquences », conseille Mohammed El Bouzidi.

« Il faut sensibiliser les collaborateurs aux bonnes pratiques informatiques et travailler en réseau local si les systèmes d'information internes ne sont pas fiables. Cette mesure vise à préserver les serveurs stratégiques d'une exposition externe. Et inciter les responsables des centres hospitaliers en Afrique à investir davantage sur le volet informatique et cybersécurité. »

Pour Frédéric Lemaire, il faut *« disposer d'un système immuable de sauvegarde des données. Lorsqu'il est utilisé avec un modèle de sécurité RBAC (Role Based Access Control) et une authentification à plusieurs facteurs, ce système constitue un dispositif solide pour permettre la récupération et limiter les dommages. »* Mais, comme l'explique Mohammed El Bouzidi, face aux risques de cyberattaques, l'Afrique doit privilégier la prévention.

En adoptant, par exemple, des logiciels open source, lesquels sont moins coûteux. Ils offrent de surcroit un bon niveau de sécurité. Cette solution s'oppose à la riposte qui, en plus d'engendrer des dégâts énormes, nécessite des moyens et du temps pour juguler la crise. Car les cyber menaces risquent fort d'augmenter. *« Avec la démocratisation future de la 5G, il y aura, à l'avenir, davantage de cyberattaques »*, prévient Philippe Trouchaud.

OFFSHORING
Le Maroc conserve son leadership malgré la crise

Bien que la pandémie ait impacté plusieurs secteurs de l'économie marocaine, elle a aussi été favorable à d'autres secteurs d'activités. Cette conjoncture économique spécifique a été particulièrement bénéfique à l'Offshoring, qui s'est distingué notamment via ses centres de contacts multicanaux et ses opérateurs de BPO (Business Process Outsourcing). La Covid-19 a servi de révélateur à de nouveaux modes opératoires et à des opportunités économiques, ce qui a profité au développement du secteur. L'Offshoring s'est saisi de cette opportunité pour implémenter le télétravail à grande échelle et pour renforcer sa résilience managériale. En réponse aux mesures de distanciation, de nouvelles perspectives de développement ont été envisagées, dont l'E-commerce qui connaît une progression historique dans les marchés clients.

Zakaria Gallouch

Aujourd'hui l'activité représente un chiffre d'affaires de 14 MMDH, avec plus de 120 000 emplois et 5 écosystèmes. Ce poids lourd de l'économie marocaine est le troisième secteur industriel pourvoyeur de devises du Maroc et le premier pourvoyeur d'emplois en 2020 (auparavant second après l'automobile). L'Offshoring contribue à hauteur de 5% à la croissance du PIB. A l'international, le Royaume est l'un des leaders régionaux, et notamment numéro un pour le monde francophone, où il maintient son leadership avec 50% de parts de marché. Ses champions nationaux sont engagés dans une dynamique d'expansion internationale, avec des ouvertures en Afrique et en Europe, à l'instar des groupes Majorel et Outsourcia.

Cette évolution spectaculaire résulte de la politique volontariste de l'Etat et de sa stabilité, et de l'offre

d'une infrastructure qui répond aux normes internationales. Des atouts qui bénéficient au Maroc et lui permettent de se distinguer de ses concurrents. Ils profitent également à la fédération du secteur, laquelle peut marquer son ancrage dans les cercles économiques influents.

La Fédération marocaine de l'externalisation des services (FMES) vient ainsi d'être cooptée par la Confédération générale des entreprises du Maroc (CGEM), qui n'est autre que le patronat du pays. Pour la Fédération sectorielle statutaire externe, c'est le signe de la reconnaissance du caractère stratégique de l'activité de l'externalisation de façon générale.

Continuité des services avec le télétravail

Contacté lors de la préparation de ce dossier, Youssef Chraïbi, Président de la FMES et PDG du groupe Outsourcia, a expliqué que le passage vers le télétravail s'est opéré avec fluidité car il avait été anticipé par les différents opérateurs, avant qu'il ne devienne obligatoire. *« Le premier critère a été l'anticipation. Nous avons vu la crise venir à l'avance, ce qui nous a permis d'être prêts lorsque les mesures de confinement ont été prises au Maroc. Nous avons donc migré très tôt vers le télétravail et avons transféré plusieurs dizaines de milliers de collaborateurs vers le travail à domicile. Ce choix a permis d'assurer la continuité des activités de nos clients, dans le respect de leurs exigences en termes de sécurité et de qualité de service. »* Pour les activités nécessitant la présence des collaborateurs sur site, les outsourcers ont mis en place les mesures de distanciation sociale, avec un taux d'occupation de la capacité de leurs plateaux limité à 40 %. Les salariés ont ainsi pu travailler dans le respect des normes de sécurité anti Covid-19.

L'autre facteur de la fluidité du switch est la prédisposition technologique et managériale du secteur à la collaboration à distance. *« Les acteurs du secteur disposaient déjà d'un ensemble d'outils collaboratifs, de processus dédiés à la sécurité des données et des technologies nécessaires pour télétravailler. Tout ceci a facilité la gestion des opérations à distance ».*

Sécurité des données

Pour réussir ce challenge, le management a adressé les différentes zones de compromis qui pouvaient affecter sa performance : la productivité, la qualité des services et la sécurité des données. Ces trois volets ont été évalués à distancepar les managers, en temps réel, via une panoplie de mesures et d'indicateurs dédiées. A savoir : le temps passé sur une intervention, le temps d'activités, l'assiduité...

En matière de sécurité des données, le secteur faisait partie des bons élèves bien avant la crise. Ceci s'explique par sa connexion avec des partenaires nationaux et internationaux, qui exigent des dispositifs de cybersécurité auprès des outsourcers.

« *Nous avons travaillé en étroite collaboration avec la Commission nationale de contrôle de la protection des données (CNDP). Et pour se conformer à la réglementation marocaine sur la protection des données, chaque entreprise a dû mettre en place un dispositif à la fois technique et humain, ainsi qu'une organisation adaptée* », a fait remarquer Youssef Chraibi. Il a précisé qu'à l'heure actuelle, ces mesures sont exigées par les donneurs d'ordre. « *Nous sommes obligés de nous conformer à ces exigences pour pouvoir accéder à certains marchés. Et sur ce point, les acteurs marocains sont très en avance.* »

Formation des compétences

S'agissant des défis et des challenges que doit relever le secteur de l'Offshoring, Youssef Chraibi évoque la formation et le développement du vivier de compétences. Il considère ce chantier comme prioritaire pour conserver la compétitivité.

« *Pour pouvoir accompagner cette forte croissance, la formation est le chantier le plus important. Ce secteur, qui a démarré depuis 20 ans, a connu une forte croissance ces dernières années, mais elle est limitée par la taille du bassin d'emploi du marché. Le Maroc regorge de compétences offshores, mais le besoin devient de plus en plus pressant pour les soft skills et les compétences en termes de communication et de maîtrise des langues* », insiste-t-il.

Youssef Chraibi plaide par ailleurs pour la mise en place d'un contrat programme, dans l'objectif de renforcer le leadership marocain dans la région. « *Le Maroc est pionnier dans les métiers de l'Offshoring en Afrique et il est également leader pour le monde francophone. Mais, nous sommes de plus en plus concurrencés par un certain nombre de destinations africaines, qui gagnent en attractivité* », souligne-t-il. Pour le président de la Fédération marocaine de l'externalisation des services, la solution consisterait à réduire le différentiel de coût avec d'autres destinations, tout en renforçant un positionnement haut de gamme.

TELECOMS

« Orange va investir 1 milliard d'euros par an en Afrique pour accroître la couverture réseau »

La pandémie de Coronavirus a impacté le monde entier et révélé la place prépondérante que joue le numérique pour répondre à une situation de crise. Afin que l'ensemble des populations du continent puissent en profiter, les investissements doivent se poursuivre. En effet, l'accès universel à une couverture Internet est plus que jamais nécessaire, et les grands groupes l'ont bien compris. Alioune Ndiaye, CEO d'Orange MEA, fait le point pour CIO Mag.

Alioune Ndiaye
CEO d'Orange Moyen-Orient/Afrique

CIO Mag : Face à la crise économique et sanitaire de la Covid-19, comment Orange MEA a-t-il traversé cette année 2020 ? Cela a-t-il impacté vos plans stratégiques ?

Alioune Ndiaye : Pendant la crise de la Covid-19, les infrastructures de télécommunications se sont révélées plus essentiels que jamais pour les gouvernements, les entreprises et les familles. Au début de la crise, on a vu le trafic data augmenter de 60% dans certains pays. Et sur l'année 2020, nous avons globalement constaté que la consommation data mobile par utilisateur avait quasiment doublé.

On note également que la crise a eu un effet d'accélérateur sur l'activité du Très haut débit. Nous comptons aujourd'hui plus de 33 millions de clients 4G, dans les 17 pays d'Afrique et du Moyen-Orient où nous sommes présents.

Ceci confirme que dans notre activité, le poids de la data nécessite des investissements majeurs dans les réseaux. Pour donner accès au numérique au plus grand nombre, nous allons donc poursuivre cet objectif en continuant d'investir 1 milliard d'euros chaque année, en Afrique. Le but est d'accroître la couverture et la capacité de nos réseaux et d'augmenter le débit Internet de nos 128 millions de clients.

Vous avez récemment annoncé l'arrivée de la 5G sur le continent, d'ici à fin 2021/2022. Est-ce que cette échéance

INTERVIEW

Alioune Ndiaye
CEO d'Orange
Moyen-Orient/Afrique

est réalisable ? Et quels seront les premiers pays concernés par cette nouvelle technologie ?

A.N : Nous avons désormais la 4G dans tous les pays d'Afrique et du Moyen-Orient, où nous sommes présents, sauf en RCA. Et on commence à intégrer, dans nos plannings, la 5G dans la zone MENA, au Sénégal et en Côte d'Ivoire. On pourrait voir les premiers déploiements en 2022.

En Afrique, la 5G pourra permettre, par exemple, de désengorger des réseaux mobiles saturés, notamment dans les zones densément peuplées, comme Dakar où Sonatel a déjà lancé des tests en 5G. L'objectif est d'être en mesure d'introduire cette technologie, d'ici à fin 2022. Il y aura beaucoup de travail sur la mise à niveau de notre réseau, sur des investissements à faire, sur le plan de la formation et de montée en compétence des équipes.

Mais surtout, il faut souligner que ce déploiement se fera sous réserve de la mise en place, par les autorités, du cadre nécessaire en termes de disponibilité des fréquences et d'autorisations.

Djoliba, le premier backbone ouest-africain, vient d'être mis en place par Orange. Que va-t-il apporter ? Existe-il d'autres projets de ce type pour relier d'autres pays ?

A.N : La connectivité, en particulier haut débit, est en effet un véritable accélérateur de croissance pour les pays. La croissance des usages 4G (et demain 5G) et fibre, dans les pays africains, va nécessiter le développement massif des infrastructures, mais aussi des infrastructures internationales, sous-marines et terrestres.

La stratégie d'Orange est d'être un acteur majeur de ces réseaux, tout en tirant parti de toutes les mutualisations possibles. Nous avons de nombreux projets qui illustrent notre engagement pour renforcer la connectivité en Afrique :

- Le câble sous-marin « **Africa Coast to Europe** » (ACE). Initié par Orange, en partenariat avec 16 autres opérateurs, il connecte la France aux pays d'Afrique de l'Ouest. Déjà opérationnel à Sao Tomé et Principe, ACE poursuit actuellement sa route vers l'Afrique du Sud. Il reliera, à terme, 24 pays et 400 millions de personnes.

- **Main One** est un câble sous-marin de 7 000 km, qui relie le Portugal au Nigeria. En 2019, Orange a signé un partenariat avec Main One pour créer deux stations d'atterrissement au Sénégal et en Côte d'Ivoire. Ces extensions du câble permettront aux deux pays de bénéficier d'une meilleure connectivité, de prix plus abordables et d'accéder à de nouveaux services.

- Orange fait partie du consortium « **2Africa** ». Il est notamment composé de Facebook et China Mobile, qui finance la construction d'un des plus longs câbles sous-marins du monde. D'une longueur de 37 000 km, il fera à terme le tour de l'Afrique. La mise en service du câble 2 Africa est prévue en 2023-2024. Il facilitera le déploiement de la 4G, de la 5G et de l'accès haut débit fixe pour des centaines de millions de personnes.

- Et, plus récemment, **Djoliba**, le premier réseau de fibre optique panafricain déployé par Orange. Il relie les principales capitales d'Afrique de l'Ouest. Et va permettre de développer l'accès aux technologies digitales dans la région. Les populations locales vont pouvoir accéder encore plus facilement à des services de santé ou d'éducation, ainsi qu'aux usages offerts par le cloud computing. Ou encore à des contenus hébergés dans des data centers localisés en Afrique de l'Ouest, plutôt qu'en Europe ou aux États-Unis.

En quoi le déploiement de la 5G sur le continent peut permettre d'adresser les Objectifs de développement

durable (ODD) de l'ONU ? N'est-ce pas au contraire une source supplémentaire de pollution numérique ?

A.N : La crise sanitaire a montré la forte appétence des populations pour les usages du numérique. Le déploiement d'un nouveau réseau 5G, capable d'absorber plus de connexions simultanées en mobilité, est donc nécessaire pour éviter toute saturation dans les zones très denses.

La 5G est la première norme mobile qui intègre, dans son design, l'optimisation de la consommation énergétique. Les antennes s'activent uniquement à la demande. C'est-à-dire qu'elles ne transmettent que dans la direction des terminaux qui en ont besoin et seulement au moment où ils en ont besoin. C'est donc, en réalité, une des solutions à la transition environnementale car elle est dix fois plus efficace, en terme énergétique et à consommation comparable, que la 4G.

La 5G, en Afrique comme ailleurs, va favoriser l'avènement de l'Intelligence artificielle et de nouveaux services intelligents grâce aux performances qu'elle procure en termes de vitesse, de temps réel et de temps de latence. La 5G va être une véritable révolution pour les opérations à distance, pour la ville intelligente et pour la maîtrise de l'empreinte énergétique.

Cela va contribuer à améliorer les conditions de vie et le bien-être quotidien des populations, toute chose permettant d'atteindre plus rapidement la réalisation des Objectifs de développement durable.

Propos recueillis par Camille Dubruelh

Après des études en Finances et Contrôle de Gestion, à l'Université Paris Dauphine et dans les Télécoms, à Télécom Ecole de Management, **Alioune Ndiaye** a débuté sa carrière dans l'industrie chez Pechiney. Puis, il a intégré Sonatel, en 1988, sur des fonctions d'audit et de contrôle de gestion. Il a par la suite exercé comme Directeur financier, pendant une dizaine d'années.

En 2002, **Alioune Ndiaye** devient directeur général à Ikatel, au Mali, avant de revenir, en 2012, à la Sonatel. Depuis cette date, il occupe les fonctions de Directeur Général et de président du Conseil d'administration de Sonatel Mobiles, Orange Mali, Orange Bissau, Orange Sierra Léone et de la Fondation Sonatel.

Depuis le 2 mai 2018, **Alioune Ndiaye** est le CEO d'Orange Middle East and Africa.

FOCUS
Le télétravail, porte d'entrée des cyberattaques ?

Le monde est entré dans une nouvelle année, mais la Covid-19 continue d'imposer les mêmes défis. Cachés dans les réseaux Internet nationaux, régionaux ou privés, des acteurs anonymes exploitent les zones d'incertitude générées par le télétravail pour donner l'estocade aux entreprises déjà fragilisées par la pandémie. Décryptage.

Anselme Akeko

Sur les risques cyber induits par le télétravail, le Club des experts de la sécurité de l'informatique en Afrique (Cesia) a conduit une enquête dans 18 pays africains. Il a interrogé un ensemble de responsables de sécurité des systèmes d'information (RSSI) et de directeurs de systèmes d'information (DSI). Et le Cesia a constaté que seulement 10 % de leurs collaborateurs se sont retrouvés en situation de télétravail. Le travail à distance n'a donc pas été généralisé pendant la crise sanitaire. Mais, dans les entreprises qui ont recours à cette forme de collaboration, les RSSI se sont posés plusieurs questions en amont de leurs décisions.

Selon Didier Simba, fondateur et président du Cesia, leur principale problématique a concerné la sécurité.

Sur ce point, il est difficile de leur donner tort. Le taux d'attaques cyber a en effet explosé avec la crise sanitaire. *« En France, plus 300 % d'attaques ont été enregistrées dès le mois d'avril 2020. En Afrique, 82 % des entreprises ont été victimes d'au moins une cyberattaque, soit un bond de 17 % par rapport*

à l'année précédente (65 %) », révèle Didier Simba. *« Personne n'est à l'abri. Les cybercriminels vont de plus en plus vers des entreprises qui gèrent des infrastructures critiques : l'eau, l'électricité, l'énergie, la santé. C'est déjà le cas pour les banques »*, s'inquiète pour sa part Franck Kié, consultant ivoirien en cybersécurité et également président de CyberObs et fondateur du Cyber Africa Forum.

Phishing et ransomware

Grâce au télétravail, des chefs d'entreprise ont pu permettre à leurs employés d'exécuter des tâches à distance. Seulement, les télétravailleurs sont beaucoup plus exposés à des attaques informatiques. Parmi les infractions les plus fréquentes, en ces temps de Covid, nos interlocuteurs en ont répertorié deux.

D'abord, l'hameçonnage ou « phishing ». Ce sont des mails usurpateurs de marques ou d'identité, qui sont destinés à leurrer le récepteur pour l'inciter à communiquer des données personnelles, en se faisant passer pour un tiers. Selon le rapport du Cesia, une flambée de phishing a été observée en 2020 (+ 75 %). *« Typiquement, c'est le genre d'attaques qui marche »*, assure Franck Kié. Ce consultant pour des entreprises, qui mènent des campagnes de sensibilisation sur cette menace, dit en avoir monitoré un grand nombre, en décembre 2020. Leurs taux de clics, basés sur de fausses promesses, sont largement supérieurs à ceux des campagnes de phishing classiques.

Une part croissante des cyberattaques dans le monde professionnel s'effectue aussi par rançongiciels ou « ransomwares ». Il s'agit d'intrusions informatiques ou de codes malveillants visant à bloquer le fonctionnement d'un système ou l'accès au contenu, afin d'extorquer de l'argent à la victime. *« Pendant ce temps, déplore Franck Kié, c'est une activité qui tourne au ralenti ou pas du tout. Aujourd'hui, les entreprises, qui font face à ce fléau, ne sont pas forcément de grands groupes internationaux. On parle de grosses entreprises et de PME nationales de même volume. »* Cette attaque est redoutable, d'autant plus que le paiement de la rançon ne garantit ni le rendu de vos données, ni le retour à un fonctionnement normal. Pire, la victime peut être à nouveau rançonnée. Ce qui explique que les entreprises attaquées font appel à des ressources nationales ou étrangères pour débloquer la situation.

Selon le président du Cesia, le ransomware est l'attaque informatique qui marche le mieux depuis ces trois dernières années. *« Les cybercriminels attaquent de partout, même les hôpitaux ! Ce genre d'attaque s'est fortement généralisé en Afrique »*, observe Didier Simba.

Recrutement de RSSI

A cause de la Covid-19, les entreprises sont de plus en plus attirées par les solutions collaboratives, lesquelles contribuent à la simplification et à l'efficacité des processus métier. Dans ce contexte, la sensibilisation à la cybersécurité et le travail collectif sont recommandés. Mais sur le terrain, les pratiques sont loin d'être toutes alignées sur ce mot d'ordre.

« On a donné ces outils aux collègues sans leur expliquer réellement comment s'en servir et cela a créé des brèches pour les attaques potentielles. Aussi, pendant cette période, des entreprises ont prêté, sans prévention, des ordinateurs aux employés. Elles n'ont pas expliqué qu'il fallait faire la différence entre l'usage professionnel et personnel, et c'est encore une porte ouverte », argumente Didier Simba. Franck Kié ajoute : *« Si on ne met pas en place des VPN, pour sécuriser la connexion entre le poste de travail et le réseau de l'entreprise, l'employé peut utiliser des moyens de connexion publics, qui sont plus facilement attaquables. Cela représente un énorme risque auquel les travailleurs ne sont pas toujours sensibilisés. »*

Il est également important de souligner que le continent compte encore trop peu de RSSI. Pour le président du Cesia, les entreprises ne comprennent pas la pertinence de ce poste. Pourtant, les cas d'usage évoluent. *« Il faut agir sur l'humain : désigner un responsable sécurité, lui donner les moyens, mettre en place des programmes annuels de prévention »*. Les sociétés seraient-elles frileuses ? Manqueraient-elles de visibilité ? Elles sont, en tout état de cause, moins réceptives à l'idée d'investir dans le recrutement d'un RSSI. Et empilent des couches de sécurité (pare-feu, anti-virus, etc.), qui n'offrent pas toujours la protection voulue. Ces

firmes se rendent compte de l'importance de la cybersécurité lorsqu'elles doivent faire face à des incidents informatiques. Malheureusement, entre l'alerte et le temps requis pour rétablir le réseau, l'entreprise peut avoir perdu de l'argent et sa réputation. *« Si vous exercez dans un domaine réglementé, qui vous oblige à déclarer et à protéger des données personnelles, une attaque informatique peut impacter juridiquement votre entreprise »*, redoute Franck Kié.

