FÉVRIER-MARS 2023

cio mag.com

LA RÉFÉRENCE DU NUMÉRIQUE EN AFRIQUE

CYBERSÉCURITÉ

Lutter contre les vulnérabilités pour impulser l'économie numérique

www.cio-mag.com

N°78

SOMMAIRE

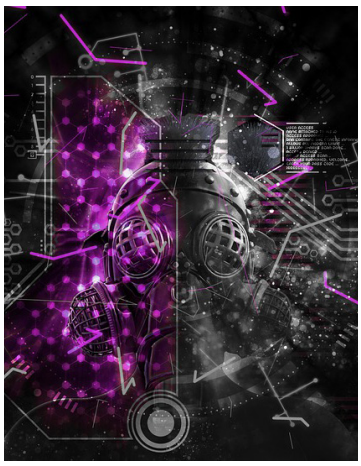
N°78 Février - Mars 2023

cio mag.com

LA RÉFÉRENCE DU NUMÉRIQUE EN AFRIQUE

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 :
Anselme Akéko (Côte d'Ivoire);
Adil Abdelali (Maroc);
Michaël Tchokpodo (Bénin);
Souleyman Tobias (Togo);
Enock Bulonza (RDC); Zoheir Zaid (Algérie); Junie Maffock (Cameroun)
Représentations de Cio Mag :
Côte d'Ivoire : Anselme Akéko :
anselme.Akéko@cio-mag.com
Tél: +225 05 55 464 994
Sénégal : Abdoulaye DIALLO :
abdoulaye33@hotmail.com
Tél : +221 775 955 002
Togo : Souleyman TOBIAS :
tobias.carlos@cio-mag.com
Tél : +228 902 638 54
Bénin : Michaël TCHOKPODO :
michael@cio-mag.com
Tél : +229 961 508 03
RDC : Enock BULONZA :
enock@cio-mag.com
Tél : +243 978 947 252
MAROC : ADIL ABDELALI :
adil.abdelali@cio-mag.com
Tél : +212 637 898 264
Régie Publicitaire et Abonnements :
info@cio-mag.com
www.cio-mag.com/sabonner

Direction artistique : Cio Mag
N° Commission paritaire 1110 T89651
N Dépôt légal Juin 2013



DOSSIER CYBERSECURITÉ

ÉDITO

Mohamadou DIALLO
Fondateur et Directeur
Général de Cio Mag

Cio Mag migre vers le 100% digital pour mieux servir ses lecteurs

2008-2023, cela fait quinze bonnes années que Cio Mag a vu le jour. Années durant lesquelles nous avons accompagné, en tant que Grand témoin, la transition numérique qui s'opérait sous nos yeux. L'on me demande souvent le secret de cette longévité d'un média de niche, qui plus est géographiquement circonscrit. La réponse se trouve dans la justification de l'existence de notre média par les acteurs qui, à l'époque, avait senti le vide autour de l'information africaine par les Africains et pour les Africains. Pour rappeler le contexte, à l'époque, les connexions internet étaient balbutiantes, voire inexistantes dans certains pays, et les réseaux sociaux n'avaient pas encore fait leur apparition. Au fil des années, nous avons su faire un savant mélange qui nous a permis de jouer sur la grande proximité, volontairement créée, avec nos lecteurs que nous rencontrions régulièrement à l'occasion des Digital African Tour ou des Assises de la transformation digitale (ATDA). Cette proximité a créé, par essence, des relations privilégiées avec nos lecteurs que nous connaissons, établissant ainsi, de manière symétrique, des échanges francs et directs. Après avoir traversé tant d'évènements, il est venu le temps d'opérer des changements majeurs pour, justement, consolider cette proximité.

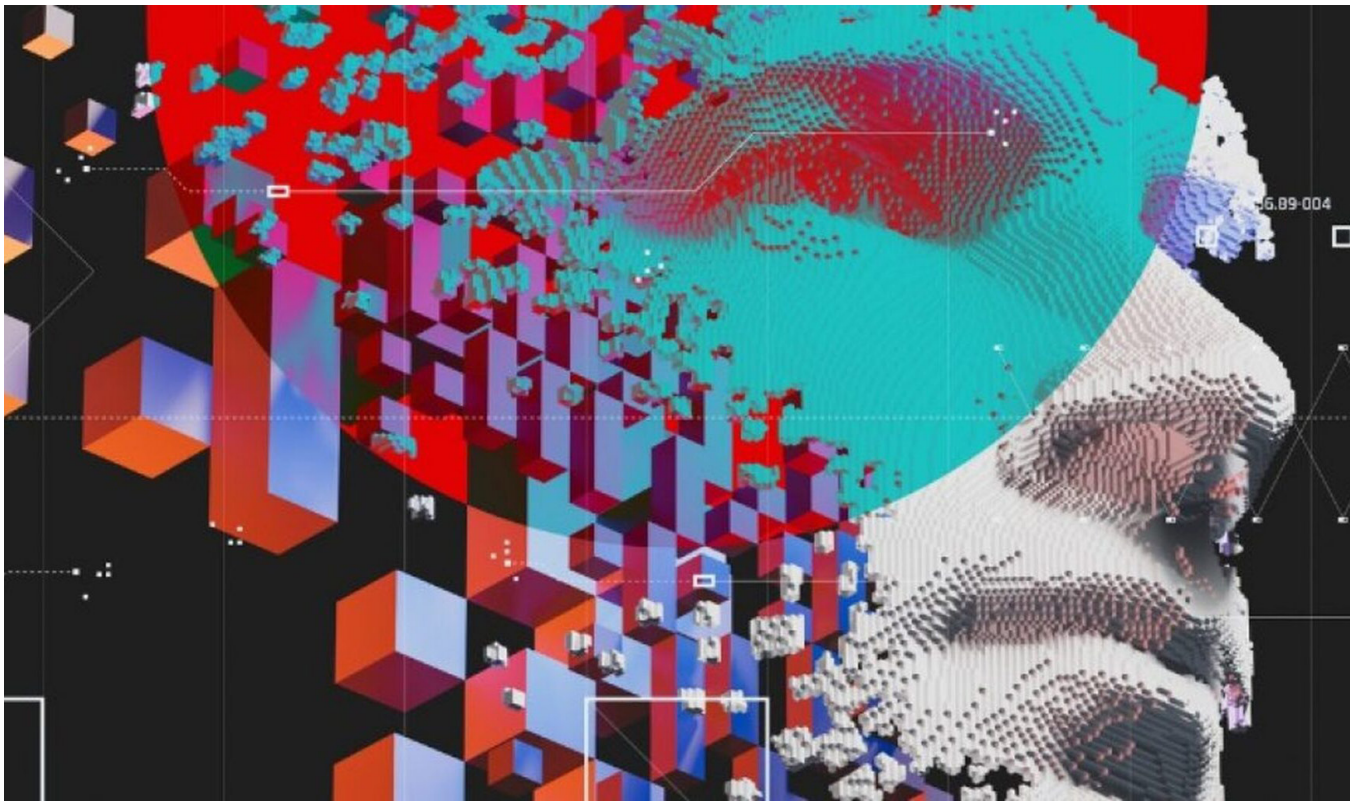
Interactivité, commodité et temps réel

De plus en plus, nos lecteurs nous indiquent leur préférence à acheter un exemplaire numérique plutôt qu'un support papier. De ce fait, pour justifier notre passage à l'ère numérique, nous avons identifié cinq bonnes raisons qui président à ce choix majeur. Il s'agit d'une orientation qui, au-delà des simples coûts d'impression, d'expédition et des délais de livraison, certes majeurs, émane surtout du besoin de créer, en permanence, plus de proximité et d'instantanéité avec les lecteurs. En effet, à l'ère de la 4e révolution industrielle, les lecteurs sont de plus en plus exigeants et s'attendent à être informés en temps réel. L'avantage avec ces procédés est que vous avez la possibilité de consulter vos flux d'informations à n'importe quel moment de la journée. Surtout, vous pouvez vous rendre sur ces plateformes depuis le confort de votre maison ou à n'importe quel autre endroit. Une fois établi, on peut alors créer de l'Interactive. Les magazines en ligne offrent plus d'interactivité (envois vers des liens d'articles, de rapports, d'études pour pousser la réflexion). Mais ils permettent également de partager plus facilement des articles intéressants sur des plateformes de médias sociaux en un seul clic ou de donner votre avis dans la section des commentaires. Cela se traduit également par la commodité dans les usages. Les magazines commerciaux en ligne offrent une connaissance du marché et une image claire de votre marché cible. Vous vous informez commodément des tendances commerciales et des derniers développements, où que vous soyez. Les magazines numériques en ligne favorisent des opportunités commerciales grâce à des prévisions pour l'avenir. L'offre de l'ensemble de ces avantages est aussi à corréler avec les bénéfices économiques à la fois pour le lecteur et pour notre média.

De ce fait, il n'est plus à démontrer que la digitalisation, considérée à juste titre comme une « quatrième révolution industrielle », est créatrice d'opportunités économiques et sociales majeures, mais apporte aussi des changements sans précédent dans nos habitudes, nos modes de vie et nos relations en société. Grâce au numérique, on peut communiquer avec nos proches, travailler à distance, optimiser nos déplacements et avoir accès à des services en ligne. Ces phénomènes de transformation universels qui se diffusent rapidement dans la plupart des sphères d'activité sont également à l'œuvre dans les médias et Cio Mag n'échappe point à cette règle.

Bonne lecture ■

#contact
mohamadou.diallo@cio-mag.com
www.cio-mag.com



INTERNATIONAL

Quelles tendances en 2023 ?

À quels types de cyberattaques faut-il s'attendre en 2023 ? Les chercheurs des entreprises spécialisées en cybersécurité ont établi de probables risques cyber qui pourraient affecter les personnes, les entreprises, les organismes gouvernementaux et financiers en 2023. Synthèse.

Michaël TCHOKPODO

Des chiffres collectés pêle-mêle, il ressort du rapport 2021 du FBI sur l'état de la cybercriminalité dans le monde que 847 376 plaintes ont été recueillies pour « crimes sur Internet. » Lesquelles ont coûté 6,3 milliards d'euros (soit 6,9 milliards de dollars) au monde. Sur le même sujet, Alessandro Profumo, patron du géant italien de l'aéronautique et de la défense, a assuré à l'ouverture du Rome Cybertech Europe 2022 que la cybercriminalité aurait coûté plus de 6000 milliards de dollars (soit 5.700 milliards d'euros) au monde.

Les experts de Kaspersky ont eux aussi livré leurs analyses. D'après eux, en 2021, la cybercriminalité a réduit de plus de 10% le produit intérieur brut (PIB) du continent africain, estimé à 4,12 milliards de dollars. Et 70% des attaques subies par les entreprises relèvent des tentatives d'hameçonnage alors que sur le continent, plus de 90% d'entre elles opèrent sans utiliser les protocoles de cybersécurité nécessaires. Si cette tendance se poursuit, les menaces auxquelles les entreprises seront sujettes vont davantage s'amplifier en 2023.

Suivant les prédictions de cette année, se profilent avec insistance des menaces en matière APT, des menaces relatives à la confidentialité des données et financières. Et en l'occurrence, des menaces pour les entreprises et le grand public. *« Les bouleversements politiques de 2022 ont provoqué des changements qui vont avoir des répercussions sur les enjeux de cybersécurité pour les années à venir, et qui vont influencer le développement des futures attaques sophistiquées »,* avait prévenu Bertrand Trastour, Directeur général de Kaspersky France & Afrique du Nord, de l'Ouest et Centrale.