Par ailleurs, les entreprises africaines ne communiquent pas sur les attaques qu'elles auraient subies. Pour Didier Simba, la raison est toute simple : *« Aucune réglementation en Afrique n'oblige une entreprise à déclarer une cyberattaque. Aucune entreprise ne va dire combien de données elle a perdu ou si elle a payé une rançon. Ce qu'on sait, en revanche, c'est que tous les pays africains sont ciblés. »*

L'humain, le maillon fort

Pour sortir de cette confusion, le président du Cesia est favorable à la création, dans chaque pays, d'une Agence nationale de sécurité des systèmes d'information (ANSSI) ou le renforcement de leurs prérogatives. *« Les ANSSI sont désormais présentes dans de nombreux pays. Elles doivent avoir les moyens de proposer de vraies stratégies et être rattachées à la plus haute instance : la primature ou la présidence. Ensuite, il faut que ces entités collaborent avec celles des autres pays, pour apporter des solutions globales et régler le problème des attaques sur plusieurs pays. »* Didier Simba poursuit en ces termes :

« Ces agences doivent produire des recommandations pour les entreprises. Elles doivent les accompagner pour investiguer, en les obligeant à déclarer ou à signaler les attaques, ainsi que ce qu'elles ont perdu. »

Le maillon fort de tout système de sécurité étant l'humain, l'expert déclare que la sensibilisation doit être la clé pour protéger l'entreprise. *« Une sensibilisation se prépare. Il s'agit notamment d'organiser des ateliers spécifiques et de mettre en place, sur toute l'année, une vraie culture cyber. »* Le président de CyberObs approuve ces recommandations et propose un benchmark des bonnes pratiques internationales. Et notamment la création d'une autorité semblable au New York State Department of Financial Services (Département des services financiers de l'État de New York). *« Cette autorité chargée de réglementer le marché financier a mis en place des règles en matière de cybersécurité. Ces règles obligent toute entreprise, opérant dans cet Etat, à rapporter, dans les 72 heures, toutes attaques informatiques dont elle serait l'objet. Votre entreprise est ainsi contrainte de mettre l'accent sur la cybersécurité pour ne pas ternir son image. »*

Franck Kié préconise également la mise en place d'un système de management de la sécurité informatique, respectant les normes ISO, lesquelles sont synonymes de connaissances et de bonne gouvernance. *« De façon générale, il faut plus de réglementation et plus de transparence pour observer plus finement l'évolution de la cybercriminalité et pour décider des mesures à prendre en termes de cybersécurité ».*

GLOSSAIRE
Comprendre le langage pour sécuriser les données et les équipements

La généralisation du télétravail, depuis la crise sanitaire, s'est accompagnée d'une augmentation des menaces sécuritaires pour les systèmes d'informations des entreprises. Aux dires des experts, la sécurité des infrastructures incombe désormais à tous les travailleurs. Et pour ceux qui ne s'étaient jamais intéressés au sujet, c'est le moment de se familiariser avec le langage des cybercriminels, mais aussi des Responsables de la Sécurité des systèmes d'information (RSSI) et des Directeurs des Systèmes d'information (DSI).

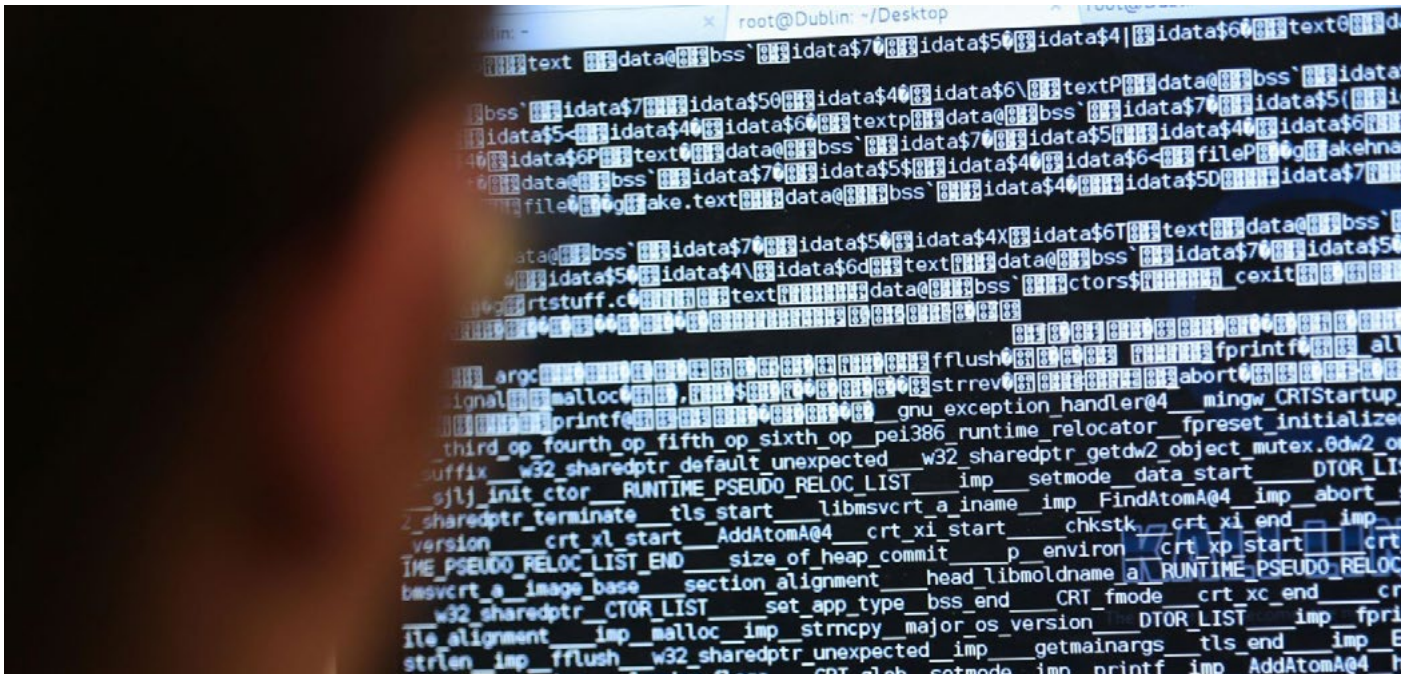
Souleyman Tobias

Les Brèches pour les Cybercriminels

La modification des habitudes de travail a ouvert des **Brèches**, que les **Cybercriminel**s exploitent depuis la crise sanitaire. Avec le télétravail, la connexion aux infrastructures professionnelles peut s'effectuer avec des terminaux privés. Et ces équipements ne sont généralement pas aussi bien protégés que ceux des entreprises.

Cet environnement hybride de travail a suscité l'intérêt des criminels informatiques. En Avril 2020, selon des données fournies par Google, plus de 18 millions de logiciels malveillants et de mails d'hameçonnage ont été repérés par les services du géant américain.

Cette tendance est venue s'ajouter aux 240 millions de **Spams** enregistrés, chaque jour, sur ses serveurs. Et tout est en lien avec la pandémie du Coronavirus.



L'Antivirus contre le Ransomware

A l'instar de ce qui est mis en place en termes de mesures anti-Covid, le télétravailleur devrait se protéger avec un **antivirus** informatique. Une fois installé sur le terminal (ordinateur ou smartphone), le logiciel détecte, bloque ou supprime des logiciels dangereux pour la sécurité des données et des équipements. Sans un antivirus, il serait par exemple possible d'être victime de **Ransomware**.

Le virus, qui peut s'installer malicieusement sur un terminal, rend illisible les fichiers et adresse une demande de rançon. Ce type d'attaque peut s'effectuer via un site web douteux ou un support externe (clé USB, disque externe, etc.).

Il est d'autant plus dangereux qu'il est à la portée de tout cybercriminel, même le plus novice. Même si les solutions pour déchiffrer les données cryptées par ce type de virus sont de plus en plus nombreuses, il vaut tout de même mieux prendre des précautions.

Travailler à distance peut donc créer une brèche. Cette faille informatique permet aux cyberdélinquants d'accéder, presque banalement, au serveur, aux données, etc. Selon le site spécialisé Tessian.com, les mails figurent, en ce moment, parmi les points faibles de la sécurité informatique. En consacrant 40% de son temps à gérer sa messagerie, on accroit les possibles hameçonnages (**phishing**) et autres intrusions malveillantes.

Un mail, dont on pense qu'il provient d'un contact fiable, peut être trompeur. Le but recherché est de faire communiquer des données sensibles (accès aux comptes bancaires, mots de passe...) et de les réutiliser à des fins criminelles.

Selon KnowBe4, une plateforme spécialisée en sécurité informatique, ces menaces ont bondi de 600% au premier semestre 2020. Il est en effet facile de tomber dans le piège lorsque l'on est pressé, stressé ou moins concentré. Et avec le télétravail, l'inattention peut s'accentuer. Alors prudence !

Le Pare-feu pour se protéger du Craker

Si la concentration protège contre les actes qui pourraient conduire à une faille sécuritaire, il est néanmoins utile de protéger l'accès au réseau. Les responsables de **sécurité** des systèmes d'information utilisent donc un pare-feu.

Ce dernier est destiné à protéger des transactions internes et externes. Il filtre les échanges au sein du réseau et ceux avec l'extérieur. Il est souvent restrictif, mais il protège des attaques souvent externes à votre réseau. Selon Digicert, le pare-feu *« est en première ligne de défense et empêche les attaques ou les menaces extérieures d'accéder à votre réseau ».*

Si le réseau professionnel est vulnérable, alors le risque de fuite de données est probant. Et les conséquences

de ces fuites sont lourdes pour les sociétés. Dans un article récent, Deloitte rappelle que *« le coût moyen d'une violation de données, résultant du travail à distance, peut atteindre 137 000 dollars US »*.

Le chiffre est extrait du rapport *« IBM Coast a Data Breach 2020 »*. En évitant une attaque sur son terminal (privé), on évite de devenir la brèche de son réseau professionnel et la porte d'entrée du **Craker**.

Les RSSI et DSI en première ligne contre les Bug

Dans le cas contraire, le **craker** pourra se servir du **crash** (une faille subite de votre système informatique) et casser les sécurités du système informatique **(cracking**). Pour minimiser les risques d'intrusion, il faut garder à l'esprit les directives des Responsables de la Sécurité des systèmes d'information (**RSSI**) ou des Directeurs des Systèmes d'information (**DSI**).

Cette attention permet de détecter le danger d'un simple **bug** (un mauvais fonctionnement souvent due à une mauvaise manipulation, à une erreur de programmation, etc.).

Le VPN pour garantir la Confidentialité

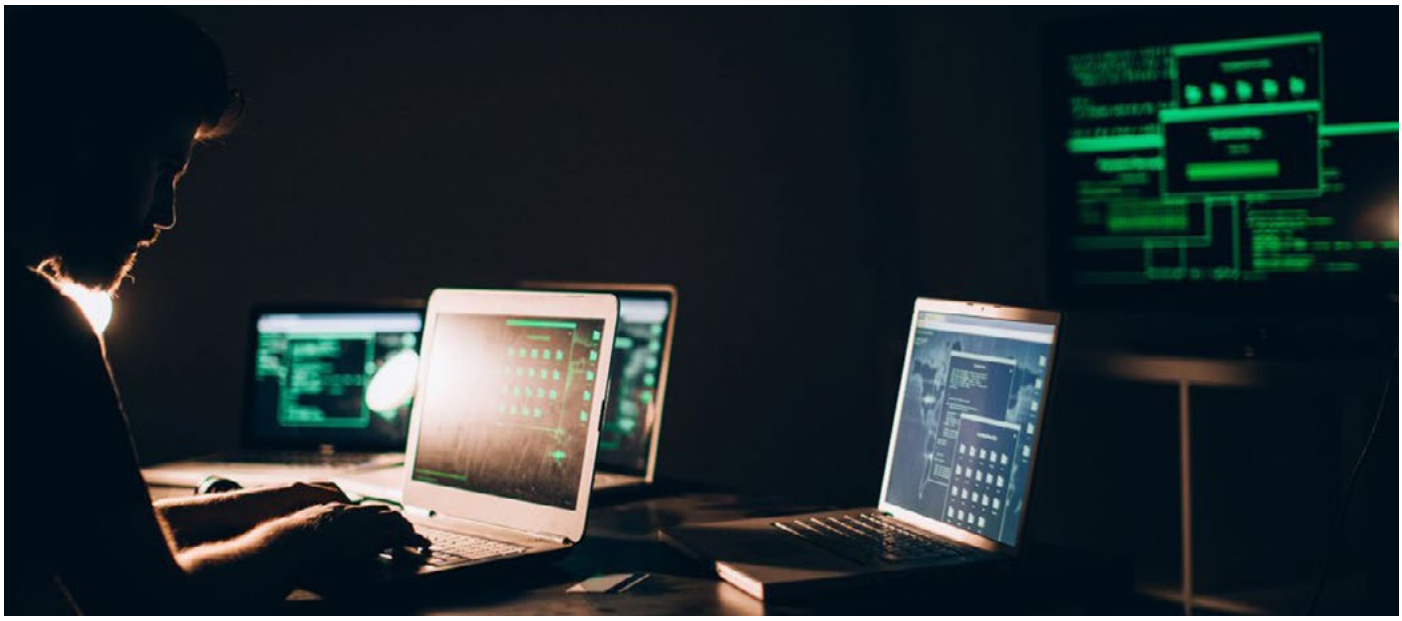
Pour les responsables de la sécurité des systèmes d'information, les enjeux sont désormais multiformes. Le capital humain étant au cœur de la sécurité, les télétravailleurs devront s'y impliquer. Quant à la mission des RSSI, elle consiste à assurer la disponibilité du réseau. Et pour que la continuité de service soit maintenue, la participation des utilisateurs compte. L'intégrité des données nécessite une pleine attention. Le respect des protocoles réseaux, mis en place dans les entreprises, doit être une préoccupation partagée.

Cela permet de garantir la confidentialité, qui prévient la divulgation des informations sensibles de l'entreprise. Il convient, à ce stade, d'insister sur l'utilisation des **VPN** mis à disposition par l'employeur.

Ces solutions de réseau privé virtuel sont une couche supplémentaire de sécurité. Dans une étude, Tessian. com indique que 91% des responsables informatiques font confiance aux télétravailleurs pour le respect des règles sécuritaires. Cependant, 41% de ces derniers ont affirmé ne pas faire attention aux consignes quand ils travaillent à distance. Pire, 51% des employés sondés estiment que les mesures de sécurité ont des impacts négatifs sur leur productivité ! En conséquence, ils n'hésitent pas à contourner ces mesures, au risque de faire voler en éclat tout le dispositif sécuritaire de l'entreprise.

La généralisation du télétravail a fait bondir la cybermenace sur les entreprises, en prenant de court les équipes techniques, qui étaient habituées à travailler en vase clos. Elles ont maintenant besoin de se faire comprendre de tous les employés qui exercent à distance. D'où la nécessité, pour les télétravailleurs, de maîtriser un tant soit peu le langage de la cybersécurité.

C'est la première et l'incontournable condition pour que tous soient impliqués dans la protection des infrastructures professionnelles des entreprises.



CYBERCRIMINALITÉ
Taire une cyberattaque, bonne ou mauvaise idée ?

Avant de signaler une cyberattaque à leurs collaborateurs et à leurs clients, les entreprises privilégient souvent le silence ou prennent du temps avant de communiquer sur le sujet. Les experts, interviewés par CIO Mag, en ont expliqué les raisons, qu'ils ne cautionnent pas. Et renseignent sur les meilleures attitudes à adopter.

Aurore Bonny

Un tabou ? Une honte ? Un aveu d'incapacité ? Dans quelles cases se range l'information de cyberattaque d'une entreprise victime ? *« Lorsqu'on est par exemple victime d'un cas de Ransomware, il est extrêmement tabou d'en parler sur la place publique, car cela renvoie l'image d'une entreprise qui a été incapable de protéger ses réseaux »*, explique Karim Ganame, Docteur burkinabè en cybersécurité. Les entreprises qui ne sont pas obligées, par une quelconque loi, de signaler leur situation de vulnérabilité, auront en effet plusieurs raisons de limiter leur communication. Leur crédibilité, leur réputation et leurs économies pèsent dans la balance. *« Les clients et les partenaires peuvent perdre confiance et causer un grand détriment à l'entreprise »*, déclare Karim Ganame.

Prenons par exemple le cas des banques. Lorsque le piratage informatique a eu pour effet de voler des informations sur les clients ou leur argent, la réputation de l'organisme bancaire est mise en mal. Et pour limiter les effets négatifs sur l'entreprise, il devient difficile - voire impossible – de communiquer. *« Un tel incident entraîne une perte d'activités et c'est exactement la raison pour laquelle les entreprises choisissent de ne pas divulguer des informations »*, affirme Ruphus Muita, consultant kenyan en sécurité de l'information. Pour Boubacar Bah, expert guinéen en cybersécurité, l'incapacité de certaines entreprises à signaler des incidents révèle aussi l'absence des systèmes de monitoring. Une situation surtout rencontrée en Afrique, où *« la plupart des entreprises africaines ont un problème de signalement »*. *« Le flux d'informations n'est pas contrôlé. Sans ces systèmes, on ne peut savoir ce qui se passe exactement. Il est difficile de percevoir l'intrusion et la façon dont elle a pénétré le système d'information. Les alertes d'antivirus, qui donnent des signalements, ne sont pas des références. Elles ne suffisent pas à assurer la sécurité globale. Il faut donc une politique de sécurité bien établie »*.

Toutes ces raisons sont-elles assez importantes pour justifier un silence ? Les clients et les partenaires des entreprises impactées n'ont-ils pas droit de savoir à quoi ils sont exposés ? Pour ces spécialistes, peu importe les enjeux, il faut informer pour prévenir et guérir. L'information sur les incidents doit être communiquée aux acteurs concernés de sorte à les inciter à prendre des mesures préventives. Et pour gagner du temps et limiter les dégâts, on évitera les solutions vouées à l'échec et on recourra à l'aide extérieure. *« C'est difficile à faire, mais une entreprise peut, dès le départ, être honnête avec ses partenaires et ses clients en leur expliquant clairement la problématique et ses conséquences, tout en communiquant sur la stratégie adoptée pour sortir de la crise »*, suggère Adeshina Adewumi, entrepreneur nigérian en e-commerce.

Solutions de sécurité

S'agissant de l'attitude à adopter, selon Ruphus Muita et Karim Ganame, la première étape consisterait surtout à identifier l'attaque et sa source, pour mieux contenir le problème. *« L'identification de la source peut être très difficile, mais il est important de le faire rapidement. Les cyberattaques peuvent durer plusieurs jours, voire plusieurs mois, sans être détectées »*, atteste Ruphus Muita. Quant à la seconde étape, elle concerne les pertes, qu'il convient de déterminer. Dans le secteur bancaire, il peut s'agir

d'argent ou d'informations sur les clients. L'étape suivante consiste à mettre en place des mesures, qui permettront de mettre un terme à l'attaque. A ce stade, les sources identifiées sont corrigées par des professionnels, ainsi que celles qui ont été identifiées au cours du processus.

Pour prévenir de futures attaques, il est également important d'engager un consultant. A charge pour lui d'auditer les systèmes et les mesures de cybersécurité mises en place. L'équipe d'audit, qui doit être composée de hackers éthiques, évaluera l'ensemble de l'environnement et testera la sécurité du réseau de la banque, ainsi que des systèmes utilisés. Cette équipe recommandera également des mesures à prendre et des solutions de sécurité à acquérir, afin d'être en capacité de surveiller la sécurité en temps réel et d'identifier les attaques avant qu'elles ne se produisent. Pour Karim Ganame, les cas de réponses aux incidents sont très complexes. Au début des attaques, les gens sont incrédules. Mais, au fil du temps, ils se rendent compte qu'ils sont vraiment attaqués et quand ils ne sont pas préparés, ils agissent comme ils le peuvent.

L'entreprise de cybersécurité de Karim Ganame intervient dans ce genre de situation. La technologie est branchée sur les réseaux des victimes pour détecter toutes les infections, lesquelles sont ensuite isolées. On explique ensuite au client comment les pirates sont parvenus à intégrer le réseau. Dans les cas où il n'y a pas eu sauvegarde des informations et que le logiciel pirate ransomware s'empare des données chiffrées, le client se retrouve parfois dans l'obligation de négocier la rançon avec les pirates. Et le montant peut être au-delà des possibilités de l'entreprise victime. *« La décision est difficile et je ne la privilégie pas, mais c'est souvent le choix qui s'impose. C'est parfois le seul moyen pour maintenir la compagnie sur le marché. Certaines ont dû mettre la clé sous la porte par manque de moyens. Pour éviter le pire, il faut se préparer d'avance ».*

Conformité des systèmes d'information

Cette affirmation soulève la problématique de l'absence de cybersécurité ou d'une préparation peu efficace et négligée. Karim Ganame a constaté qu'en Afrique, le travail des pirates est facilité par le manque de mises à jour des technologies achetées et installées. Il faudrait pourtant pouvoir déterminer les failles dont le pirate a profité pour s'introduire dans le réseau et savoir quelles vulnérabilités ont été exploitées. De concert avec les autres experts, il indique que *« sans ces informations, même une reconstruction de système après attaque n'est pas une garantie ».*

D'apres Boubacar Bah, la plupart des entreprises africaines ont également un problème de signalement. En l'absence de systèmes de monitoring déployés au sein de leurs infrastructures, le flux d'informations n'est pas contrôlé. Sans ces systèmes, il est impossible de savoir ce qui se passe exactement. Et il est difficile de savoir s'il y a eu une intrusion au sein du système d'information. Les alertes d'antivirus, qui donnent des signalements, ne sont pas des références. Elles ne suffisent pas à assurer la sécurité globale. Il faut donc une politique de sécurité bien établie.

Ces acteurs aguerris ont fourni d'autres recommandations, telles que des simulations de cyberattaques et des tests de réflexes de réactivité. *« Si c'est bien géré et que cela fait partie de la routine, il sera facile de détecter et de suivre tout problème »,* souligne Adeshina Adewumi. Les entreprises doivent aussi former en permanence les employés sur ce qu'est la cybersécurité et ses principes. Elles doivent s'assurer que leurs réseaux disposent de bons pare-feux et doivent maintenir les systèmes d'exploitation à jour, car certaines mises à jour de systèmes d'exploitation sont destinées à corriger les failles de sécurité.

Il importe également de choisir le bon antivirus pour l'entreprise et de le maintenir à jour, de bien sécuriser les points d'accès Wifi et d'utiliser une solution de contrôle du réseau pour empêcher les appareils malveillants ou inconnus de se connecter au réseau. Il est aussi nécessaire de séparer et de limiter correctement l'accès aux informations critiques en les réservant à des personnes spécifiques, d'adopter des mots de passe forts et de les changer régulièrement.

Concernant la préservation de la notoriété et de la confiance avec les partenaires et les clients, les entreprises doivent, en tout temps, s'assurer d'une communication efficace, afin de garantir leur crédibilité, même en temps de crise. *« Une gestion efficace de la crise évitera à l'organisation de perdre des clients et des partenaires, car la confiance ne sera pas rompue »,* confie l'expert kenyan. Pour Boubacar Bah, les Etats ont également un rôle important à jouer dans la protection des entreprises. Ils doivent notamment s'impliquer en mettant en place des structures, lesquelles vont accompagner les entreprises. Et fourniront des règles de bonne pratique et de conformité de leur système d'informations.

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
- atelier de prototypage numérique
- incubation technologique
- accélération de start-up à l'international

En 2021, les Orange Digital Centers seront présents au Sénégal, en Tunisie, en Jordanie, en Ethiopie, au Maroc, au Burkina Faso, en Côte d'Ivoire, en Sierra Leone, au Botswana, en République Démocratique du Congo, en République Centrafricaine, en Egypte, à Madagascar, en Guinée Conakry, en Guinée Bissau, au Mali, au Libéria et au Cameroun.

orange™

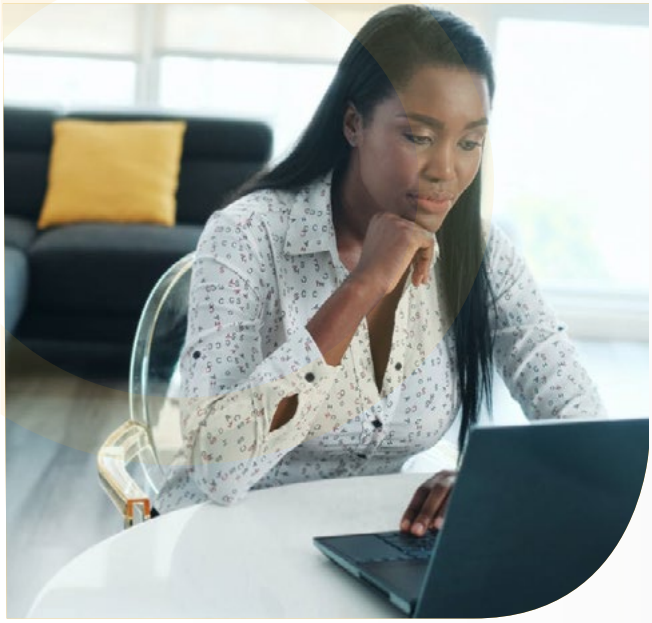
Vous rapprocher de l'essentiel

ASTUCES

Les bonnes pratiques à mettre en place pour télétravailler

Depuis mars 2020, certaines entreprises œuvrant en Afrique ont opté pour le télétravail afin de préserver leur personnel contre la pandémie du Coronavirus et pour se conformer aux mesures édictées par les autorités sanitaires. Ce nouveau mode de travail doit néanmoins faire face à des difficultés. A commencer par le manque de compétences, le problème d'accès à la connexion Internet et les faibles mesures de cybersécurité sur le continent. Tout ceci impacte l'élan de productivité des employés. Face à ces nombreux défis, quelles sont les bonnes pratiques à mettre en place pour un télétravail réussi ? Le point avec CIO Mag.

Enock Bulonza



D'après un sondage réalisé par le Club d'experts de la sécurité de l'information en Afrique (Cesia), entre le 1er et le 24 janvier 2021, dans 18 pays d'Afrique, 58 % des entreprises enquêtées n'ont pas été préparées à déployer un dispositif de travail à distance. Cette enquête révèle également que moins de 10 % des collaborateurs des entreprises africaines ont été en télétravail durant cette année de pandémie.

Plusieurs raisons expliquent cette faible proportion : le manque de sécurité informatique en dehors des locaux des entreprises, les délestages électriques, mais aussi la mauvaise connexion Internet.

En République démocratique du Congo (RDC), par exemple, 50% de la population n'a pas accès à une connexion et seuls 12 à 15% des habitants sont connectés régulièrement, d'après le ministère des Postes et télécommunications et des nouvelles technologies de l'information et de la communication (PTNTIC). Ces statistiques mettent en lumière les difficultés de la mise en place du télétravail dans un continent en voie de développement.

Selon plusieurs experts, le télétravail, qui s'effectue hors des locaux de l'employeur de façon régulière et volontaire, améliore l'organisation du travail et s'appuie sur les technologies numériques. Pour qu'il soit bénéfique à l'employé et à l'employeur, ce dispositif de travail à distance exclut toute improvisation et demande une certaine organisation. De la planification de son temps de travail à la prise de mesures de cybersécurité, voici quelques bonnes pratiques à mettre en place pour un télétravail réussi.

1 Séances de mise à niveau

Le télétravail s'est imposé pour certaines entreprises, alors même qu'elles n'étaient pas préparées à ce nouveau mode de travail. En Afrique, une pléthore d'employés éprouve encore d'énormes difficultés à s'adapter à cette organisation par manque de préparation et d'information. Pour maintenir l'équilibre de la productivité à l'heure du télétravail, il est important que les employeurs organisent des échanges, des séminaires ou des ateliers de mise à niveau sur ce nouveau mode de travail. Il s'agit d'expliquer aux employés l'usage des nouvelles

technologies et des outils collaboratifs, de sorte à favoriser l'interaction entre les membres de l'équipe.

2 Organiser son cadre de travail

Dans de nombreuses villes africaines, compte tenu de la précarité ou encore de l'exiguïté des maisons, il n'est pas facile de disposer d'un cadre de télétravail insonorisé. Pourtant, il est important de s'installer dans un environnement calme, avec accès à l'électricité, à la connexion Internet, à l'eau potable et de disposer d'un siège et de mobilier. L'idéal, pour les télétravailleurs, serait d'organiser un bon cadre de travail, de sorte à améliorer la concentration et la productivité.

3 Planifier son temps de travail

Les observateurs, qui soutiennent qu'un télétravail réussi commence par la planification de son temps de travail, sont nombreux. Pour certains, l'essentiel pour un télétravailleur serait de considérer son domicile comme son lieu de travail et pas seulement comme un lieu de détente. C'est un élément essentiel dans l'identification des axes prioritaires de son travail. L'employé peut ainsi conserver ses automatismes, notamment en termes d'horaires. Et inclure l'heure du début de travail, la pause, la pause-déjeuner et la participation aux réunions en ligne.

Cette planification du temps de travail permet à l'employé de conserver un équilibre entre sa vie personnelle et professionnelle.

4 Les mesures pour la cybersécurité

Dans un monde en plein mutation, le télétravail n'est pas épargné par l'activisme des hackers. Les cybermenaces ont augmenté de manière exponentielle avec la pandémie de Coronavirus. En 2020, plusieurs entreprises œuvrant en Afrique ont reconnu avoir été victimes des menaces de cybersécurité. Selon le Cesia, 69% des attaques concernaient le phishing, 29% l'ingénierie sociale et 44% les tentatives de connexion Internet.

Dans la sphère du télétravail, les mesures pour la cybersécurité impliquent des dispositions de protection des données, sensibles ou non. Elles sont prises par l'employeur et l'employé pendant ses heures de travail. Et s'effectuent au sein d'une infrastructure numérique. Ces dispositions renferment des techniques de protection, dont la mise à jour régulière des logiciels utilisés. La sécurisation des appareils et des objets connectés est également requise, ainsi que l'enregistrement continu des données dans un support hors-ligne. Le changement régulier de mot de passe est également conseillé. Il doit combiner les chiffres, les lettres et les symboles. Ces simples mesures de prudence permettent déjà de travailler à l'abri des éventuelles attaques.

TÉMOIGNAGES

Les secrets des DSI pour travailler en toute sécurité depuis son domicile

Vigilance, prévision, authentification, chiffrement… Comment sécuriser son poste de travail lorsqu'on travaille depuis son domicile ? CIO Mag vous livre les astuces des DSI pour protéger les données de l'entreprise face à la recrudescence des attaques en ligne.

Anselme Akeko

Ayi Mawuena d'Almeida, directeur du-département des Technologies de l'information, de la sécurité et de l'organisation à la Banque ouest-africaine de développement (BOAD)

« Redoubler de vigilance par rapport aux risques cyber »

L'apparition de la pandémie de la Covid-19 a d'importantes répercussions sur les plans humain, économique et concernant la sécurité informatique. Nous nous sommes adaptés, en privilégiant, autant que faire se peut, le travail à distance, tout en garantissant un maximum de sécurité face à la montée en puissance des cyberattaques. Très rapidement, chaque collaborateur a pu bénéficier d'une connexion entièrement sécurisée. La sécurité est un point clef.

Le télétravail est, par définition, une activité « hors les murs ». Il impose de gérer la sécurisation des flux, de contrôler les flottes d'appareils et, bien-sûr, de sensibiliser les équipes.

Les collaborateurs doivent redoubler de vigilance vis-à-vis de tous les types de risques cyber. Ces derniers ont vocation à compromettre des informations personnelles et d'autres, qui appartiennent à l'entreprise. L'utilisation de VPN, la connectivité persistante, la téléphonie sécurisée, l'authentification forte... sont autant d'activités qui ont pris de l'ampleur. L'anticipation, l'adaptabilité et l'agilité sont les principaux atouts pour réussir ce nouveau challenge. Et les DSI l'ont démontré en optimisant les environnements à distance et en veillant à ce que les collaborateurs disposent de la bonne technologie pour travailler dans des conditions optimales.

Lisette Ebonzo, DSI au ministère de la Fonction publique, de la réforme de l'Etat, du travail et de la sécurité sociale (République du Congo)

« Authentifier systématiquement les accès »

Les bonnes pratiques à mettre en œuvre pour travailler en toute sécurité depuis son domicile :

1-Favorisez l'usage d'équipements fournis et contrôlés par l'entreprise/l'administration ;

2 - S'équiper d'un ordinateur avec des logiciels, des antivirus et antimalwares, des pare-feux et d'autres systèmes de sécurité informatiques ;

3- S'assurer de la sécurité réseau domestique par :

- la protection du routeur via un mot de passe ;
- l'installation d'un réseau privé virtuel (VPN) sur le routeur ;
- la filtration des adresses MAC ;
- la désactivation des transmissions Wifi.

4- Utiliser un compte séparé pour le travail avec des outils de cybersécurité en fonction de l'entreprise/l'administration.

5- Crypter les données et gérer les habilitations ;

6- Ne pas télécharger et ne pas cliquer avant d'avoir vérifié que l'expéditeur est légitime ;

7- Mettre en place les outils de collaboration en s'assurant des nouvelles politiques de cybersécurité ;

8- Authentifier systématiquement les accès à distance ;

9- Limiter les communications et les transferts des fichiers ;

10- Séparer les activités personnelles des flux professionnels ;

11- Mettre à jour régulièrement les paramètres de sécurité ;

12- Mettre en place une charte de sécurité.

Yao Charles, DSI du District autonome de Yamoussoukro (Côte d'Ivoire)

« Chiffrer les données »

Depuis 2016, le District autonome de Yamoussoukro a introduit le télétravail dans sa politique managériale. Dans un contexte marqué par la crise sanitaire, le développement du télétravail a entrainé une hausse de la malveillance informatique sur les systèmes d'information. Ce qui a eu pour conséquence : l'inaccessibilité des sites Internet, le vol de données sensibles, les demandes de rançon à l'aide de logiciel piégé, le piratage de comptes, etc.

Dans le souci de limiter les risques d'une cyberattaque, il est souhaitable de :

- Installer un antivirus et un pare-feu ;
- Utiliser un compte personnel avec des droits limités ;
- Procéder à la mise à jour régulière du système d'exploitation et des logiciels utilisés ;
- Utiliser des mots de passe forts ;
- Activer l'option de chiffrement WPA2 ou WPA3 du Wifi du domicile et désactiver la fonction WPS, ainsi que le Wifi invité ;
- Privilégier l'échange de données sensibles à travers les stockages disponibles depuis un VPN, mis à disposition par la collectivité ;
- Eviter toute transmission de données confidentielles via la messagerie (boîte mail) ; des services grand public de stockage (type OneDrive), des services grand public de partage de fichiers (type WeTransfer) *(phrase à reformuler, on ne comprend pas s'il faut ou non éviter toute transmission des services grand public…).* A défaut, chiffrer les données avant de les transmettre et transférer les clés de chiffrement via un canal de communication distinct.

El Hadj Mody Seck, chef du Centre d'information, de communication et des TIC (CIC-TIC), Haut-commissariat de l'Organisation pour la mise en valeur du fleuve Sénégal (OMVS)

« Un challenge qui demande beaucoup de précautions »

Pour travailler en toute sécurité depuis son domicile, il faut que les prérequis techniques et de protection des données soient réunis, et disposer d'une bonne infrastructure (connexion Internet). C'est essentiel pour la réussite de cette mission. L'autre aspect à ne pas négliger est la sécurité des données, car depuis son point de connexion, les données d'entreprise peuvent être manipulées. Il est important de prendre en compte ces paramètres pour éviter une deuxième pandémie : la pandémie informatique pour son entreprise.

En dehors du télétravail à son domicile, le DSI est également, par moment, en mode hybride, avec le travail en visioconférence depuis son bureau ou avec des collègues au bureau, ainsi qu'avec d'autres interlocuteurs, à domicile, loin du lieu de travail. D'autres flux et d'autres sources d'attaques sont à craindre. Le DSI fait face à la gestion du contenant et du contenu, ce qui constitue un véritable défi. A charge pour lui d'être en capacité d'assurer une continuité de service, de sécurité et de sauvegarde des données pour tout l'écosystème. Si le challenge est intéressant, il requiert néanmoins la prise en compte d'un grand nombre de précautions.

Retour d'expérience

Hatem Trigui, Directeur central des Systèmes d'information - Caisse des Dépôts et Consignations (Tunisie)

« La CDC Tunisie a anticipé le risque »

La CDC a entrepris un certain nombre d'actions, au cours de l'année 2019. Parmi elles : la migration vers Office 365, l'installation des firewalls de qualité, la réalisation d'une mission d'audit de la sécurité du SI, la désignation d'un RSSI, la constitution du Comité de Sécurité du SI, l'élaboration de la charte de bon usage des ressources informatiques et sa signature par tout le personnel, la dotation de tous les utilisateurs d'un laptop performant et sécurisé.

Ajoutons à cela les choix stratégiques, adoptés dès la création de la caisse (2012), à savoir : la construction d'un mini-Datacenter, très respectable, avec des équipements virtualisés, ainsi que la mise en œuvre d'un Système d'information intégré, de renommée.

Toutes ces actions ont permis à la CDC d'être au rendez-vous, un certain 17 mars 2020 (NDLR : date du 1er confinement), pour basculer à quasi 100% en mode télétravail. En effet, seul le responsable du Bureau d'ordre central (BOC) a été contraint de passer sur son lieu de travail, tous les jeudis, pour scanner le courrier reçu, en format papier et le transférer aux concernés, en format numérique. Il arrive également aux premiers responsables de se rendre au bureau pour signer des documents officiels.

En seulement quelques jours, le personnel de la Caisse s'est adapté à ce nouveau mode de travail, ce qui est le signe d'une capacité exceptionnelle dans la gestion de changement. On a découvert qu'il était possible de travailler sans imprimante et sans fax, qu'on pouvait se réunir, discuter et prendre les décisions sans pour autant se réunir physiquement (Teams, presque jamais utilisé depuis sa mise en place en mai 2019, est subitement devenu l'outil de travail en groupe par excellence).

Et, cerise sur le gâteau, tout le personnel a été doté, à la fin du mois d'avril 2020, d'un Smartphone professionnel, avec un forfait Internet pour pouvoir travailler confortablement depuis son domicile.

Ce changement de modèle n'aurait pu être aussi fluide et transparent sans l'engagement de l'équipe DSI, qui s'est mobilisée pour se mettre à la disposition de tous les utilisateurs, 24h/24, 7j/7.

Du côté de la sécurité, la mission d'audit est arrivée à point nommé. Des actions quick wins ont été mises en œuvre par anticipation. Les accès au SI se sont faits à travers des VPN sécurisés (double authentification, mots de passe dynamiques récupérés par sms...) et pendant des durées limitées.

Par l'occasion, de nouveaux articles ont été rajoutés à la charte de bon usage des ressources informatiques, tels que : l'utilisation exclusive des équipements de la Caisse à des fins professionnels, l'interdiction de l'utilisation des Wifi publics ou des équipements personnels pour le travail à distance, une attention particulière aux tentatives d'attaques en mode télétravail... Et force est de constater que nous n'avons pas enregistré d'incidents particuliers, en matière de cybersécurité, pendant les périodes de confinement.

Par ailleurs, dans ces conditions inhabituelles, et dans l'objectif de garantir une productivité acceptable, nous avons mis en place un mécanisme de suivi des activités. Tout le personnel a été invité à partager, à la fin de chaque semaine, son plan d'action, ainsi que l'avancement de ses travaux. A la grande surprise, le suivi régulier du Plan de continuité des activités (PCA) par le Comité exécutif (COMEX) a démontré que la productivité était meilleure qu'en temps normal.

Pour conclure, malgré le fait que la Covid-19 ait pu affecter un certain nombre de collègues (heureusement sans beaucoup de douleurs), le personnel de la CDC a vécu, pendant une année, une expérience inédite. Cette situation a donné aux TIC et aux spécialistes IT la valeur qu'ils méritent. Et cette dynamique, générée à cause/grâce à la pandémie, est devenue un réflexe, qui a persisté au retour en mode présentiel. D'ailleurs, ce nouvel état d'esprit a été l'un des facteurs de réussite du projet de mise en place de la de la gestion électronique des courriers, lequel inclut le parapheur électronique, déployé lors du dernier trimestre 2020.

ADMINISTRATIONS
Les pays africains à l'épreuve de la résilience

L'Afrique n'a pas courbé l'échine face à la révolution numérique et à la résilience nécessaires pour riposter à la pandémie de Covid-19. Entre improvisation, adaptation et maintien de la tendance de transformation, enquête sur la stratégie des Etats à assurer la cybersécurité des entreprises et des administrations contraintes au télétravail.

Michaël Tchokpodo

Aux premières heures de la pandémie liée à la Covid-19, le Bénin a adopté le télétravail. Les effectifs des administrations ont été réduits. Cette forme de travail à distance a duré plusieurs semaines. Déjà, avant la crise, les personnels administratifs avaient été formés à l'utilisation des outils informatiques. Et un pack informatique était disponible, de même que l'accès à la connexion internet. Cette tendance s'est poursuivie dès le déclenchement de la pandémie.

Le 26 mars 2020, le Bénin a créé le portail national des services publics. Il centralise les services administratifs tels que la demande de certificat de nationalité, le casier judiciaire… Les citoyens ont la possibilité d'accéder aux informations de plus de 560 services publics en ligne. Ils peuvent effectuer des demandes d'e-services et les obtenir depuis leur téléphone ou leur ordinateur, sans aller à l'administration publique. Selon la Conférence des Nations unies sur le commerce et le

développement (CNUCED), le Bénin est, avec l'Estonie, le pays le plus rapide au monde en matière de création d'entreprise via un téléphone portable.