Les menaces à anticiper

En novembre 2022, Kaspersky Security Services publiait Kaspersky Security Bulletin (KSB), sa série annuelle de prédictions et de rapports analytiques sur les changements clés dans le monde de la cybersécurité. Elle a insisté, au titre des menaces persistantes avancées (APT), sur le prochain WannaCry et les drones pour le piratage de proximité. Selon les statistiques, les cyber-pandémies les plus remarquables se produisent à intervalle de 6 à 7 ans. Si la dernière en date, qui remonte au 11 mai 2017, porte sur le ransomware auto-répliquant WannaCry ayant exploité une vulnérabilité d'EternalBlue, il y a de fortes chances qu'une telle attaque se répète, surtout au regard des tensions politiques mondiales qui ne sont pas prêtes de s'apaiser.

Le piratage de proximité à l'aide des drones peut se traduire par des intrusions physiques et informatiques. Il peut donc arriver que ces appareils volants lâchent des clés USB malveillantes dans des zones à accès limité, dans l'intention qu'un passant les ramasse et les branche sur une machine. Parmi ces menaces avancées, sont attendues en 2023 : les logiciels malveillants délivrés par le SIGINT, l'essor des attaques destructrices et les serveurs de messagerie comme cibles prioritaires. Il est aussi redouté les APT visant des technologies, des producteurs et des opérateurs satellitaires, le Hack-and-leak comme étant le nouveau black et un nombre croissant de groupes APT qui passeront de CobaltStrike à d'autres outils.

Leader technologique dans la détection des cybermenaces, Gatewatcher voit les choses autrement. Pour cette entreprise, 5 prédictions majeures sont susceptibles de caractériser l'année 2023 en matière de cybersécurité. D'une part, elle annonce la recrudescence des cyberattaques par malwares et l'investissement des entreprises dans les solutions de détection des menaces sur le réseau afin de répondre à l'évolution constante des cybermenaces.

D'après ses experts, le secteur de l'industrie pourrait désormais subir une quadruple extorsion, à savoir : le chiffrement de données et des demandes de rançons, le vol de données suivi de la vente sur le dark web, le déni de Service pour amplifier la pression, l'arrêt et la prise de contrôle de l'outil de production.

À en croire Gatewatcher, 2023 sera une année de prise de conscience des dirigeants quant à l'impact d'une cyberattaque sur le business. Enfin, conclura-t-elle, l'évolution du cadre réglementaire viendra renforcer les actions déjà engagées et les règles en matière de cybersécurité.

" La menace évolue rapidement"

« Le paysage des menaces est devenu de plus en plus volatil, réitère le rapport du Global Security Outlook 2023. Les groupes cybercriminels professionnalisés ont continué de croître et de créer un volume plus élevé de nouveaux types d'attaques. La volatilité n'est pas seulement risquée. Le temps nécessaire à l'élaboration d'une réponse crée un coût d'opportunité pour la cybersécurité d'une Organisation d'experts. Les équipes de cybersécurité se sentent parfois obligées d'ignorer les activités stratégiquement importantes pour traiter des problèmes tactiques immédiats. »

Ces défis, les directeurs des systèmes d'information (DSI) y sont souvent confrontés. Début janvier 2023, Kaspersky a révélé de nouvelles tendances cybersécuritaires qui devront s'observer en 2023. D'après ces experts, la stratégie selon laquelle les cybercriminels annoncent publiquement avoir attaqué le système d'une entreprise et donnent un compte à rebours avant la publication des informations volées pourrait se poursuivre cette année.

Mieux, les cybercriminels vont continuer à faire croire à de fausses fuites. L'objectif consiste non seulement à renforcer leur notoriété à travers l'intérêt des médias envers leurs attaques, mais surtout à nuire à la réputation d'une entreprise ou d'un pays. En plus de ces cibles, les individus pourraient également subir des vols de données à caractère personnel à condition que des renseignements sensibles, à l'instar des adresses e-mail, deviennent accessibles au public. Ces données peuvent donc être exploitées à des fins d'hameçonnage et d'ingénierie sociale. Un autre point important, c'est le Malware-as-a-service, les attaques via le cloud et les données pouvant être compromises à partir du dark web.

Comment se protéger ?

Alors que les cyberattaques peuvent prendre des proportions inimaginables, l'économie d'Internet devra constituer l'avenir en Afrique. Selon la Société financière internationale et Google, cités par l'économiste camerounaise Vera Songwe, cette économie devrait contribuer à hauteur de 180 milliards de dollars à l'économie globale du continent d'ici à 2025, pour atteindre 712 milliards de dollars en 2050. Un gain colossal pour insuffler une nouvelle dynamique aux économies africaines.

> *« Le paysage de la menace évolue rapidement et les entreprises n'ont pas d'autre choix que de s'y adapter »,*

fait remarquer Bertrand Trastour avant de préconiser : *« afin de protéger une grande entreprise ou un organisme gouvernemental contre les menaces en vogue, il est nécessaire de surveiller son empreinte numérique. Il est important d'être prêt à enquêter et à intervenir en cas d'incident, car il n'est pas toujours possible de bloquer les cyberattaquants avant qu'ils ne pénètrent le périmètre de l'organisation. Cependant, empêcher le développement d'une attaque et limiter les dommages potentiels est une tâche absolument faisable. »*

Gatewatcher propose diverses solutions aux entreprises : *« Afin d'identifier les faiblesses de leur SI et de leur surface d'exposition à la menace, les entreprises devraient mettre en place des audits réguliers et adopter les bonnes pratiques de patch management. Investir davantage dans les ressources humaines et dans les technologies leur permettra également d'avoir une vision plus complète de leur SI. »*

Elle insiste néanmoins sur l'évolution du cadre réglementaire en matière de cybersécurité. Dans le contexte européen, deux législations sont envisagées : la directive NIS2 et le règlement européen Cyber Resilience Act.