Lors de la clôture de la 9ème édition des Assises de la Transformation digitale en Afrique (ATDA) 2020, Dr. Hamadoun Touré, ministre malien de la Communication et de l'Economie numérique, a déclaré que le numérique offre l'opportunité au pays de mettre fin à son enclavement et qu'il joue un rôle central dans la région. *« Au vu du développement de liaisons par fibre optique à travers les différents pays voisins et du travail de régulation et de réglementation, nous ne pouvons qu'être optimistes. La floraison de nos talents locaux, qui démontrent un énorme potentiel d'innovation, agit dans le même sens. Et nous mettons tout en œuvre pour promouvoir un environnement technologique propice au développement de notre société, ainsi qu'au rayonnement des innovations de nos jeunes aussi bien en Afrique qu'à l'international. »*

Ecosystème prospectif

Tout comme le Bénin, le Sénégal a dématérialisé une centaine de procédures administratives pour faciliter la vie aux usagers. Parmi elles, le permis de construire, l'obtention du diplôme du baccalauréat, les procédures liées à l'urbanisme, etc. Depuis 2012, le pays a déployé 5 000 km d'infrastructures fibre optique, dans 45 départements. Il envisage la construction d'un troisième Datacenter, de type TIER III, qui s'ajoutera aux deux autres équipements d'ores et déjà fonctionnels.

Aux Comores, après une décennie d'investissement dans les infrastructures et les réformes numériques, ce n'est qu'en octobre 2018 qu'une feuille de route a été élaborée pour impulser la transformation numérique du pays. En janvier 2019, l'Agence nationale de développement du numérique (ANADEN) a été créée. Quelque 10 millions de dollars ont été mobilisés pour financer les premiers projets et les réformes numériques. Malgré cette orientation tardive, un cadre règlementaire a pu être mis en place. La dématérialisation des procédures, dont la passation des marchés publics, s'est effectuée par la suite. Et la création et la gestion d'entreprises en ligne est annoncée pour 2021.

Au cours de cette décennie, la transformation digitale sera au cœur des politiques publiques en Afrique.

« L'arrivée de la Covid-19 nous a permis de mesurer la pertinence de ces choix politiques et l'efficacité de la dynamique de transformation engagée. C'est ce qui nous a permis de moins souffrir pendant cette pandémie et d'enregistrer des avancées significatives », constate Chamsoudini Mzaouiyani, Directeur général de l'Agence nationale de développement numérique (ANADEN).

En règle générale, les populations et l'administration ont souffert de la Covid-19. C'est ce qui explique le basculement vers le télétravail. Aux Comores, où l'écosystème numérique se met progressivement en place, cela a constitué un véritable défi. En revanche, le Sénégal a poussé un ouf de soulagement, car il avait développé des plateformes et sensibilisé les administrations à leur utilisation pour optimiser le travail. Cheikh Bakhoum, Directeur général de l'Agence de l'informatique de l'Etat (ADIE), ajoute qu'avant la pandémie, les gens n'adhéraient pourtant pas systématiquement à cette initiative.

Télétravail et e-services

La pandémie de la Covid-19 a donc contraint les administrations sénégalaises à adopter le télétravail et des e-services, tels que la messagerie administrative, la plateforme de dématérialisation du courrier dans les administrations, celle de gestion de projet, etc. La crise a conforté le Sénégal dans sa dynamique de transformation numérique. Et les Etats africains moins avancés dans ce domaine se sont mis à jour. *« Nous nous activons dans la perspective d'une troisième vague ou d'une autre catastrophe, de sorte que le télétravail soit une réalité pour l'administration publique. La fracture numérique, que l'on peut constater, est en train d'être résorbée à travers le programme que nous portons au niveau de l'ANADEN, avec l'appui de partenaires »,* assure Chamsoudini Mzaouiyani.

Le télétravail est une activité professionnelle effectuée, tout ou partie, à distance du lieu de travail. Il a généralement lieu à domicile et nécessite l'utilisation d'un outil informatique et d'une connexion internet pour rendre des travaux, participer à des réunions d'équipe et suivre des webinaires. Bien que très pratique, cette méthode de travail engendre des failles de sécurité, qui exposent à des attaques informatiques. En son temps, l'Agence nationale de la sécurité des systèmes d'information (ANSSI Bénin) avait élaboré un guide du télétravailleur pour éviter les risques d'attaque. Elle leur conseillait de renforcer la sécurité du réseau domestique. Au nombre des préconisations : *« Changer le mot de passe du Wifi par un mot de passe complexe, en privilégiant le chiffrement WPA2. Eviter de nommer le réseau Wifi en son nom propre. Privilégier une connexion dédiée (boîtier 4G, autre SSID, etc.) à son usage personnel et qui soit différente du Wifi utilisé pour l'usage domestique ».*

Souveraineté numérique

Si des attaques informatiques sont perpétrées dans le monde entier, la cybercriminalité sévit tout autant dans le cyberespace africain. *« Au-delà de la Covid-19, les attaques constituent notre quotidien. Mais, notre objectif est de protéger nos infrastructures, nos équipements et nos plateformes. Nous disposons pour cela d'équipes dédiées. Elles supervisent toutes nos installations. Et chaque fois que nous subissons des attaques, nous faisons face pour que notre système puisse résister »,* réagit l'ADIE.

Aux Comores, le diagnostic des risques d'attaques informatiques a facilité l'élaboration d'une stratégie nationale de cybersécurité. A l'instar du Bénin et du Sénégal, le pays a construit son Computer Incident Response Teams (CIRT) national, avec une équipe de réponse, de défense et d'anticipation des attaques cyber. Il s'est également doté d'une structure chargée de la protection des données personnelles et de la relation avec les citoyens. En résumé, si les risques cyber n'ont pas été un frein à la généralisation du télétravail, l'ambition de ces Etats africains est de poursuivre la dynamique de transformation numérique.

Tous les chantiers envisagés ont pour finalité de parvenir à la souveraineté numérique. A commencer par la construction de Datacenter, la mise en œuvre effective de la Télévision numérique terrestre, l'interconnexion à travers la fibre optique, l'Intelligence artificielle, la big data… Et l'épineux problème du financement. De toute évidence, les Etats africains ne disposent pas encore de données chiffrées pour évaluer l'économie générée par l'adoption du télétravail. Mais, ils reconnaissent à l'unanimité que les nouvelles méthodes de travail ont réduit les déplacements, aussi bien à l'interne qu'à l'extérieur des pays.

INTERNATIONAL

Les multinationales adaptent leurs outils pour se protéger contre les risques cyber

Elles ont des milliers d'employés répartis sur plusieurs pays, voire sur plusieurs continents : les entreprises multinationales. Avec la crise de la Covid-19, elles aussi ont été forcées de se réorganiser. Habituées au travail multi-sites, ces sociétés étaient tout de même déjà bien préparées au passage massif vers le télétravail. Alors, quels outils ont été utilisés par les entreprises Orange, Atos ou Huawei pour garantir la sécurité informatique de leurs données et celles de leurs clients ? Comment organisent-elles le télétravail pour répondre aux impératifs cybersécuritaires ? Et quelles sont leurs observations et leurs recommandations autour de la cybersécurité sur le continent ? Le point avec CIO Mag.

Zakaria Gallouch et Camille Dubruelh

Les grands groupes, qui ont été sollicités dans le cadre de ce dossier, se caractérisent par la taille de leur expansion, la rigueur de leurs modèles managériaux et leur maturité technologique. Globalement, ils ont négocié leur passage au télétravail avec aisance. Cette réalité vaut pour les organisations multinationales, qui adoptent des canaux de collaboration à distance sûrs et efficients.

« Chez Huawei, ce switch n'a pas vraiment été un gros changement car nous avions l'habitude de ce genre de scénario. Nous travaillons selon un schéma multi-sites et nos ingénieurs interviennent à distance. Depuis longtemps nous développons nos propres outils pour travailler à distance », atteste Adnane Ben Halima, Vice-Président en charge des relations publiques pour la région Méditerranée de Huawei Northern Africa.

L'impact de la crise sanitaire n'a pas été insurmontable pour ces organisations. Elles disposent des outils collaboratifs dédiées et de collaborateurs formés. Ils optimisent leur utilisation tant pour la performance et la qualité des prestations, que pour la sécurité des données.

Baïdy Si, chef des services de cybersécurité en Afrique francophone chez Atos, rapporte qu'en moins d'une semaine, 96% des 105 000 collaborateurs étaient en télétravail.

« Le Groupe a assuré des livraisons d'ordinateurs ou de modems quand il était nécessaire. En moins de 48 heures et grâce à une mobilisation incroyable, plus de 12 500 ordinateurs fixes ont été transférés du bureau au domicile de nos collègues. »

La cyberprotection interne assurée

Il en a été de même pour les processus de cybersécurité. Ils sont passés au premier plan avec l'adoption massive du télétravail. En matière de protection de données personnelles, les grandes structures disposaient déjà de politiques, de procédures et de processus. Et l'effet de la crise sur la gestion des données a été atténué.

« Notre politique de sécurité Groupe étant très mature, nos systèmes informatiques et nos process sécurité étaient déjà en place lorsque la pandémie s'est déclarée. Le niveau de sécurité n'a ainsi pas été impacté et les salariés ont pu télétravailler sans encombre », souligne Emmanuel Cheriet, Directeur Maghreb et Afrique de l'Ouest chez Orange Cyberdéfense.

Le groupe Atos, qui dispose d'un dispositif de protection des données personnelles, a agi pareillement. Les employés ont rigoureusement classifié, traité et stocké les données sensibles.

« Toutes les données sont chiffrées et protégées par une authentification à deux facteurs, ce qui permet de limiter l'accès à une liste de personnes préalablement définie », précise Baïdy Si. Il ajoute que la communication interne permet d'instaurer une prise de conscience collective des gestes à adopter.

« Tous nos employés, sans exception, suivent des formations obligatoires. Elles les sensibilisent aux risques et les éduquent sur les bonnes pratiques à adopter. »

Ce rappel est crucial. Il consiste à prévenir les risques inhérents aux usages des collaborateurs. La vigilance est permanente, même avec des dispositifs de sécurité matures et bien rodés.

« Avant de procéder à des interventions sur les réseaux des clients, un ensemble de règles doit absolument être respecté pour garantir la sécurité des opérations. Chaque intervention peut en effet produire une catastrophe », prévient Adnane Ben Halima.

Chez Orange, l'ensemble des employés du groupe est formé en continu à une charte des bonnes pratiques. Emmanuel Cheriet s'en explique. *« En interne, nous avons communiqué sur les règles « d'hygiène informatique » auprès de nos équipes. Nous les avons informés sur les attaques majeures afin de les sensibiliser sur les risques accrus engendrés par la situation, durant toute cette période. »*

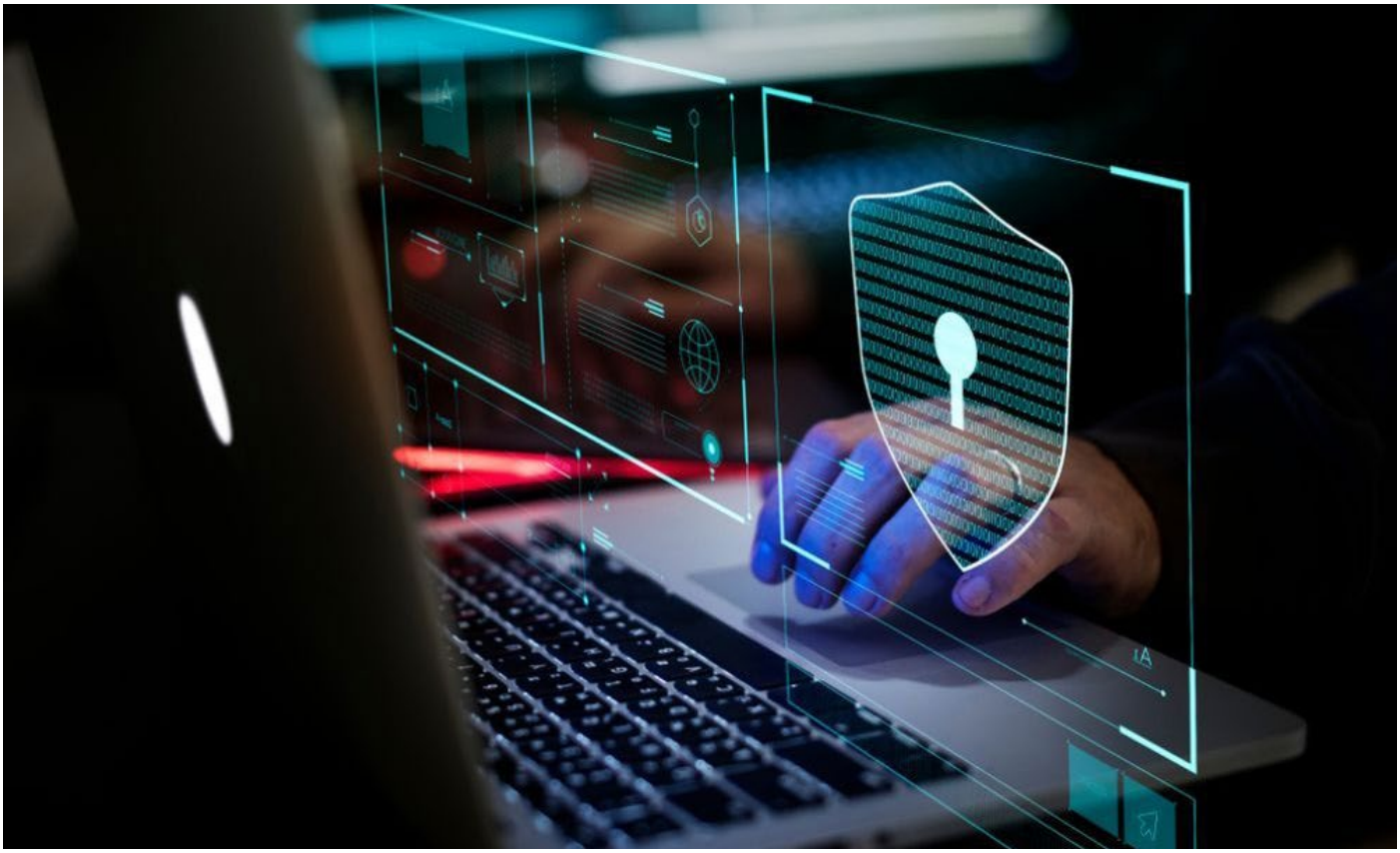
Sécuriser le passage au télétravail

Les entreprises, dont les politiques de protection et les modes d'usage des équipements matériels et logiciels présentaient des carences, ont subi des défaillances au plan de la cybersécurité.

Les grands groupes ont été sollicités pour intervenir sur les dispositifs de sécurité des entreprises clientes. Le télétravail a en effet augmenté les risques de cybersécurité, notamment l'hameçonnage (phishing, smishing), les rançongiciels ou l'exploitation des vulnérabilités des systèmes et réseaux. Il a fallu une réactivité particulière pour mettre à niveau les différentes organisations, sur le plan de la cybersécurité.

« Chez nos clients, en Afrique francophone, le principal défi a consisté à sécuriser le passage au télétravail », fait remarquer Baïdy Si. Il a également fallu présenter, à la clientèle, le protocole d'accompagnement déployé par le groupe.

« Dans un premier temps, nous avons déployé une offre d'audit flash, pour que nos clients aient une visibilité à 360° sur leur niveau d'exposition aux risques cybers. Par la suite, nous les avons accompagnés dans la correction des vulnérabilités détectées, pour qu'ils gagnent en assurance face à ces risques et pour leur permettre de télétravailler sereinement. » L'objectif principal de cet accompagnement intensif consiste à accélérer les processus de digitalisation des clients et à les installer sur une plateforme



technico-organisationnelle, qui puisse à la fois fluidifier et sécuriser le travail à distance.

« Durant cette période, nous nous sommes avant tout investis pour aider nos clients à se sécuriser. Et pour les protéger au moment où leur transformation numérique s'accélérait, avec la mise en place de solutions pour sécuriser le travail à distance (exemple : solution VPN, Authentification Multi-facteurs, etc.) », précise Emmanuel Cheriet d'Orange Cyberdéfense.

Des techniques de protection de nouvelle génération voient le jour. L'intelligence artificielle est intégrée dans les protocoles de défense. Ces techniques permettent de détecter et de répondre, en temps réel, aux menaces d'intrusion. La cybercriminalité évolue en effet de manière accélérée et les hackers sont mieux formés. Ils utilisent la force de l'Intelligence artificielle pour mener des attaques plus efficaces et plus dangereuses pour les organisations.

Harmoniser les pratiques sur le continent

La crise a été un accélérateur dans l'adoption du télétravail. Les entreprises, même les plus récalcitrantes, ont dû s'équiper d'outils adaptés pour assurer la continuité de leur activité.

« La crise a permis de lever les freins culturels qui entravaient le passage au travail à distance. Et il a été prouvé que le télétravail ne nuisait pas à la productivité », constate Baïdy Si.

« Pour autant, l'usage exclusif du travail en distanciel a ses limites. Les travailleurs souhaitent plus de flexibilité et une proportion télétravail/présentiel sur site plus équilibrée. »

La pandémie a également influencé les cultures d'entreprises. D'importants changements ont opéré tant dans les rapports sociaux qu'au niveau des usages. A charge pour les organisations de créer un cadre propice à l'épanouissement des collaborateurs, à visibiliser la cybersécurité à chaque niveau de l'organisation et à maintenir la performance collective et individuelle.

Le travail à distance requiert une bande passante respectable et une connexion stable. Et sur ce point, les pays d'Afrique n'avancent pas à la même vitesse. La qualité des réseaux sur le continent n'est pas homogène.

« Au début de la crise, les réseaux étaient submergés et saturés. Avec les opérateurs, nous avons réagi très

rapidement pour faire face à cette montée en puissance de l'utilisation Data », témoigne Adnane Ben Halima. Il constate qu'en Afrique, l'offre en connectivité mobile a pris le dessus sur les connexions fixes, en dépit du fait qu'elles soient indispensables pour les téléservices assez lourds, comme l'éducation ou la santé.

La raison ? Les coûts élevés des investissements et des amortissements technologiques trop faibles. Les solutions pérennes et la stabilité des infrastructures technologiques de pointe reposent principalement sur la volonté politique.

« Sur le continent africain, les pays évoluent différemment. L'usage des Tics n'est pas le même d'une région à l'autre. Mais, nous savons que le changement dans cette région du monde peut se faire très rapidement et que les secteurs clés pourront rapidement être liés aux TICs », ajoute le Vice-Président en charge des relations publiques pour la région Méditerranée de Huawei Northern Africa.

Quant à la réglementation, elle s'organise. Elle est de plus en plus exigeante, notamment pour les acteurs économiques et institutionnels dont la stratégie intervient dans le fonctionnement des différents Etats. Il en est de même pour les filiales de grands groupes internationaux, qui pilotent l'exposition aux risques cyber de leurs filiales et de leurs partenaires sur le continent. Il leur est imposé un certain nombre de règles, de processus et de mises en conformité.

En matière de compétences, les ressources qualifiées sont largement siphonnées par les besoins européens, eux-mêmes sous tension. Le marché de la cybersécurité sur le continent est principalement porté par le secteur financier, lequel a opéré sa digitalisation depuis quelques années. C'est une opportunité pour l'Afrique et l'occasion de développer un vivier de compétences qualifiées, au service de sa cybersécurité et plus généralement pour sa souveraineté numérique.

Avec la crise sanitaire, les entreprises ont pris conscience de l'importance du renforcement de leur résilience face à l'évolution des risques. Cela nécessite de revoir l'organisation, l'infrastructure et les processus de continuité des activités pour les rendre plus solides.

Cette prise de conscience a également été perceptible au niveau des directions générales. Elles ont vu que la transformation des services, qui était engagée depuis quelques années avec le numérique, s'était accélérée pendant la crise de la Covid-19. Mais, de nouveaux risques numériques sont apparus. Ils sont de plus en plus structurés, de plus en plus dangereux pour les organisations et plus agiles face aux systèmes de cyberdéfenses, notamment avec l'entrée de l'Intelligence artificielle dans les boites à outils des cybercriminels.

Publireportage

ENTREPRISES

Deux géants de la cybersécurité mondiale pour deux stratégies complémentaires

Spécialiste mondial des infrastructures numériques de confiance, Exclusive Networks s'appuie sur des fournisseurs leader du marché, à l'instar de Palo Alto Networks, leader mondial de la cybersécurité. Elle propose des technologies pour protéger la vie numérique des personnes, des entreprises et des Etats. Louis-Joseph Sidibé, Directeur de la région Afrique de l'Ouest et centrale et Ercan Aydin, Vice-président Afrique & Moyen-Orient de Palo Alto Networks, nous apportent plus de détails.

Louis-Joseph Sidibé
Directeur de la région Afrique de l'Ouest et centrale chez Exclusive Networks

Ercan Aydin
Vice-président Afrique & Moyen-Orient de Palo Alto Networks

CIO Mag : Le basculement vers le télétravail, dû à la Covid-19, a fait augmenter les risques de cybercriminalité. Quel est l'ampleur des menaces sur les cyberespaces et sur les infrastructures numériques en Afrique ?

Louis-Joseph Sidibé : Le télétravail permet l'accès aux ressources critiques d'une entreprise en travaillant à distance. Dès que cela est possible, la manière de sécuriser la structure concernée devient différente. A cause du télétravail, beaucoup d'entreprises utilisent des outils tels que Zoom, Teams... avec des failles de sécurité ou des logiciels craqués par des hackers. Exclusive Networks propose des solutions qui renforcent la connectivité en authentifiant l'utilisateur, à l'instar de la solution Prisma de Palo Alto Networks,

INTERVIEW

Louis-Joseph Sidibé

Directeur de la région Afrique de l'Ouest et centrale chez Exclusive Networks

leader en matière de cybersécurité en mode télétravail.

Ercan Aydin : Pendant la crise de la Covid-19, les entreprises ont dû adapter leurs routines à la nouvelle réalité et les hackers aussi. Le seul moyen de sécuriser la main-d'œuvre à distance est d'amener les employés à se connecter à partir de leurs ordinateurs portables, via une connexion VPN sécurisée. C'est la méthode sécurisée et privée pour entrer virtuellement dans le réseau du siège de l'entreprise.

Palo Alto Networks offre des solutions pour sécuriser une main-d'œuvre distante via Prisma Access et GlobalProtect.

La sécurité réseau GlobalProtect ™ pour les terminaux est la solution VPN intégrée sur site. Chaque pare-feu de nouvelle génération de Palo Alto Networks est conçu pour prendre en charge un accès sécurisé et permanent avec GlobalProtect, à mesure que la main-d'œuvre mobile se développe. Prisma Access est l'option idéale lorsque vous avez besoin de faire évoluer rapidement votre main-d'œuvre distante.

Peut-on évaluer les pertes enregistrées ?

LJ.S : L'industrie de la cybercriminalité utilise des attaques inconnues et difficiles à identifier. Ainsi, les dégâts causés sont énormes parce qu'il y a des entreprises qui n'ont pas mis à jour leurs techniques de défense. Palo Alto propose une riposte, qui évalue les pertes économiques - ou celles liées à l'image - par rapport à chaque secteur d'activité et en fonction du type de cyberattaques.

E.A : Le coût d'une cyberattaque peut être examiné sous deux angles. Premièrement, le coût initial d'une cyberattaque : les hackers prennent des informations sensibles et demandent une somme d'argent spécifique.

Le deuxième coût, moins tangible et plus désastreux, est lié à l'image d'une entreprise. Si une banque voit ses données divulguées et que des hackers ont accès aux informations sensibles des clients, la réputation de la banque sera fortement dégradée. Si cette confiance est rompue, cela coûtera beaucoup plus que le coût réel du paiement des hackers. Et cela s'applique à tout autre secteur qui détient des données sensibles.

Quelles sont les tendances en matière de cybersécurité pour l'Afrique ?

LJ.S : Les solutions étaient basées sur la prévention et la protection des infrastructures critiques d'une structure contre des attaques. Aujourd'hui, l'approche consiste à protéger et faire de la remédiation. La nouvelle stratégie consiste à mettre en place des outils permettant de donner de la visibilité sur l'ensemble des cyberattaques, mais aussi de réagir et de remédier à ces attaques.

E.A : L'objectif principal de Palo Alto Networks est d'être le partenaire de cybersécurité de choix. Voilà pourquoi nous adoptons une approche différente sur la façon dont nous présentons nos solutions à nos clients. Nous voulons les aider à établir la bonne stratégie de cybersécurité et nous assurer que chaque angle a été inspecté, afin qu'ils réduisent au maximum leur surface d'attaque.

Quelle est la stratégie d'Exclusive Networks et de Palo Alto Networks pour accompagner les différentes entités sur les besoins de cybersécurité en Afrique ?

LJ.S : Nous avons deux stratégies. Celle qui permet de mettre en place des outils et des solutions qui protègent le système d'information, télécoms et communication, pour une entreprise privée ou l'Etat. La deuxième a trait à la souveraineté nationale. Nous accompagnons et discutons avec un grand nombre d'Agences nationales de la sécurité des systèmes d'information

INTERVIEW

Ercan Aydin
Vice-président Afrique & Moyen-Orient de Palo Alto Networks

(ANSSI), dans la sous-région. L'objectif est de leur proposer des solutions pour donner de la visibilité sur le trafic entrant, sur le taux de cybercriminels, les sources et les typologies, afin d'atteindre l'assurance cyber. Mais aussi, pour s'assurer que l'espace numérique interne ou externe est bien protégé. Au-delà de la solution technique, il s'agit d'apporter aux ANSSI, de manière cadrée, la formation et de les accompagner.

E.A : Il n'existe pas de solution universelle. Chaque entreprise dispose d'un réseau spécifique. Palo Alto Networks traite chaque client d'une manière unique. Il existe cependant un état d'esprit, que nous devrions tous adopter pour protéger notre espace numérique.

La stratégie Zero Trust se décline en cinq étapes : définir la surface de protection, cartographier le flux de transactions, concevoir un réseau Zero Trust, créer la politique de Zero Trust et surveiller et entretenir le réseau. Enfin, examiner tous les journaux, internes et externes, jusqu'à la couche 7. Zero Trust est une approche dynamique, laquelle consiste à collecter tous les journaux et à mettre en place des rapports. Ceux-ci vous aideront à améliorer graduellement votre stratégie.

Propos recueillis par Michaël Tchokpodo

Louis-Joseph Sidibé est spécialisé dans la transformation digitale, l'Internet des objets connectés et la cybersécurité. Chez CFAO Technologies, il a travaillé en qualité de Business Development Manager des Territoires Extérieurs pour le Mali, la Guinée, la Gambie et la Mauritanie depuis 2014. A partir de février 2019, il a occupé ce même poste, mais en cybersécurité, chez Exclusive Networks, avant d'être promu en février 2021, Directeur des ventes pour l'Afrique de l'Ouest et du Centre.

Ecran Aydin est titulaire d'une maîtrise en administration des affaires de l'Université d'Istanbul Bilgi et d'un diplôme en sciences économiques et administratives du département de sciences politiques et d'administration publique de l'Université de Gazi. Au cours d'une carrière technologique de 30 ans, il a occupé plusieurs postes de direction au sein de diverses organisations, notamment chez Cisco Systems, Juniper Networks et Trend Micro. Ecran Aydin a rejoint Palo Alto Networks en 2012 en qualité de Vice-président Afrique & Moyen-Orient.

CEDEAO
Quelle stratégie de cybersécurité pour la sous-région ?

Avant le Covid, les Etats membres de la Communauté économique des États de l'Afrique de l'Ouest (Cedeao) étaient confrontés à des menaces telles que la fraude, l'usurpation d'identité, le vol de données, le ransomware, l'hameçonnage, l'incitation à la haine raciale, le déni de service, etc. Si ces menaces n'étaient pas spécifiques à la région, elles ont toutefois progressé en Afrique de l'Ouest durant la pandémie. A commencer par les contrefaçons, qui ont imposé de nouveaux défis.

Anselme Akeko

Dr Koffi Kouamé Raphaël
Directeur par intérim de la Direction de l'Economie numérique et des postes de la Commission de la Cedeao

Dr Koffi Kouamé Raphaël, directeur par intérim de la Direction de l'Economie numérique et des postes de la Commission de la Cedeao, considère que l'augmentation des cybercrimes pendant la crise sanitaire est due à l'utilisation accrue des technologies numériques. Et notamment avec l'enseignement à distance, le e-commerce, le télétravail, etc.

Par exemple, en Afrique de l'Ouest, le taux de pénétration d'Internet est passé de 47,44% à 66,4%, de décembre 2019 à décembre 2020.

Pour ce spécialiste en électronique des systèmes de télécommunications, les cybercriminels profitent « *beaucoup* » de la pandémie pour procéder, entre autres choses, à des escroqueries. Elles sont basées sur des offres de produits médicaux ou sur d'autres achats en ligne.

Développer une cyberculture

« Depuis le début de la crise, une bonne partie de la population ouest-africaine travaille en ligne. Elle est de plus en plus exposée aux cyberattaques, car elle n'a pas développé une cyberculture. En outre, elle n'est pas suffisamment informée des différents risques liés aux télétravail », commente Koffi Kouamé Raphaël. L'expert maitrise son sujet. Avant de rejoindre la Cedeao, en 2004, il a travaillé dans le secteur privé. Aujourd'hui, il dirige l'Agenda ou le Programme de cybersécurité de la communauté.

Sa mission consiste à renforcer les capacités des États membres pour mieux répondre aux cybermenaces et pour lutter contre la cybercriminalité. Ses responsabilités comprennent la coordination et la supervision du déploiement du réseau à large bande régional.

Il est également chargé de l'harmonisation des politiques et des cadres réglementaires, avec, pour objectif, la création d'un environnement propice à la croissance dans le secteur des télécommunications/TIC. La mise en place d'un marché commun des TIC, libéralisé et sécurisé, en Afrique de l'Ouest est aussi à l'ordre du jour.

Selon Koffi Kouamé Raphaël, la Cedeao n'a pas adopté de mesures spéciales pour sécuriser le télétravail. Le sujet est traité dans le cadre global de la lutte contre la cybercriminalité. Mais, il faudrait concevoir des outils de promotion de l'hygiène informatique auprès du grand public et sensibiliser les décideurs publics et privés sur leurs responsabilités.

« Les outils ont été conçus, mais l'impact de la distanciation sociale imposée par la pandémie a

considérablement retardé ces campagnes de sensibilisation dans les Etats membres. Elles débuteront au cours de la dernière semaine de mars 2021. »

Cybersécurité dans la sous-région

Pour soutenir le développement du secteur et encourager l'utilisation des services TIC sécurisés, la Cedeao a initié l'Agenda de cybersécurité communautaire. Ce programme se décline en cinq lignes d'actions : (1) Politique, législation et cadre règlementaire, (2) Gestion de la cybercriminalité, (3) Résilience des infrastructures de l'information, (4) Renforcement des capacités, (5) Coopération internationale. En ligne de mire, le renforcement de la cybersécurité et la lutte contre la cybercriminalité. Dans tous les pays, les attaques cyber s'accentuent et elles occasionnent *« des pertes financières énormes, qui sont annuellement chiffrées en millions de dollars ».* Dans le cadre du programme, la Cedeao a également adopté une stratégie régionale de cybersécurité et de cybercriminalité. Elle a vocation à améliorer le niveau des mécanismes nationaux et la politique régionale de protection des infrastructures critiques. Le but est d'assurer la résilience et la sécurité des infrastructures, et des services essentiels de la région. Des formations ont été dispensées aux forces de police, aux procureurs, aux magistrats et aux juges.

Elles consistent à renforcer leurs capacités en matière d'enquête et de poursuites judiciaires pour les infractions liées à la cybercriminalité.

En parallèle, les Etats sont accompagnés dans la mise en place de laboratoires d'investigation numérique, notamment pour la collecte et la sécurisation des preuves électroniques. Sur le volet cybersécurité, après avoir évalué le niveau de préparation des pays, la Cedeao intervient pour l'installation des équipes d'intervention en cas d'incidents de sécurité informatique (CSIRT).

L'engagement de la Cedeao est réel. Toutefois, la mise en œuvre de l'Agenda ne se fait pas sans difficultés. Dr Koffi fait remarquer que pour satisfaire le besoin des Etats, il faudrait davantage de moyens financiers. La problématique de la cybersécurité et de la cybercriminalité devrait par ailleurs figurer au rang des priorités dans les programmes nationaux de certains pays. Sur le plan technique, un grand nombre de pays ne dispose pas d'une masse critique d'expertises suffisante dans le domaine de la cybersécurité et de la cybercriminalité.

Au niveau national, pour faciliter l'harmonisation de la législation dans le cadre de la coopération régionale et internationale, il faudrait encore que les instruments communautaires s'adaptent rapidement. Malgré cela, la Cedeao a enregistré des progrès significatifs dans la mise en œuvre du programme, notamment avec l'appui des partenaires techniques et financiers.

Législation en matière de cybercriminalité

La Cedeao a été très tôt sensibilisée sur la problématique de la cybersécurité.

Les défis imposés aux Etats sont nombreux. Ils concernent les besoins en renforcement des capacités, les manques de sensibilisation et de culture de cybersécurité, ainsi que la quasi absence de cyberstratégies nationales. Les positions prédominantes, occupées par certains pays de la région dans le classement mondial de la cybercriminalité, font également partie du lot.

Dans ce contexte, trois actes communautaires ont été adoptés pour renforcer le cyberespace ouest africain : les actes additionnels sur les transactions électroniques, ceux sur la protection des données à caractère personnel et la directive sur la lutte contre la cybercriminalité. La sous-région est ainsi la première en Afrique à avoir adopté une législation en matière de cybercriminalité. La Cedeao est également la Communauté économique régionale (CER) qui compte le plus grand nombre de pays africains à avoir ratifié ou signé la Convention de Malabo de l'Union africaine et celle de l'Union européenne, laquelle est connue sous le nom de Convention de Budapest.

L'un de ses avantages est de pouvoir être ratifiée par tous les pays du monde et de disposer d'un mécanisme de coopération. Un point d'autant plus important qu'en dehors de la coopération entre Etats dans le domaine de la cybercriminalité, celle entre les secteurs public et privé, notamment les fournisseurs de services Internet, est indispensable pour la collecte des preuves électroniques.

Dr. Amani Abou-Zeid
Commissaire de l'Union africaine (UA) en charge des Infrastructures, de l'énergie et des TICs.

AFRIQUE

« Les chefs d'Etats ont élevé la cybersécurité aux rangs des projets phare de l'agenda 2063 »

La pandémie de Covid-19 a profondément bouleversé les usages, tant dans les entreprises privées que dans les organismes internationaux. Au-delà des Etats, les institutions supranationales ont elles aussi été contraintes d'adapter leurs systèmes de cybersécurité. Plus globalement, elles ont dû repenser les normes et accorder une plus grande place à ce thème, face à la multiplication des cyber-attaques. Le point avec Amani Abou-Zeid, Commissaire de l'Union africaine en charge des Infrastructures, de l'énergie et des TICs.

CIO Mag : - La pandémie de Covid-19 a mis le digital sur le devant de la scène, notamment parce que la crise induit de nouvelles pratiques, comme le recours massif au télétravail. Télétravail. Sommes-nous ainsi plus exposés aux risques cyber ?

Dr Amani Abou-Zeid : Avec la pandémie du coronavirus, la politique du télétravail s'est démocratisée et s'est généralisée. Néanmoins, le recours massif au télétravail a mis à rude épreuve, à tous les niveaux, les équipes de sécurité informatique des entreprises. Le télétravail expose les employés et leurs entreprises, ainsi que les organisations, à des dangers et à des failles dans la cybersécurité. Ils sont plus fortement exposés que dans les locaux de l'entreprise.

Dans ce contexte, comment adapter les stratégies sécuritaires ? L'UA a-t-elle émis des recommandations spécifiques dans ce sens ?

A.A.Z : La pandémie a accéléré le rythme des cyberattaques et aussi influencé le modus operandi des cybercriminels. Ils profitent de la conjoncture actuelle pour cibler les travailleurs à distance par des campagnes de phishing ou via des logiciels malveillants et d'autres menaces, qui cherchent à compromettre leurs comptes pour prendre le contrôle des serveurs et des réseaux.

D'après les statistiques, en 2020, une cyberattaque a été tentée toutes les 39 secondes. Et 80% des entreprises ont vu une augmentation des cyberattaques, alors que

Dr. Amani Abou-Zeid

Commissaire de l'Union africaine (UA) en charge des Infrastructures, de l'énergie et des TICs.

INTERVIEW

le coût de la cybercriminalité a dépassé 1 milliard de dollars, soit l'équivalent de 1% du PIB mondial.

En ce qui nous concerne, dès les premiers mois du confinement, nous avons constaté l'urgence de renforcer la cybersécurité, avec de nouvelles normes de sécurité plus sûre et plus efficaces.

A cet effet, nous avons organisé des séminaires en ligne pour sensibiliser les Etats membres et les organisations régionales sur les dangers qui accompagnent le télétravail. Nous avons développé des directives pour gérer efficacement les ressources et les systèmes informatiques. Et nous avons aussi initié des programmes de formation à distance sur la protection et la sécurisation des employés, ainsi que sur celle des données et des dispositifs, en dehors des limites physiques de l'organisation.

En interne, comment cette question de la cybersécurité a-t-elle été abordée par les collaborateurs ?

A.A.Z : Dans un premier temps, les responsables de la sécurité informatique ont formulé des recommandations de sécurité pour les télétravailleurs. L'adoption des mesures « d'hygiène informatique » a ensuite été adressée à l'ensemble du personnel pour diminuer les menaces pesant sur le personnel et l'organisation.

Nous avons renforcé la cyberrésistance des infrastructures et des structures existantes. Par la suite, nous avons adopté une approche proactive et plus intégrée de sorte à consolider les systèmes, les réseaux et les logiciels et pour instaurer, in fine, la résilience de notre réseau.

Comment l'UA, en tant qu'organisation supranationale, a réussi (ou pas) à réorganiser ses activités pour s'adapter à la situation ?

A.A.Z : A l'instar des autres organisations, l'Union africaine s'est conformée aux recommandations de l'Organisation mondiale de la santé afin de protéger la santé et la sécurité de ses employés.

Nous avons immédiatement instauré le télétravail pour l'ensemble du personnel et nous sommes passés du présentiel au distanciel pour les réunions et les évènements physiques.

Globalement, la pandémie ne nous a pas empêchés de progresser dans la mise en œuvre de notre programme et je peux avancer que la crise a accéléré, de façon remarquable, l'adoption, par nos décideurs politiques, des technologies numériques. Cette année, nous avons même organisé virtuellement le Sommet des chefs d'Etats, ce qui n'était pas envisageable avant. L'organisation a aussi pris les devants pour coordonner une réponse collective aux retombées sociales et économiques de cette crise, notamment avec la création d'un fonds spécial Covid-19 et via l'élaboration des plans de redressement sectoriels, pour aider les secteurs les plus touchés, tels que l'aviation et le tourisme.

De façon générale, quelles sont les recommandations et les stratégies mises en place autour de la question de la cybersécurité sur le continent ? Ont-elles évolué suite à la crise sanitaire ?

A.A.Z : Au niveau continental, nos Chefs d'Etats ont élevé la cybersécurité aux rangs des projets phare de l'agenda 2063. Ils ont également instruit la Commission à travailler avec tous les pays pour harmoniser les législations et les règlementations. Et ont été amenés à coordonner les initiatives pour assurer la sécurité et la confiance dans notre espace numérique.

La crise de la Covid-19 a révélé la nécessité d'investir dans la sécurité, au même titre que les infrastructures. Et à l'urgence de sensibiliser les populations, notamment les enfants, sur les risques et les menaces liés au cyberespace.

Pour accélérer la transformation numérique du continent, il est désormais essentiel de sécuriser notre environnement numérique commun, en amont des risques, par le biais d'une stratégie continentale.

Au niveau de l'UA, les réglementations pour protéger les données sont-elles suffisantes compte tenu des évolutions technologiques actuelles (5G/IOT/Cloud…) ?

A.A.Z : L'introduction des technologies émergentes - telles que l'Intelligence artificiel, l'IoT, le cloud computing - et l'utilisation croissante des plates-formes numériques pour travailler, faire des achats et communiquer, tout cela génère chaque jour une très grande quantité de données. Elles sont transférées et stockées dans des serveurs situés hors du continent et sont souvent exploitées à des fins commerciales. Cette situation pénalise le secteur privé africain et expose les citoyens aux risques liés à la sécurité et la violation de leurs vies privées.

Pour l'heure, seuls 28 pays, soit 50%, disposent des règlementations et des cadres institutionnels requis pour assurer la protection des données personnelles des citoyens. C'est préoccupant car cela freine l'utilisation effective des technologies numériques.

En sus des cadres existants visant à protéger la vie privée des Africains, la Commission de l'Union africaine développe, en lien avec toutes les parties concernées, une politique africaine sur les données. Elle vise essentiellement à maximiser l'utilisation de cette ressource. Et a vocation à faciliter un transfert intersectoriel et transfrontalier des données pour bâtir une économie numérique inclusive et durable.

De nombreux pays n'ont pas encore traduit ces mesures dans leurs législations nationales. Que peut faire l'UA ?

Pour sensibiliser sur la nécessité d'adapter les lois et les réglementations existantes à l'ère du numérique, l'Union africaine travaille avec les gouvernements et également avec les parlements, à travers le Parlement panafricain (PAP).

Il s'agit de créer des conditions favorables pour généraliser et accélérer la numérisation et la modernisation des secteurs clé tels que l'éducation, la santé ou bien l'agriculture, lesquels vont à leur tour changer la vie des Africains.

Propos recueillis par Camille Dubruelh

Deux fois élue à ce poste, **Dr. Amani Abou-Zeid** est la Commissaire de l'Union africaine chargée des Infrastructures, de l'énergie et des TIC. Depuis plus de 30 ans, elle occupe des postes de direction dans des Organisations internationales. Et notamment au sein de la Banque africaine de développement, où elle a mis en œuvre des programmes de développement multisectoriels nationaux et continentaux, a l'instar de la plus grande centrale solaire du monde.

Dr. Amani Abou-Zeid a lancé le marché unique africain du transport aérien et de l'énergie, ainsi que la première Stratégie africaine de transformation numérique. Elle a développé le deuxième Programme décennal pour le Développement des infrastructures en Afrique, avec les principaux programmes et initiatives continentaux d'intégration africaine, dans le cadre de l'Union africaine Agenda 2063.

De nationalité égyptienne, le **Dr Abou-Zeid** a une formation multidisciplinaire : Génie électrique - Université du Caire ; MBA - Université Senghor ; MPA - Université de Harvard et Ph.D. Développement social et économique - Université de Manchester.

Le Dr Abou-Zeid a été sélectionnée, à plusieurs reprises, comme l'une des femmes africaines les plus influentes. Elle a été décorée de nombreux prix et de distinctions au plan international.