« La directive NIS2, qui se substituera à la présente directive NIS, imposera aux acteurs économiques de toutes tailles la mise en place des mesures plus strictes de cybersécurité. Quant à la loi sur la cyber-résilience (Cyber Resilience Act), elle viendra renforcer les règles en matière de cybersécurité. Une telle réglementation pourrait créer un véritable cadre de confiance qui impacterait aussi les fabricants d'objets connectés », précise le rapport.

Pour les chercheurs de Kaspersky, l'un des moyens pour protéger une organisation contre les menaces serait de toujours garder les logiciels de tous les appareils utilisés à jour. Une méthode pour empêcher les cybercriminels d'infiltrer le réseau en exploitant les vulnérabilités existantes. À force de développement, les menaces vont toujours exister. Il serait toujours préférable de les anticiper afin de réduire les coûts et les dégâts qu'elles peuvent engendrer ■

ANALYSE

« Les changements de nos comportements en ligne rendront plus floue la frontière entre mondes physique et virtuel »

Benoît Grunemwald, expert Cybersécurité ESET

Les attaques cybers ne connaîtront pas de trêve en 20223 ! Elles s'intensifieront et évolueront au rythme des usages. Pire, les cybers attaquants resteront dans l'anticipation. Alors que les usages tournent de plus en plus vers le cloud, Benoit Grunemwald, Expert cybersécuirté ESET attire notre attention sur les enjeux. « Autant la popularité des services dans le Cloud ne faiblit pas, autant l'intérêt des attaquants ne faiblit pas non plus », rappelle-t-il. Projection sur l'année 2023 !

INTERVIEW

Cio mag : Quelles sont les (nouvelles) menaces (apparues) avec la crise économique que traverse le monde, surtout pour les entreprises ?

B.G : les attaques menées contre les entreprises ont notamment eu comme conséquence l'indisponibilité et la fuite de données, accrues par les rançongiciels. Avec la crise économique actuelle, la concurrence est à son paroxysme et l'économie mondiale est tendue. Ce n'est donc pas le bon moment pour que le système d'information de l'entreprise soit indisponible, quelle qu'en soit la cause : une attaque cyber ou une défaillance. Parce qu'en réalité lorsque cette situation se présente, les clients et prospects se tourneront vers d'autres fournisseurs ou saisiront l'occasion pour négocier les prix en leur faveur.

De même, il faut souligner que dans ce contexte global de crise, les règles de la concurrence loyale sont mises à rude épreuve. Ainsi, l'espionnage industriel, permettant de tirer parti des découvertes des concurrents et de limiter potentiellement les dépenses de R&D, se pratique. L'utilisation des réseaux sociaux est mise à contribution, en complément du traditionnel message d'hameçonnage. Les équipes d'ESET ont pu identifier, en 2022, plusieurs menaces perpétrées par des groupes bien organisés. Nous avons publié un rapport résumant l'ensemble de ces menaces.

Comment la cybersécurité peut-elle participer à la résilience des entreprises dans un contexte de relance après cette crise économique ?

B.G : Le premier challenge est d'assurer la reprise de production face aux risques de non-disponibilité du système d'information. En mettant en place les dispositifs optimaux de cybersécurité, l'entreprise peut garantir la protection de ses données stratégiques, mais aussi celles détenues sur ses clients. Ce qui signifie que dans l'entreprise, il y a une politique de respect de la conformité et de la confiance, ce qui lui donne un avantage concurrentiel.

Quelles solutions ESET met-elle à la disposition des entreprises pour les accompagner dans leur cyber résilience post crise économique ?

B.G : Les solutions de cybersécurité ont bien évolué depuis 30 ans. Elles s'appuient de plus en plus sur l'IA et le cloud, faisant face au nombre croissant et à la complexité des menaces ; vulnérabilités et comportement des attaquants. Au traditionnel et toujours nécessaire antivirus, il convient d'ajouter des outils de surveillance et de recherche de nouvelles formes de menaces : la Sandbox Cloud pour révéler les logiciels malveillants encore inconnus, l'EDR pour détecter les comportements suspects, la Cyber Threat Intelligence pour comprendre et se défendre contre les larges volumes d'attaques ou au contraire les attaques très ciblées.

2023 s'annonce avec de nouveaux défis. Quels sont ceux répertoriés par ESET pour la cybersécurité de ses partenaires ?

B.G : Les frontières entre travail et vie privée deviennent de plus en plus étroites, à cause du télétravail et de la vie numérique. Cette réalité a pour conséquence l'accroissement de l'exposition aux attaques. Parce qu'il est important de rappeler que tout ce qui devient populaire le devient également pour les criminels. Cela vaut pour les plateformes dans le Cloud. Les cyberattaques contre le Cloud représentaient 20 % de toutes les cyberattaques en 2020. Autant la popularité des services dans le Cloud ne faiblit pas, autant l'intérêt des attaquants ne faiblit pas non plus.

Alors quelles perspectives cybers sécuritaires pour 2023 ?

B.G : ESET prévoit qu'en 2023 les changements de nos comportements en ligne, tant dans notre vie professionnelle que personnelle, rendront encore plus floue la frontière entre le monde physique et le monde virtuel. L'étendue des applications cloud offre des possibilités infinies de créer, collaborer, acheter, vendre ou jouer. Supplantant les limitations initiales du cloud, les technologies actuelles libèrent les utilisateurs du coût de possession du matériel et de la gestion des mises à jour. Mais lorsque nous aurons tout basculé sur le Cloud, quels risques nous attendent ?