FORMATION

Comment l'Afrique construit son vivier de compétences en cybersécurité ?

L'écosystème de protection et de défense contre les cybermenaces ne s'improvise pas. Il se prépare. Les pays africains comme le Sénégal et le Bénin l'ont compris. Leur construction de modèles de viviers de cybersécurité reflète la dynamique africaine en la matière.

Michaël Tchokpodo

Dans un rapport publié en septembre 2020, Kapersky, Editeur de cybersécurité, a détecté 28 millions de cyberattaques en Afrique, entre janvier et août 2020. Une véritable bombe numérique plane au-dessus du cyberespace africain. *« A l'heure actuelle, ces données sont encore bien en-dessous de ce qu'on peut trouver en Europe ou en Amérique du Nord »*, précisait Clément Domingo, inégnieur en cybersécurité et Hacker, dans une interview à Jeune Afrique. *« Mais, ils augmentent à mesure que la numérisation du continent s'améliore [...] Les entreprises africaines sont exposées aux dix attaques les plus communes, qui ont été identifiées par l'ONG Open Web Application Security Project »*, ajoutait-il.

Pour ce Franco-Sénégalais, connu sous le pseudonyme SaxX, les trois cybermenaces les plus suspectées sont : le ransomware qui consiste à demander une rançon contre la restitution de données chiffrées ; l'exposition des données sensibles mal protégées à cause des défauts de configuration de systèmes et l'injection SQL, laquelle donne accès aux pirates et à la base de données d'une structure.

Confiance, sécurité et résilience

Pour s'assurer de la confiance numérique des internautes, l'Afrique doit relever un défi de taille. Il consiste à accélérer la transformation numérique pour s'adapter, dans le contexte actuel, aux exigences de vie et de travail qu'impose la pandémie de la Covid-19.

L'un des premiers outils qui permet d'asseoir cette confiance, c'est la mise en place de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), une initiative portée par les États. En la matière, le Bénin fait exception dans la sous-région.

L'ANSSI-Bénin s'est dotée d'une stratégie nationale de cybersécurité, assortie d'un plan d'actions triennal (2020-2022), composé de 47 actions, reparties sur cinq axes. L'objectif est de répondre aux nouveaux enjeux liés aux usages numériques et aux menaces informatiques.

Le Sénégal, qui ne dispose pas d'une agence spécialisée, a élaboré une Stratégie nationale de cybersécurité, à l'horizon 2022 (SNC2022). L'ambition est de faire du pays *« un cyberespace de confiance, qui soit sécurisé et résilient pour tous. »* Cette stratégie de cybersécurité émane d'une Stratégie nationale (SN2025).

Elle est basée sur un cadre institutionnel et règlementaire solide. Khoudia Gueye Ndoye, directrice des infrastructures et des systèmes d'information de l'Université virtuelle du Sénégal explique : *« la construction de cet écosystème est basée sur l'élaboration de la Stratégie sécurité nationale (SSN), sur la création en 2008 de la Commission de protection des données à caractère personnel (CDP), ainsi que sur celle de l'École nationale de cybersécurité à vocation régionale (ENVR), créé en novembre 2018. »* Malheureusement, ce projet d'école n'a jusque-là pas abouti.

Une question de souveraineté

« Au fil du temps, les compétences se créent. La cybersécurité est devenue une question d'enjeu national et même sous-régional, car la transformation digitale impacte tous les citoyens du monde », renchérit Khoudia Gueye Ndoye.

Le Bénin pour sa part organise depuis 2017, le HackerLab, un test de niveau pour détecter des talents en cybersécurité. La 4ème édition de cet évènement aura lieu cette année. Parmi les lauréats de cette compétition, 95% sont aujourd'hui des analystes au bjCSIRT, l'équipe de réponse aux incidents de sécurité informatique. De la même façon, le Sénégal dispose de son Cyber Incident Response Team (CIRT). A l'Ecole supérieure multinationale des télécommunications (ESMT), les formations sont axées sur la protection des données personnelles et les infrastructures.

Des formations personnalisées sont notamment proposées aux managers pour améliorer la gouvernance de la cybersécurité. Elles ciblent les étudiants en formation initiale et les cadres et techniciens pour la formation continue.

« Nous nous inspirons du référentiel de compétences dans les thématiques porteuses de valeurs et comptons surtout sur l'implication des experts professionnels dans l'élaboration des curricula », souligne Adamou Moussa Saley, membre du Collège scientifique et pédagogique de l'école.

Eviter la fuite des cerveaux

Au regard du rythme de transformation digitale que connaît l'Afrique, le nombre de diplômés reste parfois insuffisant pour couvrir la demande. *« Il faudrait mettre en place des laboratoires techniques pour les tests de vulnérabilité, pour les simulations d'attaques, d'espionnage et de traçage des incidents »,* envisage Khoudia Gueye Ndoye. Il serait également nécessaire de former des ressources humaines telles que des virologues et des pentesteurs éthiques, des cyber-juristes, des auditeurs IT et de la cybersécurité, des Délégués à la Protection des Données (DPO), etc.

D'après Miguel Sossouhounto, du bjCSIRT, le Bénin veut mettre en place des modules de formation intégrés aux différents cursus : du primaire, du secondaire, des universités et des lycées agricoles. Si la formule reste encore à définir, une école du numérique va ouvrir bientôt ses portes à Cotonou.

Et pour éviter la fuite des cerveaux, le Bénin mise sur la création d'écosystèmes de start-ups spécialisées en cybersécurité. Elles proposeront leur expertise aux entreprises et aux Etats.

CYBERSÉCURITÉ
Palmarès des pays africains les plus safe

Malgré d'importantes lacunes dans la cybersécurité en Afrique, certains pays sont régulièrement cités en exemple au regard de leur implication dans la lutte contre la cybercriminalité.

Aurore Bonny

« Trois milliards et demi de dollars ». C'est le coût de la cybercriminalité en Afrique, en 2017, selon Serianu, une société panafricaine de Conseil en Cybersécurité et en affaires. C'est la raison pour laquelle ce fléau est *« l'un des défis les plus urgents qui pèse sur l'activité économique en Afrique »*. Et c'est donc *« une menace pour le développement »*.

Pour l'heure, les conditions requises pour juguler ce phénomène ne sont pas réunies. Parmi ce qui fait défaut, on peut citer les paramètres pour mesurer la cybersécurité, les formations professionnelles en matière de cybersécurité, les mécanismes et les capacités techniques pour lutter contre le spam, les taux de standards de cybersécurité et les législations qu'il convient d'améliorer ou d'inclure.

Aujourd'hui, les pays africains qui ont achevé des stratégies nationales de cybersécurité sont encore trop peu nombreux. Quelques-uns ont mis en place ce qui correspond à des équipes nationales de réponse aux incidents informatiques (CIRT) ou à des groupes multipartites de professionnels de la cybersécurité. Et moins de dix pays africains ont ratifié la Convention de Budapest sur la Cybercriminalité, ainsi que la Convention de Malabo de l'Union africaine sur la Cybersécurité et les données personnelles.

Cependant, des efforts sont consentis par certains pays pour sécuriser leur cyberespace national. Le Rwanda, le Kenya, l'Egypte, et l'ile Maurice ont un niveau d'engagement élevé selon l'IUT. D'autres, comme le Nigéria, la Tanzanie, l'Ouganda, la Tunisie, le Bénin, la Côte d'ivoire, le Botswana, le Ghana, la Zambie, le Cameroun, le Maroc et le Burkina Faso ont un niveau moyen. Les autres pays du continent sont plutôt faiblement engagés. L'Agence estonienne d'indice national de cyber sécurité (INCS) a mesuré l'état de préparation des pays pour prévenir les cybermenaces et pour gérer les cyberincidents.

De son étude, il ressort que l'Indice national de cybersécurité (INC) au Bénin est à 54,55%, de 54,55% au Nigéria, de 65% en Ouganda, de 49,35% au Kenya et de 48,05% à l'Ile Maurice. Ces pays sont donc en tête du classement africain.

L'ile Maurice est le meilleur exemple en termes de cybersécurité en Afrique. Elle est régulièrement citée par les experts. Selon Anna Collard, directrice générale de KnowBe4 Africa, c'est l'un des pays africains les mieux préparés.

« Le gouvernement donne la priorité au secteur des TIC et a élaboré une vision pour transformer Maurice en une île SMART, d'ici à 2030. C'est l'un des rares pays africains disposant d'un cadre juridique pour lutter contre la cybercriminalité ».

Les Mauriciens bénéficient d'une stratégie nationale de cybersécurité. Le pays a adhéré aux conventions sur la cybersécurité, telles celle de l'Union africaine ou celle de Budapest sur la cybercriminalité. Un protocole de cyberincidents a été finalisé et un portail centralisé de signalement des incidents permet de détecter et de surveiller le trafic malveillant en temps réel. Il contribue à améliorer sa préparation aux cybermenaces. Le suivi du plan national de réponse aux cyberincidents est facilité par un comité, lequel réunit le secteur public et le secteur privé.

Cyberespace sécurisé ?

En Afrique de l'Ouest, le Bénin a également fait des progrès considérables pour se hisser dans le top 10 africain. L'indice national de cybersécurité du pays est de 54.55%, pour un taux de développement numérique de 30,41 %, selon l'INCS. L'indicateur de la gestion des

crises et des risques dans la lutte contre la cybercriminalité affiche 100%, tout comme la protection des données personnelles. Les réponses aux cyberincidents pointent à 50%, contre 60% pour la protection des services numériques et 67% pour celle des services essentiels. Les services d'identification électronique et de confiance atteignent 78% ; le développement des politiques 43% ; l'éducation et le développement professionnel 67% et la contribution mondiale à la cybersécurité atteint 33%.

Pour l'année 2018, l'UIT a classé le Bénin à la 8ème place africaine, alors qu'il occupait la 148ème place sur 164 pays, l'année précédente. Le gouvernement béninois a expliqué cette amélioration par des initiatives fortes, telles que la mise en vigueur du Code du Numérique. Ce dernier force l'admiration, sur le plan international, par sa cohérence et son exhaustivité. Un livre entier est consacré à la lutte contre la cybercriminalité et la promotion de la cybersécurité.

La stratégie nationale de cybersécurité du Bénin a vocation à *« garantir un cyberespace sécurisé pour une économie numérique florissante »*. Aurélie Adam Soule Zoumarou, ministre du Numérique et de la digitalisation, pense que cette stratégie *« changera profondément le secteur du numérique au Bénin, en renforçant la sécurité au sein des projets numériques et en bâtissant une confiance numérique plus forte »*.

Le pays doit toutefois accroitre son expertise dans le domaine. Car pour l'heure, elle est encore peu abondante. La sécurité numérique n'est pas suffisamment prise en compte dans les projets et la culture de cybersécurité est encore peu développée. Quant au budget alloué à la mise en œuvre du plan d'action de la stratégie au niveau des institutions, il n'existe pas.

Protection des infrastructures

Le Rwanda figure parmi les mieux dotés et dans le pilier organisationnel, son score est élevé. L'indice national de cybersécurité est de 27,27% et de 38,76 pour le développement numérique.

Le pays des mille collines dispose d'une Agence nationale de cybersécurité, pour superviser la protection des Infrastructures d'information critiques (IIC). Une Autorité rwandaise de la société de l'information a également été créée dans le but d'assurer le contrôle de la gestion des infrastructures gouvernementales. L'Autorité rwandaise de régulation des services publics est pour sa part chargée de la surveillance des acteurs du secteur privé (tels que les opérateurs et les fournisseurs de services). Elle contrôle aussi la politique nationale de cybersécurité (NCSP) et l'Agence nationale de cybersécurité (NCSA).

Paula Ingabire, ministre en charge du Numérique, assure que le Rwanda répond au menaces croissantes en renforçant ses capacités dans les secteurs privés et public, tout en établissant des partenariats avec des gouvernements et des organisations étrangères. Elle est convaincue que les Etats doivent apprendre les uns des autres et qu'il leur incombe d'utiliser leur expertise, leurs ressources et leurs efforts collectifs pour lutter contre les acteurs malveillants.

Le gouvernement rwandais s'emploie également à sensibiliser les populations sur les menaces du monde numérique. Avec des partenaires internationaux, tel l'UNICEF, il s'implique dans les campagnes de protection des enfants en ligne. Les Rwandais ont également droit à des campagnes telles que le « Get Safe Online », pour être sensibilisés et protégés contre les risques de sécurité dans le cyberespace.

Bases juridiques et coopératives

Au Kenya, l'indice national de cybersécurité est de 49,35%, pour un développement numérique de 41,69%. Il est également parmi les meilleurs en Afrique. Ses piliers juridiques et sa coopération sont importants.

Ils sont marqués par une collaboration locale multipartite entre le gouvernement, les différents Cyber Incident Response Team (CIRT), les institutions financières, ainsi qu'avec les opérateurs de télécommunications, les universités, les fournisseurs d'infrastructures d'informations critiques, de services d'utilité publique, de contenu et d'enregistrement de noms de domaine, etc.

Depuis la loi de 1998 sur l'information et les communications, le Kenya a donné mandat à l'Autorité des communications du Kenya (CA) pour développer un cadre national de gestion de la cybersécurité. Une équipe nationale de réponse aux incidents informatiques au Kenya - Centre de coordination (National KE-CIRT / CC) - a été créée.

Un cadre de collaboration multi-

agences est responsable de la coordination nationale de la cybersécurité. C'est le point de contact national du Kenya sur les questions de cybersécurité. La promulgation de la loi de 2018 sur l'utilisation abusive de l'ordinateur et la cybercriminalité s'inscrit également dans ce contexte. Elle a *« largement contribué au renforcement de ce cadre de collaboration multi-agences, notamment sur les aspects clés qui soutiennent la résilience nationale en matière de cybersécurité ».*

Avec sa stratégie nationale de cybersécurité, lancée en 2014, le gouvernement kenyan s'est engagé à assurer la sécurité et la prospérité du pays, ainsi que celles de ses partenaires. Il considère également *« la cybersécurité comme un élément clé »*, en offrant aux organisations et aux particuliers une confiance accrue dans les transactions en ligne et mobiles. Et en encourageant les investissements étrangers, tout en ouvrant un ensemble plus large d'opportunités commerciales sur le marché mondial.

Le Kenya dispose également de quelques-unes des meilleures entreprises et références en matière de cybersécurité en Afrique. Parmi elles, Serianu, Lafont Innovation LLC, Enovise et tant d'autres.

Avec un indice national de cybersécurité de 50,65%, l'**Ouganda** emboite le pas au Rwanda et au Kenya. Il a pris d'importantes mesures d'harmonisation des processus de cybersécurité et de protection des données, ainsi que des mesures collaboratives de poursuites et d'enquête. Dans ce pays d'Afrique de l'Est, la cybercriminalité est criminalisée et la coopération internationale joue un grand rôle dans l'amélioration de la cybersécurité.

Cybersécurité versus cyberattaques

En Afrique de l'Ouest, le Nigéria est une référence, avec 54,55% d'indice national de cybersécurité. L'indicateur national de développement des politiques de cybersécurité est de 71%. Il est renforcé par une unité spécialisée, laquelle est chargée de l'élaboration de la politique nationale de cybersécurité.

Sur le plan éducatif, la cybersécurité pointe à 67% dans l'enseignement primaire, secondaire et supérieur. La contribution du pays à la cybersécurité mondiale atteint 67%. En plus de la ratification de Convention sur la cybercriminalité, le Nigéria héberge une organisation régionale et internationale de cybersécurité : l'Association africaine de la sécurité de l'information (AISA). S'agissant de son indicateur de protection des données personnelles, il pointe à 100%, tandis que la réponse aux cyberincidents est de 83%, contre 67% pour les services d'identification électronique et de confiance.

D'importantes organisations, telles la Commission nigériane des communications (CNC), font de substantiels efforts pour soutenir la campagne de cybersécurité dans le pays. Certains experts considèrent pourtant la cybersécurité nigériane comme médiocre, au regard des cyberattaques qui sont favorisées par l'absence d'un cadre juridique et de règlementation adéquats. Cela pourrait contraindre les organisations à adopter des mesures pour protéger les données qu'elles détiennent et à mettre en place des contrôles minimaux de cybersécurité. Le Nigéria est d'ailleurs l'un des pays au monde qui subit le plus de cyberattaques.

Plus de la moitié des incidents ne sont pas relevés. Et ce, malgré l'existence du Centre national de coordination de la cybersécurité (NCCC) et d'une équipe nigériane de préparation aux urgences informatiques (NgCERT) qui veille à la gestion des incidents de cybersécurité dans les différents secteurs publics et privés. La prévention des attaques est à la peine.

Au Nigéria, contrairement à des pays comme le Kenya ou l'Afrique du Sud, les entreprises ne sont pas obligées de signaler les violations des données aux consommateurs concernés et à l'agence gouvernementale. Seule l'équipe nigériane d'intervention en cas d'urgence informatique (nCert) a développé un formulaire incitant les gens à signaler les vulnérabilités et les incidents.

L'Afrique du Sud fait également partie des pays du monde les plus attaqués par la cybercriminalité et pourtant, elle est parmi les mieux préparés. L'indice national de cybersécurité est de 27,27%, pour un développement numérique réalisé de 54,80%.

Le pays dispose d'une stratégie nationale de cybersécurité et essaie de renforcer sa législation et ses politiques en matière de cybersécurité. Il est doté d'un cadre politique national de cybersécurité (NCPF) et a défini une approche ciblée et cohérente pour sécuriser le cyberespace national. Il solutionne divers aspects, notamment le manque de coordination entre les divers organes gouvernementaux et l'absence d'un cadre réglementaire efficace pour soutenir la cybersécurité du pays. Et intervient également pour remédier à l'insuffisante sensibilisation au manque de capacités, de compétences et de ressources en matière de TIC. Par ailleurs, le NCPF définit les lignes directrices relatives à la cybersécurité en Afrique du Sud, tout en soumettant le gouvernement à l'élaboration des politiques et des stratégies détaillées de cybersécurité.

Renforcer la législation

En Afrique du Sud, il existe également des organisations et des départements gouvernementaux engagés, même s'ils sont difficilement coordonnés. Parmi eux : le Centre de recherche scientifique et industrielle (CSIR), l'Agence nationale des technologies de l'information (SITA), l'Agence de sécurité de l'État (SSA), le Service de police sud-africain (SAPS), des Hawks, de la Force de défense nationale sud-africaine (SANDF), le Département des communications et des technologies numériques (DCDT) et de la défense (DOD).

La Cybersécurité en Afrique du Sud, c'est également plusieurs projets de lois. Mais, ils sont limités et leur mise en œuvre manque de vélocité, ce qui contribue à faire du pays *« un eldorado pour les cybercriminels »*.

Il détient le triste record du *« troisième plus grand nombre de victimes de la cybercriminalité dans le monde »* et les pertes financières sont estimées à 2,2 milliards de rands par an.

Dans le Top 20 de l'Indice global de cybersécurité de 2018, établi par l'UIT, figurent également la Zambie, le Burkina Faso, le Gabon, le Sénégal, la Gambie, le Ghana, la Côte d'ivoire, le Botswana, la Tanzanie, l'Ethiopie, le Malawi, et les Seychelles.

Certains pays sont en bas de classement mondial en matière de cybersécurité. En 2020, Comparitech a classé l'Algérie comme *« le pays le moins cybersécurisé au monde, malgré une légère amélioration de son score »*. Il doit cette place à l'absence de nouvelle législation et à une législation considérée comme la plus pauvre, avec une seule loi, laquelle concerne la vie privée. Le taux d'infection des logiciels malveillants est de 19,75% et 26,47% des ordinateurs sont infectés par les logiciels malveillants. Sa préparation aux cyberattaques est considérée comme très faible.

Aurore Bonny

TÉLÉTRAVAIL
Quand les employés deviennent des « responsables informatiques »

La crise sanitaire a forcé de nombreuses entreprises à switcher vers le télétravail. Si certaines étaient bien préparées et fonctionnaient déjà avec une partie des effectifs à distance, pour d'autres, la bascule a été plus problématique. Dans tous les cas, ce nouveau mode de travail requiert des fondamentaux en termes de sécurité informatique, afin d'éviter les attaques contre les salariés et donc contre l'entreprise. Benoît Grunemwald, expert chez ESET, entreprise technologique leader dans les solutions de cybersécurité, fait le point sur les bonnes pratiques à mettre en place.

Camille Dubruelh

Benoît Grunemwald
Expert chez ESET

« Pour beaucoup d'entreprises, le recours massif au télétravail imposé dès les premiers confinements n'a été qu'une mise à l'échelle ». Pour Benoît Grunemwald, évoquer la bascule vers le télétravail et les problématiques de sécurité informatiques nécessite d'observer les bonnes pratiques, mises en place par certaines entreprises bien avant la crise. En effet, nombre d'entre elles fonctionnaient avec des employés en télétravail ou des prestataires à distance. La crise sanitaire n'a été qu'une généralisation de ce fonctionnement, pour s'appliquer de manière plus ou moins importante à la grande majorité des employés.