Quelle que soit la manière dont nous en sommes arrivés là (certainement aidés par les confinements dus à COVID-19), nous y sommes maintenant ! Il est probable qu'aujourd'hui même, nous soyons connectés à notre environnement préféré dans le Cloud. Il s'agit ici d'environnements numériques à grande échelle dans le

Cloud, tels que Discord, Slack et Microsoft Teams. Nous pourrions inclure de nombreuses applications sociales comme Facebook, WhatsApp, LinkedIn et Tinder, ou même des jeux comme Fortnite et Valorant. Il en existe trop pour les énumérer, mais tous prévoient une même réalité : des millions d'utilisateurs se forgent une vie hybride et révisent notre définition de la sécurité et de la confidentialité. Cette floraison d'environnements dans le Cloud offre des possibilités inimaginables de créer, collaborer, acheter, vendre et jouer.

Dépassant l'étendue des précédentes technologies Cloud, qui ont d'abord libéré les utilisateurs des limitations liées aux coûts du matériel et des longs intervalles entre les mises à jour. Les environnements Cloud actuels offrent des possibilités hybrides transformatrices. Et alors que nous avons tout misé sur le Cloud, il est impératif de prendre la mesure des enjeux de la cybersécurité ■

Propos recueillis par Souleyman Tobias

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

Didier Simba, président du Club d'experts de la sécurité de l'information en Afrique

FOCUS

Stratégie ou stratégies africaine(s) ?

Avec environ 850 millions d'internautes en 2022, l'Afrique continue d'améliorer son taux de connectivité. Cette progression s'accompagne fort malheureusement des cybermenaces. Sur le continent, les politiques de transformation digitale n'ont pas forcément anticipé la sécurisation du cyberespace. Même si, par la suite, de nombreuses initiatives sont prises pour doter le continent d'un référentiel en matière de cybersécurité, du chemin reste à parcourir. Et pour cause, l'hétérogénéité des stratégies, chaque pays étant excessivement jaloux de sa souveraineté numérique.

Souleyman TOBIAS

Construire un écosystème numérique de confiance partout sur le continent reste un vaste chantier. Cela nécessite la mise en place de mesures juridiques appropriées, les ressources humaines qualifiées, les ressources financières nécessaires et bien d'autres dispositifs comme des cadres de coopération faites de confiance entre différents acteurs.

En 2015, la première session du Comité technique de l'UA spécialisé sur la communication et les technologies (STC-CICT-1) a relevé *« qu'il existe un besoin urgent de développer une approche globale et une stratégie cohérente en matière de cybersécurité au niveau continental pour promouvoir la paix et la sécurité dans la société de l'information »*. Un an après l'adoption de la Convention de Malabo (2014), le STC-CICT-1 a donc formulé plusieurs recommandations à l'endroit des Etats africains pour la cybersécurité. L'approche recommandée par le Comité technique reposait sur plusieurs points. Elle devrait être stratégique, avec notamment *« l'harmonisation des législations nationales, les règlements, les normes et lignes directrices »* pour créer *« des cadres régionaux et internationaux efficaces pour lutter contre la cybercriminalité »*.

Dans l'édition 2022 du *« Baromètre de la cybersécurité en Afrique »*, une étude du Club d'experts de la sécurité de l'information en Afrique (CSIA), Didier Simba, le président du Club, parle d'une *« disparité à travers les Etats africains en matière de maturité en cybersécurité »*.

Et pourtant, les cybermenaces causent d'énormes pertes au continent. La transformation digitale tous azimuts en cours en Afrique porte donc en elle-même les germes de la recrudescence des actes criminels en ligne. Face à cette réalité, les Etats africains n'ont pas d'autres choix que de faire de la cybersécurité une priorité au même titre que la sécurité physique de leurs territoires.

Des défis communs

En 2021, le rapport d'évaluation des cybermenaces en Afrique publié par Interpol illustre le caractère transfrontalier de la cybercriminalité. Trois présumés cerveaux d'un vaste réseau de cybercriminels ont été arrêtés en novembre 2020, à Lagos au Nigeria, à la suite d'une enquête conduite par Interpol, en collaboration avec Group-IB et la Police nigériane. Leurs activités ont pu compromettre les systèmes d'entreprises publiques et privées dans plus de 150 pays depuis 2017, selon Interpol. La menace n'épargne aucune région du continent et se chiffre à plusieurs dizaines de milliards US. Africa Cybersecurity Market l'estimait à 2,32 milliards pour 2020. Interpol, dans son rapport de 2021, indiquait qu'*« en tant que région embrassant la transformation numérique, l'Afrique doit investir massivement pour améliorer la sécurité et la sûreté du cyberespace »*. L'organisation internationale de la Police a souligné qu'*« en raison de la nature très changeante et transnationale de la cybercriminalité, seule une réponse coordonnée et rapide permet de la combattre efficacement »*.

Franck Kié, consultant en cybersécurité

Des stratégies peu «ouvertes»

Pour Didier Simba, Président-fondateur de CESIA (un réseau africain de professionnels de la sécurité numérique, avec près de 180 membres dans 18 pays en Afrique), *" l'idéal serait de parler de stratégie africaine "*, mais force est de constater que nous avons des *" stratégies africaines "*. Un constat qui s'explique par *" des stratégies géopolitiques "*. L'expert en cybersécurité estime que la prise de conscience est réelle, mais le manque de collaboration demeure la faille des pays. Même s'il y a *« un décalage de prise de conscience des enjeux de la cybersécurité entre les différents pays »*, la brèche, poursuit le RSSI, c'est le fait que *« chaque pays définit et met en œuvre une stratégie nationale de la cybersécurité, laquelle est propre au contexte du pays concerné et aborde peu, voire pas du tout, la collaboration avec les autres pays ».*

Le même constat ressortait dans le *« Global Security Index 2020 »* publié par l'Union internationale des Télécoms. L'étude portait sur 44 pays africains. Parmi eux, 32 n'avaient aucun accord bilatéral sur la cybersécurité et seulement 19 avaient signé ou ratifié des accords multilatéraux. Une tendance que Didier Simba explique par *« la priorité réservée à la sécurité de l'État »*, entraînant la peur des Etats de *« divulguer des données ayant un impact sur la sécurité nationale des pays ». « Le frein de la collaboration pour une stratégie africaine est là »,* soutient Didier Simba.

Pour Franck Kié, Consultant en cybersécurité et Associé gérant de Ciberobs (plateforme sur la cybersécurité en Afrique), il y a toutefois une prise de conscience au plus haut niveau sur ce sujet. Cependant, il existe toujours des défis comme *« la mise en place de la régulation et la gouvernance adéquate, l'investissement dans des infrastructures et solutions à niveau pour répondre aux attaques, mais aussi la nécessité d'avoir une main-d'œuvre locale disponible »*, indique-t-il. Le Commissaire général de Cyber Africa Forum (plateforme de référence réunissant chaque année des acteurs clés du public et du privé) propose, face à ces défis, l'actualisation de la Convention de Malabo. Comme le Cyber Africa Forum, Franck Kié rappelle qu'il existe d'autres initiatives pour amener le continent à faire bloc face aux cybercriminels. Il évoque en exemple la Déclaration de Lomé issue de la Conférence sur la cybersécurité qu'a abritée le Togo en mars 2022.

Les bons signaux

La prise de conscience est le premier bon signal que notent les experts. La Conférence de Lomé *« permet au pays non seulement de réunir les experts du monde entier pour débattre du sujet, mais aussi et surtout de définir une feuille de route nationale de cybersécurité »*, analyse Didier Simba. Pour ce dernier, les bonnes tendances sont plutôt des dynamiques sous-régionales. C'est d'ailleurs ce qui ressort dans le *« Baromètre de la cybersécurité en Afrique »* publié par le CESIA, explique-t-il.

Toutefois, selon le Global Security Index 2020 de l'UIT (GCI-2020), l'Île Maurice reste le meilleur exemple du continent. Avec un score de 96.89 sur 100, le pays se positionne comme le 1er dans la mise en place des différentes mesures sur lesquelles portait l'enquête, à savoir : les mesures juridiques (19.27/20), techniques (20/20), organisationnelles (18.38/20), le renforcement des capacités (19.54/20) et les mesures de coopération (19.70/20). En ce qui concerne notamment les mesures techniques, le pays dispose donc, entre autres, de l'ensemble des organes et mécanismes nécessaires identifiés par l'UIT pour la prévention, la lutte et la sensibilisation contre la cybersécurité.

Selon Franck Kié, *« aujourd'hui, il y a de plus en plus de pays africains qui sont à la pointe sur ces sujets. La dynamique est en bonne voie. Il y a une coopération régionale et sous-régionale qui s'accroît »*. Le Commissaire général de Cyber Africa Forum se réjouit de voir *« des pays émergents comme le Bénin, le Togo, la Côte d'Ivoire prendre le leadership sur ces sujets en proposant des solutions et initiatives ».*

À l'instar du Bénin (6e au rang africain et 1er en Afrique francophone et de l'Ouest, selon le GCI 2020), la prise de conscience des pays africains se traduit par la mise en place de plusieurs dispositifs comme les stratégies nationales de sécurité

numérique. Un outil pour construire la confiance numérique. Face à l'économie de la cybercriminalité, le Bénin encourage par exemple la promotion d'une économie vertueuse et la coopération.

Selon les données de cette enquête de l'UIT récoltées dans 44 pays africains, seule une dizaine de pays totalisent une note globale au-dessus de 50 points sur 100. Il s'agissait de l'Afrique du Sud, du Bénin, du Botswana, de la Côte d'Ivoire, du Ghana, du Kenya, du Nigeria, de la République de Maurice, de l'Ouganda, du Rwanda, de la Tanzanie et de la Zambie. Mais plusieurs pays améliorent depuis leurs arsenaux. Le Togo par exemple a, dès 2021, pensé à la domestication de ses données critiques. Le pays s'est donc doté d'un Datacenter Tiers III, l'un des tout premiers de la sous-région. Tout en renforçant son arsenal juridique et les capacités techniques, le pays fait de la sensibilisation de masse à travers son Agence nationale de la Cybersécurité (ANCy) et Cyber Défense Africa, une joint-venture public-privé, fer de la lance de la stratégie de riposte du pays. Comme au Togo, les équipes d'intervention informatique d'urgence (CERT), de sécurité et d'intervention en cas d'incident informatique (CSIRT) sont désormais opérationnelles dans une vingtaine de pays.

La Côte d'Ivoire peut être citée comme l'un des pays de la sous-région ouest-africaine à prendre très tôt la protection de son cyberespace au sérieux. Dans l'optique de freiner la prolifération des brouteurs (terme ivoirien pour désigner les cyberarnaqueurs), la Côte d'Ivoire a mis en place, dès les années 2010, des mesures de contre-offensives. Le pays s'est doté, en 2011, d'une plateforme de lutte contre la cybercriminalité (PLCC). Fin 2021, le Colonel Moussa Guelpétchin Ouattara, le Directeur de l'Informatique et des Traces technologiques (DITT) a annoncé que la PLCC traitait entre 4500 et 5000 plaintes par an. En 2013, le pays s'est doté d'une loi contre la cybersécurité et continue d'améliorer son arsenal dont une stratégie nationale de cybersécurité 2020-2025.

Lors de la 8e édition du Forum international de Dakar sur la paix et la sécurité en Afrique, en octobre 2022, le président sénégalais Macky Sall a estimé que les dérives du numérique menacent la paix, la sécurité et donc la stabilité des Etats africains. Le pays dispose d'une stratégie nationale de lutte contre la cybercriminalité parmi les mieux élaborées, estiment des chercheurs du Centre d'études stratégiques pour l'Afrique. Dans leur publication intitulée *« Leçons d'Afrique en matière de cybersécurité »*, Abdul-Hakeem Ajijola (expert en cybersécurité et président du groupe d'experts en cybersécurité de l'Union africaine) et Nate Allen (professeur adjoint d'études de sécurité au Centre d'études stratégiques de l'Afrique) ont déclaré que *« les stratégies nationales de cybersécurité de trois pays africains seulement, Eswatini, Kenya et Sénégal, répondent aux critères minimaux essentiels ».*

Selon les deux chercheurs, ces critères portent sur l'évaluation des menaces pour mesurer l'ampleur des cybermenaces, l'élaboration d'un plan d'action qui fixe les objectifs et les actions concrètes à mener ; une planification des actions, la répartition claire des rôles des parties concernées et une affectation précise de budget. Aussi, recommandent-ils aux Etats la mise à jour périodique, chaque cinq ans au moins, de leurs stratégies nationales de lutte contre la cybercriminalité.