« Comment traitions-nous ces populations à distance avant la crise ? questionne l'expert d'ESET. Quel équipement, quelle sensibilisation, quelles infrastructures étaient déployés pour que les données auxquelles les travailleurs accèdent soient sécurisés ? C'est cela que nous devons regarder afin d'élargir ces pratiques. »

Sécuriser les mots de passe

Passer en télétravail nécessite le plus souvent d'avoir recours à un Cloud et des outils collaboratifs, pour partager les documents et maintenir un travail d'équipe. Premier impératif dans ce cadre, selon Benoît Grunemwald, sécuriser les mots de passe des employés. Dans un premier temps, ceux-ci doivent être forts et différents pour chaque application.

Aussi, le document sur lequel sont consignés ces mots de passe doit être bien protégé.

Mais ceci n'est pas suffisant selon l'expert, qui

conseille d'utiliser l'authentification forte. Il s'agit d'un code à six chiffres reçus sur le téléphone de l'employé, assurant ainsi une deuxième protection au cas où les mots de passe aient été volés.

Ce code change toutes les 30 secondes, et assure ainsi que la personne qui se connecte est bien celle qu'elle prétend être. Cette pratique, très simple et peu couteuse à mettre en place, est systématiquement recommandée par ESET, que ce soit en interne ou en externe, pour les clients.

« Nous proposons notre solution, ESET Secure Authentification. En termes de coût, financier et humain, c'est très abordable et simple à déployer », assure Benoît Grunemwald.

C'est une solution qui s'intercale dans des applications existantes. Car si les grands fournisseurs de messagerie proposent cette authentification forte, ce n'est pas le cas des petites applications. C'est pour cela que nous proposons cette solution ».

Si celle-ci était déjà déployée auprès des clients d'ESET avant la pandémie, le recours massif au télétravail a poussé l'entreprise à la proposer d'avantage aux partenaires. Car la crise a engendré une inversion de la proportion du personnel en travail à distance et de celui présent sur site.

Le gros avantage avec cette solution : n'importe quel téléphone mobile peut générer le code d'authentification forte, ce qui la rend accessible au plus grand nombre.

En Afrique, les risques de l'obsolescence

Sur le continent, des spécificités se dégagent en termes de cyber risques selon l'expert. En effet, le rapport trimestriel d'ESET sur les menaces fait état, sur le continent, de nombreuses machines attaquées à cause d'anciennes vulnérabilité. Il s'agit en fait d'ordinateurs qui ne sont pas à jour ou qui utilisent des logiciels obsolètes.

L'entreprise recommande ainsi à ses clients africains de mettre à jour les systèmes d'exploitation, les applications et tous les éléments actifs du réseau. Car ces derniers, vieux de plusieurs années, comprennent souvent de nombreuses failles. Il s'agit des routers, des imprimantes, des écrans, de tous les objets connectés au réseau, qui comprennent des vulnérabilités.

Analyser les risques

La bascule vers le télétravail implique donc une plus grande analyse des risques, selon l'expert. Car il s'agit le plus souvent d'une population qui n'avait pas l'habitude de travailler depuis l'extérieur. Certains membres du personnel qui accèdent à des informations confidentielles au sein de l'entreprise, comme les comptables, se sont ainsi retrouvés en télétravail dans ce contexte de crise.

Benoît Grunemwald conseille alors de baser cette analyse-risque sur trois piliers :

- La disponibilité des données, c'est à dire qu'elles soient disponibles et accessibles uniquement au personnel qui en a besoin ;
- L'intégrité des données, c'est à dire qu'elles restent justes et non falsifiées ;
- La confidentialité, tant en interne qu'en externe où personne ne doit avoir accès à certaines données.

Les clés de la confiance

« La beauté de l'agilité informatique, est qu'elle permet d'assurer la sécurité sur n'importe quel poste de travail, au sein de l'entreprise, comme à l'extérieur. Même en utilisant un poste lambda, on peut continuer à travailler sans mettre en danger la sécurité de l'entreprise », assure Benoît Grunemwald.

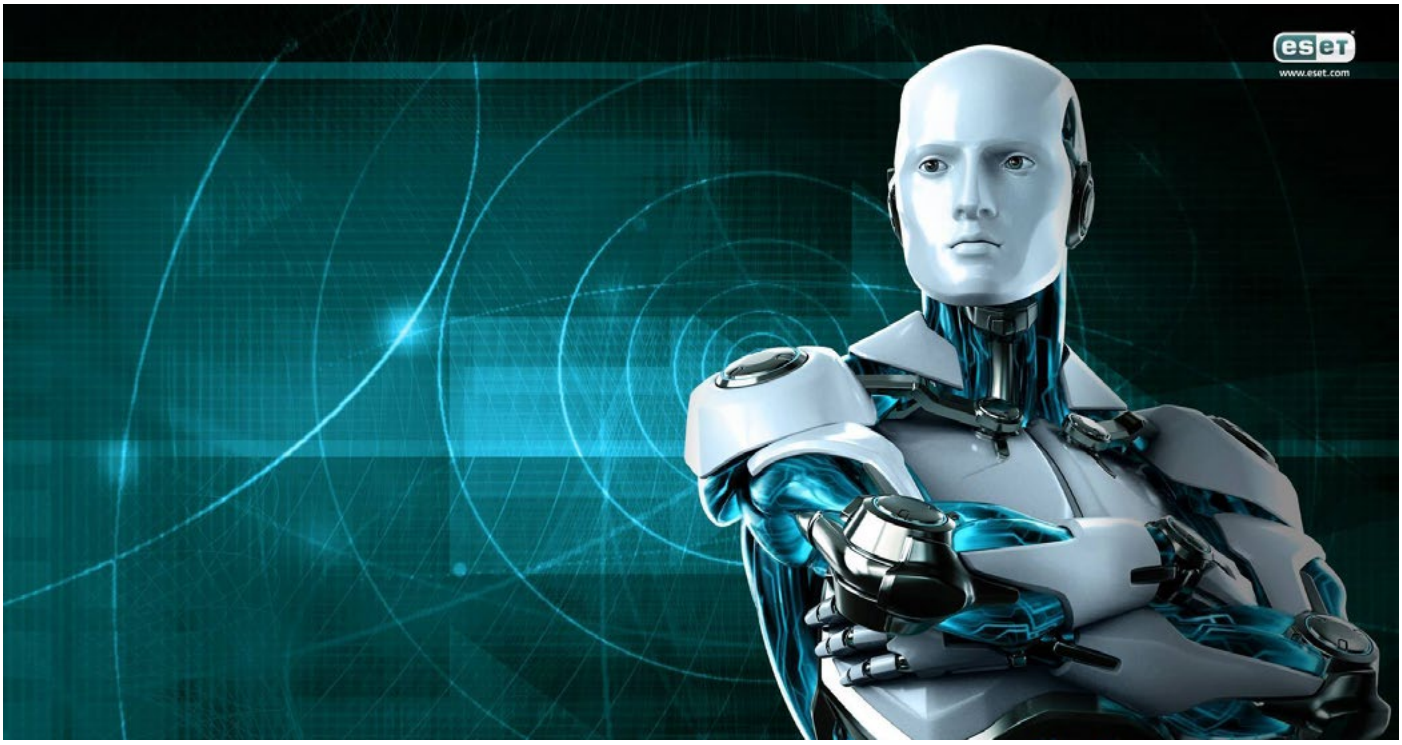
Pour autant, cela demande plus de préparation, plus de moyens et plus d'étapes pour sécuriser les postes.

Et ceci requiert un travail énorme de sensibilisation des employés et de mise en place de solutions techniques. Ainsi donc, doivent être déployés des filtres anti-phishing, anti-spams, ceci dans une démarche d'accompagnement de l'utilisateur.

Car, *« chaque terminal connecté au même réseau devient un attaquant potentiel »,* rappelle Benoît Grunemwald, qui attire l'attention sur la nécessité de *« ne pas oublier les objets connectés au réseau, dont les smartphones sur lesquels il est nécessaire d'installer un antivirus ».*

« L'employé n'est pas là pour être un expert informatique, ajoute l'expert d'ESET. On gagne du temps s'il est informé, mais il n'a pas vocation à tout savoir sur la sécurité ».

Des solutions simples existent pour sensibiliser l'ensemble des employés, comme mener de fausses campagnes de phishing, avec bienveillance. Ensuite, c'est une question de confiance. *« Lorsqu'on travaille ailleurs qu'au sein de l'entreprise, chaque employé devient un responsable informatique. Il faut donc l'informer pour qu'il devienne un maillon fort de cette cybersécurité »*, conclue l'expert.



START-UP

Le secteur de la cybersécurité, un marché prometteur mais difficile

Les entrepreneurs africains du domaine de la cybersécurité s'activent sur un continent attractif autant pour l'innovation que pour la cybercriminalité. L'écosystème est encore très difficile pour les jeunes pousses.

Aurore Bonny

Si l'on consulte la multitude d'études sur le marché de la cybersécurité africaine, on apprend que les compétences dans le domaine sont fortement requises. Et qu'avec un nombre d'internautes pouvant atteindre le milliard, d'ici à 2022, il faut s'attendre à ce que les dépenses en cybersécurité pointent à 170,4 milliards de dollars, l'année prochaine. Et pourtant, une importante partie de la population africaine est encore sous-éduquée sur les notions de cybercriminalité et de cybersécurité.

Cette constatation a été émise dans le rapport 2019 de KnowBe4 sur la sensibilisation à la cybersécurité. Ce même acteur de la sécurité, qui compte plus de 800 répondants dans 8 pays africains, a révélé que 53% des Africains interrogés pensent qu'il suffit de faire confiance aux emails de personnes qu'ils connaissent.

Et 64% ne savent pas ce qu'est un ransomware, alors qu'ils pensent pouvoir facilement identifier une menace pour la sécurité. Par ailleurs, 28% des personnes consultées ont été confrontées à un email

de phishing et 50% ont été infectés par un logiciel malveillant, tandis que 52% ne savent pas ce qu'est l'authentification multi facteurs. Pour Anne Collard, directrice générale de KnowBe4 Africa, il est clair que *« les Africains ne sont pas préparés à ces menaces, ce qui en fait des proies de plus en plus faciles pour les cybercriminels »*.

Au nombre des points faibles en la matière : des gouvernants préoccupés par d'autres questions urgentes ; de faibles budgets pour la cybersécurité ; une grave pénurie de professionnels de la sécurité ; un manque de sensibilisation et de compétences autour de la protection en ligne malgré la connectivité qui s'améliore ; le manque de législation et d'application de la loi…

« L'Afrique compte parmi les régions à la croissance la plus rapide, en termes d'activités de cybercriminalité. De nombreux criminels considèrent le continent comme un havre de paix pour leurs opérations illégales », affirme Annie Collard.

Il y a tant à penser et à accomplir sur le continent et pourtant, admet Boubacar Bah, consultant en cybersécurité, l'Afrique n'est pas très avancée en ce qui concerne la révolution du numérique.

« Avant de parler de cybersécurité, il faut se demander où en est l'Afrique dans son développement numérique ». Cet employé de Krysecu, une jeune entreprise guinéenne de cybersécurité, lancée en janvier 2021, considère que les start-up ont un rôle important à jouer tant la question de l'intégrité territoriale du numérique et des données est importante sur le continent.

« Tout ne peut pas être confié aux firmes étrangères. Des données doivent rester en Afrique. Les entrepreneurs africains doivent s'activer dans ce sens », reconnait Boubacar Bah. Ils devront toutefois affronter des difficultés promptes à les décourager ou à les neutraliser en vol. A commencer par l'absence de structures de soutien à la Recherche et Développement. C'est le premier exemple cité par Karim Ganame, Docteur burkinabè en cybersécurité et Fondateur de Streamscan, une compagnie avant-gardiste qui détecte les nouvelles générations de cyberattaques. Comparant le contexte africain au contexte du Canada, où il est basé, il constate qu'au pays de l'érable, les compagnies sont soutenues dans tous les domaines d'inventions. *« Certains programmes d'Etat permettent de soutenir jusqu'aux salaires des employés, afin de motiver les jeunes et les entrepreneurs. Je constate que ce n'est pas le cas en Afrique »*.

Confiance dans les solutions africaines

S'agissant du marché de la cybersécurité, qui est dominé par les entreprises étrangères, Karim Ganame suggère que les Africains prennent davantage conscience qu'il ne sert à rien de financer l'innovation venant des pays étrangers.

« Chaque fois que vous achetez une technologie, qui vient d'un autre pays, vous financez les capacités d'innovation de ce pays, tout en limitant la capacité d'innovation locale ». Il considère que les Africains ne doivent pas manquer de confiance en leurs propres solutions et en leurs capacités.

Face aux nombreux obstacles, peut-on parier sur un avenir prometteur pour les start-up de cybersécurité africaines ? En douter consisterait à accorder le monopole du savoir technologique à certains et pas à d'autres. Pour Boubacar Bah, le savoir dans les nouvelles technologies n'est pas restreint.

« Il faut juste une volonté d'apprendre et de se former dans le numérique ». Ces lacunes, il les perçoit comme « un terrain vierge », *« une occasion propice pour les entrepreneurs africains de rafler les marchés, avant que les ressources ne soient exploitées, de sorte à gagner en expérience »*. Il perçoit l'avenir comme prometteur pour les jeunes pousses du domaine de la cybersécurité.

« Il faut se former dans les nouvelles technologies et appliquer ces connaissances aux réalités africaines. Il ne faut pas seulement copier les exemples venant d'ailleurs, mais se renseigner sur les réalités, afin de répondre aux réels besoins africains ».

Pour créer des compagnies de cybersécurité, qui soient des leaders mondiaux - et non seulement continentaux -, Karim Ganame mise sur les nombreux talents. Des talents dotés d'énergie, de capacités et de motivation. Il considère que les Etats subsahariens n'ont pas encore compris la valeur ajoutée que représente ce capital humain, ainsi que le fonctionnement des nouvelles technologies.

C'est ce qui expliquerait que ces pays ne sont pas vraiment enclins à soutenir les start-up créatives. Pour le Fondateur de Streamscan, les Africains devraient avoir davantage confiance en leurs capacités et devraient s'encourager mutuellement.

Soutien aux jeunes pousses

« Aucun pays ou continent n'a le monopole de la connaissance. Plus le local est consommé, plus les moyens de se développer existent. Et plus il est possible d'engager d'importants moyens de production et d'intervention. L'Afrique a raté plusieurs choses dans le développement numérique, mais elle peut encore réaliser que l'innovation est un levier de croissance. A charge pour les gouvernements de s'impliquer réellement dans l'encouragement et le soutien des jeunes pousses », soutient Karim Ganame.

Ruphus Muita, expert kenyan en cybersécurité, ne dit pas autre chose. Il est convaincu que ces start-up ont une chance de dominer le monde de la cybersécurité, tant que la direction reste à la pointe de l'information. *« Pour qu'une entreprise se hisse au sommet, elle doit acquérir les dernières technologies et prendre les bonnes décisions commerciales. Ce sont les décisions prises par la direction qui déterminent la destination d'une start-up ou d'une entreprise établie ».*

Adeshina Adewumi est cofondateur nigérian et PDG de One Kiosk Africa, une solution de commerce électronique opérant en Afrique. Sa solution, qui tire parti de la géolocalisation et de l'apprentissage automatique, permet aux propriétaires de magasins de détails informels d'accéder au marché et au financement, grâce aux données de vente. L'entrepreneur, qui est membre d'association de promotion du développement numérique en Afrique, pense que l'avenir n'est pas à percevoir, mais à vivre présentement. Il apprécie la capacité des jeunes entreprises africaines à s'adapter aux technologies pour répondre aux scénarios locaux. Des capacités qui sont plus rapides et plus précises que celles des solutions fournies par leurs homologues étrangers.

De son point de vue, les meilleures start-up de cybersécurité pour le continent africain viendront de l'Afrique, même si elles doivent encore être formées. A charge pour celles qui sont d'ores et déjà créées de s'affirmer, en prenant le pouvoir et en arrachant leur part du marché, sans attendre qu'elle leur soit donnée, car ce ne sera pas le cas. *« Personne ne vous donne le pouvoir gratuitement. Je pense que dans le domaine de la cybersécurité, les start-up africaines doivent aller au-delà de la norme. Elles doivent se dépasser et prouver qu'elles sont meilleures »*, soutient Adeshina Adewumi. Et pour atteindre ses objectifs, les résultats et les excuses ne coopèrent pas. *« Les résultats suppriment les excuses et ne peuvent être cachés »*. Seul le marché répond en fonction de ces résultats.

PAIEMENTS DIGITAUX
Switchs nationaux de paiement : les facteurs clés de succès

Aujourd'hui, l'inclusion financière est reconnue comme un vrai catalyseur de développement et de réduction de la pauvreté. Et de nombreux acteurs du monde financier ont mis l'accent sur l'importance de la réduction de l'utilisation de moyens de paiement scripturaux au profit de moyens de paiement digitaux.

Ces derniers permettent en effet de réduire un certain nombre de risques liés à l'utilisation du cash, tels que le vol ou la perte. Le paiement digital offre à la population un éventail de services liés aux moyens de paiements digitaux (transferts d'argent, e-commerce, accès aux crédits, à l'épargne, etc.). De nouvelles offres financières digitales se développent de manière exponentielle grâce à l'arrivée, sur le marché, de nouveaux types d'acteurs, dont les Etablissements de Monnaie Electronique (EME). Dans ce contexte de multiplication des initiatives et des acteurs, l'enjeu d'interopérabilité devient primordial pour la mise en commun des infrastructures, des réseaux de distribution et, de manière générale, des canaux d'accès à ces services financiers. Le tout s'inscrit dans un objectif global de proposition de valeur forte pour les populations, tant sur l'offre elle-même (avec un large panel de services), que sur la couverture géographique des services financiers (avec le développement de l'offre en milieu rural).

Norme d'interopérabilité

Dans cette logique, et afin d'instaurer une interopérabilité des paiements digitaux à l'échelle nationale, de nombreux gouvernement ont opté pour la mise en place d'un switch et éventuellement d'un schème national de paiement. Ces dispositifs, qui sont mis en place au niveau du Système national de paiement d'un pays, permettent à tout acteur de l'écosystème de paiement (banque, institution de microfinance, établissement de monnaie électronique, FinTechs, etc.) d'acheminer une transaction financière digitale vers un autre acteur de cet écosystème.

Le schème définit une norme globale d'interopérabilité. Elle comprend, sans s'y limiter, les règles commerciales, les normes techniques, les répartitions des revenus entre les institutions financières participantes, l'image de marque commune et les règles relatives aux litiges et à la protection des clients.

Le switch fait plus étroitement référence à la technologie, qui est au cœur du système de paiement.

Ce dernier est souvent accompagné d'un schème, lequel définit les règles et les normes, mais peut parfois être implémenté seul.

Il existe deux grandes catégories de systèmes de switching. L'un permet d'instaurer une interopérabilité au sein du monde monétique et l'autre une interopérabilité des moyens de paiement financiers mobiles. Certains modèles « hybrides » ou étendus permettent par ailleurs d'établir une passerelle entre les mondes monétique et mobile. C'est ce type de modèle que BearingPoint a décidé d'étudier plus en détail.

Concernant les enjeux et les objectifs de ces switchs, les systèmes étudiés ont tous été instaurés à l'initiative du gouvernement et sont, pour la plupart, mis en place par l'entité de gestion d'autres systèmes nationaux de paiement de détail. L'objectif premier de tels projets est d'augmenter l'inclusion financière du pays, tout en limitant les risques liés à l'utilisation du cash et en instaurant une meilleure transparence dans les paiements. Certains pays ont également décidé d'instaurer un caractère obligatoire d'interfaçage au switch pour tous les fournisseurs de services financiers électroniques. L'objectif est de garantir une interopérabilité rapide et complète des paiements à l'échelle nationale. C'est le cas de Maurice et de son switch national MauCAS. Il a été rendu obligatoire pour toutes les banques du pays.

Quel modèle de gouvernance ?

Concernant les produits et les services offerts, les cas d'usage autorisés les plus courants, grâce à la mise en place d'un switch, sont par exemple les transferts de personne à personne ou P2P. Dans ce cas d'espèce, l'émetteur et le récepteur peuvent être un portefeuille électronique (wallet) ou un compte en banque. Et les paiements de factures peuvent s'effectuer depuis un compte en banque - ou un wallet - vers le compte bancaire d'un facturier. Il peut également s'agir des paiements d'une institution gouvernementale vers une personne (G2P). Sur ce plan, on peut citer les paiements des prestations sociales ou des salaires des fonctionnaires. Ou les paiements marchands entre un consommateur et un commerçant, sur un lieu de vente, ainsi que les opérations de Cash-in (dépôt d'argent) et de Cash-out (retrait d'argent), auprès d'un Guichet automatique de billets. Le switch permet la mise en œuvre de ces différents types d'opérations. Il les rend surtout possible, de façon interopérable, que ce soit d'un acteur à l'autre, d'une banque à un établissement de monnaie électronique, du compte d'une institution de microfinance à un wallet, etc.

Concernant la gouvernance de tels systèmes, il est important de souligner que les structures d'actionnariat des switchs étudiés sont principalement des modèles hybrides, composés à la fois de banques privées et publiques. Bien souvent, le projet est initié par le gouvernement, lequel privilégie ensuite un modèle mixte afin d'impliquer et de faire adhérer au maximum les fournisseurs de services financiers de l'écosystème.