On note également des tendances régionales. En novembre 2022, les 10 pays africains de la Ligue arabe ont annoncé à Tunis, sous l'égide de l'Organisation arabe des technologies de l'information et de la Communication (Aicto), la mise en place d'une stratégie commune de lutte contre la cybersécurité. Bien avant, en 2019, la CEDEAO, en partenariat avec l'Union européenne (UE), a lancé le projet OCWAR-C, la Réponse de l'Afrique de l'Ouest sur la cybersécurité et la lutte contre la cybercriminalité ■

Moussa Hassan Baraze, ministre de la Poste et des Nouvelles Technologies de l'information du Niger.

« La numérisation du Niger est en marche »

Convaincues que le secteur du numérique regorge d'importants gisements de croissance et qu'il constitue un puissant accélérateur dans l'atteinte des objectifs du développement, les autorités nigériennes affichent leur volonté d'accélérer la transformation du secteur, grâce à des mesures fortes. La Stratégie nationale de cybersécurité vient, à cet effet, d'être adoptée. L'objectif affiché du président et du gouvernement : hisser le pays au niveau des hubs régionaux numériques. Moussa Hassan Baraze, ministre de la Poste et des Nouvelles Technologies de l'information du Niger, détaille pour Cio Mag les principales avancées et les défis qu'il reste à surmonter pour accélérer la croissance et sécuriser le secteur du numérique.

INTERVIEW

Cio Mag : Après la ratification de la Convention de Malabo l'an dernier, le Niger vient d'adopter la Stratégie nationale de cybersécurité pour la période 2023-2027. Quelles sont les grandes lignes de cette stratégie et pourquoi n'intervient-elle qu'aujourd'hui ?

Moussa Hassan Baraze : Le Niger a adopté sa toute première Stratégie Nationale en matière de cybersécurité en décembre 2022. Avant cela, le pays s'était déjà doté de plusieurs textes législatifs et réglementaires pour lui permettre de lutter efficacement contre la cybercriminalité, l'usage malveillant des médias sociaux et d'améliorer la protection des données personnelles. En adoptant cette stratégie, résultat d'un long processus qui a duré plus de cinq ans, le gouvernement a décidé d'étoffer ce dispositif. L'objectif est de fournir au Niger un cyberespace sécurisé et résilient, favorable à l'essor d'une véritable économie numérique, condition essentielle au développement économique et social.

La Stratégie nationale de cybersécurité, qui couvre la période 2023-2027, s'articule autour des 4 lignes directrices, à savoir le renforcement de la confiance du public à l'usage du numérique par le cadre législatif et réglementaire ; le renforcement de la sécurité des systèmes d'information ; l'amélioration de notre capacité de prévention, de détection et de répression des cyberattaques et la protection des infrastructures sensibles et critiques nationales.

Aujourd'hui, sous l'impulsion du Président de la République SEM Mohamed Bazoum, la numérisation du Niger est en marche, elle est porteuse de croissance dans plusieurs secteurs et d'avancées sociales significatives. L'objectif du gouvernement est d'atteindre un taux de pénétration mobile de 100% et un taux de pénétration internet de 66% d'ici 2026. Cet accès massif à l'internet et aux réseaux sociaux constitue certes une opportunité, mais il engendrera de nombreux nouveaux défis auxquels

nous devons faire face, notamment la cybercriminalité, la désinformation, l'utilisation d'internet à des fins terroristes et l'exploitation excessive des données personnelles, pour ne citer que ceux-là. D'où la nécessité d'avoir une stratégie nationale en matière de cybersécurité.

Cio Mag : Le Niger a également annoncé la création du Centre national de cybersécurité et d'un laboratoire central d'investigation numérique. Quels sont leurs vocations ?

M.H.B : Le Centre national de cybersécurité (CNAC) a pour mission de coordonner et de mettre en œuvre la politique et la stratégie nationales de sécurisation et de défense des systèmes d'information et des infrastructures sensibles et critiques et améliorer la protection des données personnelles dans notre pays. De façon spécifique, il est chargé d'assurer notammentune veille technologique dans le domaine de la sécurité des systèmes d'information ; d'établir des directives et des normes de sécurité électronique à l'attention de l'État, des opérateurs d'infrastructures sensibles et critiques, du secteur privé et des particuliers, veiller à leur mise en œuvre et développer des mécanismes de suivi et de sanction ; d'enquêter sur toute menace et assurer la coordination nationale des activités de prévention, de détection, d'alerte et de réponses aux cybermenaces et aux cyberattaques ; de sensibiliser le public et de promouvoir une culture de la cybersécurité au Niger.

Quant au Laboratoire d'investigation numérique, il nous permettra d'analyser les supports informatiques de données, de les tracer et d'avoir des preuves. Le défi est de pouvoir sauvegarder les preuves et les données d'identification, afin d'éviter leur altération et leur falsification pour prouver l'origine et l'intégrité des documents numériques. Dans un monde de plus en plus numérisé, l'accès aux éléments de preuve impose de mettre en œuvre des techniques de recueil rigoureuses qui ne seront pas sujettes à contestation devant la justice.

Cio Mag : Il y a plus d'un an, vous aviez lancé l'étude sur le développement de l'Internet, avec comme objectif de permettre aux autorités nigériennes d'évaluer l'écosystème numérique et d'identifier les manques à combler. Quels sont les résultats de cette étude ?