Dans le cas d'un switch monétique et mobile, le modèle de gouvernance peut être un vrai défi. Les participants (banques, institutions de microfinance, établissements de monnaie électronique) étant très différents, leurs enjeux et leurs objectifs sont tout autant diversifiés, voire parfois contradictoires. Certains pays, comme la Bolivie, ont ainsi choisi de ne pas faire uniquement siéger les banques.

Comment peut-on alors concrètement choisir le modèle de switching adéquat pour un pays ? Et quels sont les facteurs clés de succès à la mise en place d'un tel système ? Pour commencer, il est primordial de favoriser au maximum l'adhésion claire et tangible de l'écosystème, en impliquant les parties-prenantes. En Inde, par exemple, les banques participantes ont fourni 100% du capital de départ et elles détenaient 10 des 15 sièges au conseil d'administration du nouveau switch. Les parties-prenantes avaient donc tout intérêt à ce que ce nouveau système remporte un franc succès. Il est également important de ne pas mettre en place, dès le départ, un modèle trop complexe et coûteux. Il est préférable de prioriser l'adhésion des parties-prenantes et de développer progressivement des fonctionnalités et des cas d'usage plus complexes.

La cible technique se trouve à l'équilibre entre un modèle suffisamment avancé et récent, mais qui soit également suffisamment proche de l'existant pour minimiser les coûts et les délais d'intégration. Il est donc primordial de déployer des services permettant des cas d'usage basiques, avant de s'orienter vers des services plus innovants, comme

l'illustre bien le modèle indien NPCI. De même, pour une adhésion rapide et effective de l'écosystème, il est recommandé de prévoir la mise en place de mesures incitatives, comme la gratuité de certains services et de ne pas seulement envisager des mesures répressives. C'est ce modèle qu'à choisi la Jordanie en offrant une gratuité des transactions pour les banques, durant les deux premières années suivant le lancement du switch.

Habitudes locales

Pour définir le modèle de switching, il est essentiel de tenir compte des habitudes de consommation locales. Certains pays ont à ce titre priorisé le lancement de services de wallets uniquement disponibles depuis des Smartphones, via une application mobile. Là où le taux de pénétration des Smartphones est faible, ce modèle peut limiter drastiquement l'adhésion de la population à ces services, ce qui a pour effet d'impacter l'inclusion financière des populations.

Dans ces pays, le canal USSD est une bonne alternative. Les services financiers sont alors accessibles depuis un mobile, sans que cela nécessite une connexion Internet ou un Smartphone. Il est de surcroit essentiel de faire évoluer le modèle en fonction des besoins de la population et des innovations du marché. Et notamment en collectant les retours utilisateurs, de sorte à adapter le modèle aux besoins de la population et des commerçants, tout en cherchant continuellement des innovations à l'international. Les autres facteurs clés de succès structurants sont la communication. Elle doit être déployée autour du switch et plus largement autour de l'intérêt, pour les populations et pour les commerçants, d'avoir recours à ces moyens de paiement digitaux plutôt qu'à du cash. Pour susciter l'adhésion des populations et des commerçants, et leur faire changer leurs habitudes de fonctionnement, une proposition de valeur forte est nécessaire. Le switch doit également être accompagné d'une communication claire sur l'utilisation des données et sur la sécurité des fonds. Les populations habituées aux moyens de paiement scripturaux, qui découvrent ces nouvelles problématiques, doivent donc être rassurées.

Enfin, un tel système ne serait possible sans le cadre règlementaire qui convient pour soutenir l'écosystème, tout en limitant les risques. Ainsi, la règlementation doit accompagner le switch et limiter les risques associés aux moyens de paiement digitaux (notamment sur les questions d'AML/CFT). La règlementation doit également favoriser l'enregistrement des nouveaux clients avec un processus en ligne (e-KYC) ou par exemple par une approche à plusieurs niveaux[1].

Jean-Michel Huet, Associé - Olivier Darondel, Senior manager - Marouane Znagui, Manager et **Chloé Chevrand - Consultante BearingPoint**

PROTECTION DES DONNÉES
Pourquoi les entreprises sont-elles plus exposées avec le télétravail ?

Diverses raisons expliquent l'exposition aux risques cyber de l'ensemble des organisations : le contexte imprévu et anxiogène, la désorganisation du cadre de travail et des comportements inadaptés, ainsi que des dispositifs de cybersécurité insuffisants (outils, gouvernance, processus, ressources, formation). Il est temps de définir une stratégie de cybersécurité, car la prochaine crise sera numérique !

Marie de Fréminville
Présidente de Starboard Advisory

La crise sanitaire de la Covid-19 a été un accélérateur exceptionnel de transformation numérique. De nombreuses initiatives ont été prises dans l'urgence pour réaliser des opérations à distance. Nous avons assisté au développement du télétravail (près de 30% de la population active à temps plein), à la création de nouveaux sites d'e-commerce, à l'utilisation croissante d'outils collaboratifs (partages de fichiers ou réunions en visioconférence) et de la signature électronique.

La Covid-19 a forcé les entreprises (même les grandes entreprises qui n'avaient pas anticipé une telle situation) à prendre des dispositions. Pour une grande partie des effectifs et sur une durée inconnue, il a fallu procéder à l'achat de PC portables, au transport de PC fixes au domicile ou encore à l'utilisation de PC privés à des fins professionnelles... Le revers de la médaille, c'est que cette période a considérablement augmenté la surface d'attaque et l'exposition au risque de vol de données, à la fraude ou aux demandes de rançons. Elle a aussi été le révélateur de la dépendance des entreprises au numérique, une technologie qui permet de faire fonctionner l'économie et de maintenir le lien social. Le Service informatique (SI) est devenu, pour la plupart des entreprises, pour les collectivités locales ou les hôpitaux, un organe vital, sans lequel l'organisation peut être paralysée ! Une fuite de données stratégiques ou personnelles peut avoir des conséquences mortelles ou peut fragiliser durablement l'entreprise, mais aussi ses parties-prenantes.

Pourquoi les entreprises sont-elles plus exposées après la crise ?

Première raison : le contexte de crise sanitaire. Il a facilité la tâche des cybercriminels. Ils sont créatifs et rapides, et la surface d'attaque a naturellement augmenté pendant la crise : utilisation accrue d'Internet, navigation sur le Web, achats en ligne et utilisation des réseaux sociaux.

L'état de confusion et d'anxiété des collaborateurs engendre de mauvaises manipulations. Les nouvelles attaques liées à la Covid-19 (malwares, attaques DNS, noms de domaines frauduleux, faux sites, spams, phishing, faux installeurs) sont nombreuses et ne sont pas identifiées par les systèmes de sécurité.

Les mobiles sont aussi des vecteurs d'attaque. De fausses applications exploitent la crise du Coronavirus et accèdent aux photos, aux vidéos, aux fichiers, à la localisation du terminal, ainsi qu'à l'autorisation de prendre des photos et d'enregistrer des vidéos.

De faux emails et SMS, provenant de grandes enseignes (vente en ligne, société de transport, banques, administrations, ONG), ont permis de récupérer les identifiants et les mots de passe de leurs utilisateurs.

Deuxième raison : le cadre de travail est désorganisé pour les utilisateurs et pour les équipes informatiques et de sécurité.

Selon une étude publiée par Tessian, la moitié des employés admettent qu'ils prennent des raccourcis en télétravail en matière de cybersécurité. En partageant par exemple des fichiers confidentiels par courrier électronique, au lieu de recourir à des mécanismes plus fiables.

Les télétravailleurs mélangent leurs usages personnels et professionnels sur leurs postes de travail (qu'ils soient personnels ou fournis par l'entreprise), et l'utilisation d'applications non-sécurisées se développe.

Les dirigeants s'estiment souvent au-dessus des règles, bien que visés par les cybercriminels ! Selon une étude publiée par MobileIron, 74% d'entre eux demandent de relâcher les mesures de sécurité mobile, 45% estiment qu'elles freinent l'utilisation de leur appareil. Et 37 % ont voulu accéder à des données professionnelles à partir d'une application non reconnue, tandis que 58 % la trouvent trop compliquée pour la comprendre.

Les usages évoluent : la tendance est de passer d'un SI central à un modèle cloud. Les utilisateurs organisent les espaces partagés et en sécurisent les accès, alors que la gestion des accès est traditionnellement mise en œuvre par l'équipe informatique.

Enfin, la charge de travail des équipes informatiques augmente : achat d'ordinateurs, installation de logiciels de sécurité, formation aux outils et aux bonnes pratiques de télétravail. La surveillance des activités à distance (les comportements changent, l'horaire de travail par exemple) crée de fausses anomalies dans les systèmes de détection.

Les équipes informatiques sont moins disponibles pour former et informer les utilisateurs des nouvelles menaces, pour compléter la liste des sites ou des mots-clés en «liste noire», et pour monitorer les accès distants.

Troisième raison : un manque d'outils et surtout des processus techniques inadaptés. Les processus techniques ont dû être adaptés à la nouvelle situation et ont pu créer des failles de sécurité : filtrages VPN, procédures de patch sur tous les équipements du SI (postes nomades, fixes, tablettes, smartphones, serveurs, équipements réseaux ou de sécurité, logiciels exposés sur Internet, solution de messagerie), extension temporaire des privilèges, configuration des équipements, politiques et fonctionnalités de sécurité, sauvegardes, contrôle de l'application des procédures.

Par ailleurs, les failles de sécurité peuvent provenir de la configuration des équipements utilisés, du wifi domestique, de la politique de mots de passe, du filtrage applicatif au niveau des pare-feux, de la gestion des autorisations (interne et externe !), du contrôle des accès et des flux, de la sécurisation des transferts de données, des systèmes de sauvegardes ou encore de la gestion des sessions utilisateurs. La gestion et les contrôles de l'ensemble de ces opérations de sécurité ne sont pas facilités par le travail à distance !

Vers une crise numérique ?

Le télétravail a créé des failles, qui ont déjà été exploitées ou seront exploitées (il faut donc se préparer à une crise numérique, après cette crise sanitaire !) et exige à la fois :

- A court terme, une vigilance accrue lors du retour dans l'entreprise : les postes de travail ont pu être infectés pendant le confinement et, avant de les reconnecter au SI de l'entreprise, il faudra contrôler les postes, auditer les systèmes, faire les mises à jour, changer les mots de passe, effacer les données stockées sur des supports personnels, supprimer des dérogations de sécurité, auditer la sécurité des fournisseurs et des sous-traitants critiques !
- A moyen terme, le lancement d'un programme cybersécurité, qui permettra le développement de ces nouveaux modes de travail de façon pérenne.
- A long terme, notamment pour des raisons de développement durable, les entreprises mettront en place une stratégie cyber. Ceci implique de comprendre les enjeux et les priorités, basés sur un audit et une cartographie des risques. Il s'agira de trouver le bon équilibre entre les outils et la technologie, ainsi qu'entre les processus et la gouvernance des données, pour transférer une partie des risques à l'assurance.

Marie de Fréminville est Présidente de Starboard Advisory et auteure de « La cybersécurité et les décideurs », Iste Editions. L'ouvrage a reçu le Prix du Livre cybersécurité 2020, décerné par le Forum International de la Cybersécurité (FIC) 2020.

TRANSFORMATION DIGITALE
Une année de télétravail et de services en ligne depuis le début de la Crise

Depuis maintenant plus d'un an, le monde est embarqué dans une crise qui perturbe le quotidien de nos entreprises, de nos administrations et du quotidien de tous les citoyens. Au cours de cette phase, nous avons assisté à la généralisation du télétravail dans les secteurs compatibles avec ce mode de travail. Et nous avons aussi été témoins de la naissance de pléthore de services en ligne pour compenser les difficultés, voire pour interdire les déplacements, au pire moment de la crise.

Salah Baïna
Consultant en transformation digitale

En mars 2020, et en l'espace de quelques jours, le terme accessibilité numérique a trouvé un écho mondial. Nous avons tous pu mesurer le degré d'accessibilité numérique de nos services essentiels. Paradoxalement, il est plus simple de s'abonner à vie à Netflix ou à Amazon Prime, que de retirer un document administratif ou de renouveler une assurance auto. Nous l'avons découvert à nos dépens.

Du fait de la Covid-19, nous avons découvert de nouvelles habitudes. Les mots télétravail, e-learning et webinaire font à présent partie de notre quotidien.

Le premier stage du programme d'acculturation accélérée au digital a ainsi été généralisé au printemps 2020.

Le digital, la priorité

La période que nous avons vécue est assez exceptionnelle. Elle est inédite dans l'histoire moderne de l'humanité. Personne n'était prêt à 100%, à l'échelle régionale comme à l'échelle mondiale. Selon les secteurs d'activités, le temps d'adaptation a été plus ou moins réduit. La bonne nouvelle, c'est que le télétravail et les services d'accueil des citoyens/clients ont permis, aux organisations publiques ou privées, d'atténuer l'effet néfaste de la crise.

Une chose est sûre, les organisations qui ne voyaient pas le digital comme une priorité ont compris, preuve à l'appui, qu'il n'y a plus de temps à perdre. Et que cela devient la priorité de toutes les priorités. Chaque service, qui n'a pas su s'adapter, a été remplacé par un substitut digital. Malheureusement, certains secteurs économiques n'ont rien pu faire face à l'arrêt des activités. Même en s'appuyant sur le digital et ses outils, les salles de cinémas sont fermées depuis mars 2020, des milliers d'avions sont cloués au sol et les villes touristiques attendent une clientèle qui tarde à venir. Certains secteurs sont tout simplement à réinventer car ils ne retrouveront plus jamais leurs formats d'avant.

Redéfinir la transformation digitale?

La transformation digitale, c'est tout simplement le fait de savoir tirer profit des nouvelles technologies de l'information et de la communication pour améliorer les performances des entreprises. Cela vaut pour les parts de marché et pour le rayonnement à l'échelle nationale et régionale.

Durant la crise, les entreprises ont changé leur façon d'interagir avec leurs collaborateurs et leurs clients en intégrant de plus en plus de technologies. La mobilité des uns et des autres incite les entreprises et les administrations à proposer de plus en plus de services en ligne, pour permettre à chacun d'y accéder en tout temps et en tout lieu et sur tout type de support. Banques, administrations, services de santé ou établissements d'enseignement… tout y passe ! Si la mobilité du client ne date pas d'aujourd'hui, c'est celle du collaborateur qui est en question avec le télétravail.

Les réunions en présentiel seront de plus en plus rares et le distanciel est bien parti pour changer durablement et irrémédiablement le fonctionnement des entreprises. Au-delà de la simple amélioration de la productivité, aujourd'hui, on assiste à la naissance et à l'épanouissement d'entreprises par excellence digitales. Des entreprises qui ont réussi à mettre le digital au cœur de leur fonctionnement.

Un grand nombre de secteurs s'est retrouvé face à des business modèles incompatibles avec le monde post-Covid. Il faut repenser l'entreprise dans sa globalité. Il est essentiel de redéfinir les missions, la chaîne de valeur de l'entreprise et surtout, de redéfinir le rôle et les compétences de chacun dans cette nouvelle version de l'entreprise. Avec un peu d'humour, on pourrait même parler de la crise de la *« quarantaine »* !

Une révolution digitale éthique et énergétique

Au Maroc comme ailleurs, nous avons tous vu, par exemple, comment nos écoles et le ministère de l'Education nationale se sont lancés dans le chantier de l'enseignement à distance, alors même que tous les prérequis n'étaient pas réunis. Et ce n'est qu'un exemple parmi d'autres. Je tiens d'ailleurs à saluer les hommes et les femmes de l'Education nationale et des établissements d'enseignement, en général, qui ont fait preuve d'agilité en s'adaptant à une situation inédite. Tout comme les DSI, qui ont fait de même avec ingéniosité pour répondre, dans des délais extrêmement courts, à des situations tout aussi inédites. C'est aussi ça le travail dans l'urgence. En tout cas, les feuilles de route Covid-19 sont par définition agiles…

La digitalisation, l'automatisation des processus, le télétravail, les portails de services en ligne et le e-commerce ont sûrement contribué à atténuer la crise. Cette prise de conscience est générale.

Avec cette première année sous le signe de la Covid-19, les responsables cherchent désormais des réponses concrètes et pragmatiques : *« Comment construire les feuilles de route de cette transformation digitale ? »* Le chantier n'est, d'ailleurs, pas seulement technologique. Il est stratégique, managérial et RH. Il est également et surtout humain. Il est aujourd'hui primordial de bien comprendre l'impact de cette transformation sur le quotidien de chacun de nous, dans nos organisations. Il faut accompagner le collaborateur dans cette compréhension et cette assimilation de la situation. Notre perception du monde qui nous entoure a changé. Nos usages également.

Aucun retour en arrière ne sera admis. Citoyens, clients, collaborateurs, managers… jusqu'au sommet de nos institutions, tout le monde va exiger de plus en plus de digital. Au Maroc, comme partout ailleurs en Afrique et dans le monde, des lois ont été amendées, d'autres ont été votées dans l'urgence. Des plateformes ont vu le jour en quelques mois afin de mieux répondre aux nouvelles exigences et aux nouveaux usages du digital. Si certains craignent, peut-être, que la vague de transformation ne s'arrête avec la disparition du virus, je me permets d'être plus optimiste !

La fin de la Covid-19 sonnera peut-être la fin de la transformation, sous la pression et l'urgence. Nous aurons enfin le temps pour penser une transformation à plus long terme. Et une transformation qui prenne également en considération d'autres contraintes. Des contraintes durables, éthiques, énergétiques. Des contraintes sociales et sociétales. Tout le monde a goûté aux fruits du digital. Gageons que cette révolution s'accentuera encore plus dorénavant et que rien ne pourra l'arrêter !

Spécialiste des Nouvelles technologies de l'information et de la communication, ainsi que du Management de l'innovation, **Salah Baïna** est docteur de l'Université de Lorraine (France). Il est également, diplômé de l'École nationale supérieure d'informatique et mathématique appliquée (ENSIMAG) de Grenoble (France).

LA RÉFÉRENCE DU NUMÉRIQUE EN AFRIQUE

cio mag.com

2021

CALENDRIER ÉDITORIAL

Janvier-Février-Mars 2021

Cio Mag 68 : Quel avenir pour la TNT en Afrique ?

Avril-Mai-Juin 2021

Cio Mag 69 : Télétravail et cybersécurité : quelles réponses face aux nouveaux défis ?

Juillet-Août-Septembre 2021

Cio Mag 70 : Le digital, formidable accélérateur pour l'atteinte des ODD. Focus sur 5 secteurs prioritaires pour l'Afrique.

Dossier Pays : Côte d'Ivoire : Quelles réformes et quel soutien aux acteurs du numérique pour libérer le plein potentiel de croissance ?

Octobre-Novembre-Décembre 2021

Cio Mag 71 : Blockchain : Cinq secteurs d'application pour l'Afrique

Dossier pays : Bénin : Enquête sur les ambitions pour devenir la plateforme des services numériques de l'Afrique de l'Ouest.

Hors-séries

Afrique : Jeunesse, innovation et entreprenariat - *Juillet 2021*

Enquête : Mobilité et africanisation des talents et des compétences, les nouveaux défis des multinationales - *Novembre 2021*

LES E-CONF CHALLENGES DE CIO MAG

Mars 2021

01 **Webinaire : IA, Télétravail et Cybersécurité**

Thème : Entre tendance et résilience, quelles préconisations?

Avril 2021

02 **Webinaire : L'innovation et l'entrepreneuriat pour soutenir la croissance**

Thème : Le Digital, formidable accélérateur pour l'atteinte des ODD (Objectifs de Développement Durable)

Juillet 2021

03 **Webinaire : Blockchain et finances publiques**

Thème : Blockchain, 5 secteurs d'application pour l'Afrique

Décembre 2021

04 **Webinaire : Mobilité et africanisation des talents et des compétences, les nouveaux défis des multinationales**

Thème : Présentation du Top 50 des personnalités qui font le numérique en Afrique

LA RÉFÉRENCE DU NUMÉRIQUE EN AFRIQUE

Oui, je souhaite m'abonner

Afrique subsaharienne

☐ 1 an	47 500 FCFA /73 €
☐ 2 ans	95 000FCFA /145 €
☐ 3 ans	142 500 FCFA /217 €

Europe et Maghreb

☐ 1 an	42 500 FCFA /65 €
☐ 2 ans	85 000FCFA /130 €
☐ 3 ans	127 500 FCFA /195 €

Dom-Tom et reste du monde

☐ 1 an	50 000 FCFA /77 €
☐ 2 ans	100 000 FCFA /154 €
☐ 3 ans	150 500 FCFA /231 €

*Frais de port inclus dans le prix

Nom ..... Prénom .....

Société ..... Fonction .....

Adresse de livraison .....

Boîte postale .....

Code postal ..... Ville ..... Pays .....

Tél. ..... Fax .....

E-mail .....

Je règle la somme de ..... €

☐ Chèque de banque à l'ordre de SAFREM Sarl

☐ Transfert bancaire (BNP Paribas Paris.

IBAN : FR76 3000 4029 3300 0100 3689 160 - BIC : BNPAFRPPPCE

Bulletin d'Abonnement à retourner à :

SAFREM Sarl - 23 Rue Colbert 78180

Saint-Quentin en Yvelines France

Tél : +33 1 30 64 80 24 / cio@cio-mag.com

http://www.cio-mag.com/sabonner

Date et signature

L'exploration
nous éclaire sur la voie à suivre

La recherche constante de l'innovation est un gage d'éclairage pour le monde intelligent

HUAWEI