M.H.B : En effet, nous avions lancé en 2021, en collaboration avec l'UNESCO, une étude sur le développement de l'internet au Niger. L'objectif de cette étude est de relever dans la plus grande objectivité les performances et les contre-performances du Niger dans le domaine digital. Il s'agit de manière spécifique de mettre l'accent sur la qualité des infrastructures numériques, la pertinence mais aussi d'identifier les insuffisances du cadre légal et réglementaire du chantier numérique nigérien.

L'évaluation a mis en exergue une forte volonté politique pour développer l'Internet et l'écosystème du numérique au Niger, et des avancées significatives ont été enregistrées. Le taux d'accès à l'Internet est passé de 24,53 % en 2019 à 33 % en 2021. Le taux de pénétration mobile est passé, lui aussi, de 51,90 % en 2019 à 61,00 % en 2021. Cependant, le rapport relève également des points de fragilité. Ils sont liés au coût de la connexion de base au large bande mobile, qui est le plus élevé dans la sous-région, au cadre juridique et institutionnel, au manque de compétences, au manque et à la qualité des infrastructures notamment en milieu rural, à la gestion des déchets électroniques, etc.

Concernant l'accès global à Internet et le taux de pénétration de la téléphonie mobile, quels sont les chiffres pour 2022 et comment accélérer encore le processus ?

M.H.B : En 2022, le Niger a encore enregistré des progrès encourageants pour les indicateurs du développement du numérique, malgré les actions malveillantes des groupes terroristes qui ont détruit plus de 145 sites à travers le pays. Le taux de pénétration internet est passé de 33% en 2021 à 35% en 2022 (chiffres au 30 septembre 2022) et celui de la pénétration mobile est passé de 61% en 2021 à 64% en 2022. Cette évolution s'explique par la volonté politique affichée par le Président de la République SEM Mohamed Bazoum, qui met l'accent sur l'amélioration de l'accès universelle à l'internet haut débit à un prix abordable et son adoption comme une condition préalable à la transformation numérique inclusive.

Cette priorité passe par la consolidation du cadre juridique, réglementaire et institutionnel incluant une revue de la politique fiscale et parafiscale du secteur

pour stimuler les investissements publics et privés dans les infrastructures numériques et leur partage, piliers essentiels pour le développement du secteur. À ce titre, nous avons allégé les procédures d'octroi des licences aux fournisseurs d'accès internet, pour l'exploitation d'infrastructures passives et /ou connexes des communications électroniques et l'exploitation des réseaux mobiles virtuels (MVNO). Nous avons également adopté le principe de la neutralité technologique pour permettre aux opérateurs d'offrir des services innovants basés sur des technologies avancées, selon les besoins du marché et nous avons libéralisé le déploiement de la fibre optique. La nouvelle loi en perspective apportera des réponses appropriées pour un meilleur encadrement des activités de télécommunications.

Dans le domaine des infrastructures, nous sommes en train d'exécuter deux grands projets, à savoir le projet de la dorsale transsaharienne à fibre optique, financé par la BAD, qui nous permet de déployer 1031 km de fibre optique et d'améliorer notre connectivité internationale à travers les sorties vers le Tchad, l'Algérie, le Nigéria, le Burkina et le Bénin. Le second projet consiste à connecter environ 2175 villages ruraux.

Notre pays jouit en outre de la confiance des bailleurs de fonds pour tous les efforts que les autorités font pour consolider la démocratie et l'État de droit. Ce qui nous facilite l'accès au financement de nos programmes et projets.

Cio Mag : En ce qui concerne l'identité électronique et la digitalisation des services aux usagers, où en est-on au Niger ?

M.H.B : Le Niger a rejoint en 2020, comme certains pays de la CEDEAO, le projet d'identification unique pour l'intégration régionale et l'inclusion en Afrique de l'Ouest, financé par la Banque Mondiale. Ce projet a pour objectif non seulement de doter les pays bénéficiaires de systèmes d'identification de personnes sécurisés, mais aussi de contribuer à l'amélioration de l'accès aux services de base, tels que la protection sociale et médicale, la retraite ainsi que l'inclusion financière et numérique à plusieurs millions de personnes, en particulier aux femmes et aux catégories sociales les plus pauvres, l'autonomisation des femmes et des filles, et la mobilité des travailleurs. La composante Niger, d'un coût global de 81 millions USD, a été officiellement lancée le 18 octobre 2022 pour une durée de cinq ans.

Cio Mag : Quels sont les autres grands projets en cours dans le domaine des infrastructures digitales ?

M.H.B : Nous pouvons citer le projet Villages intelligents pour la croissance rurale et l'inclusion numérique qui vise la connectivité large bande pour 2175 villages et à promouvoir les services financiers numériques ; le projet Niger LIRE qui a pour objectif d'améliorer la qualité des conditions d'enseignement et d'apprentissage grâce au numérique ; le projet d'Identification unique pour l'intégration régionale et l'inclusion en Afrique de l'Ouest (WURI) qui permettre de doter notre pays d'un système d'identification robuste et sécurisé de personnes. Ces trois projets sont financés par la Banque Mondiale. Il y a également le projet de la dorsale transsaharienne à fibre optique, financé par la BAD que j'ai évoqué plus haut. Nous avons également engagé la reforme de notre opérateur historique Niger Telecom pour qu'il joue mieux son rôle dans la construction d'une véritable économie numérique dans notre pays.

« L'objectif du gouvernement est d'atteindre un taux de pénétration mobile de 100% »

Très bientôt, nous allons aussi lancer les travaux de construction de notre premier datacenter.

Nous faisons également du renforcement des capacités des ressources humaines, une priorité. C'est pour cela qu'en dehors des écoles privées, nous avons créé depuis plus de 10 ans une Ecole publique supérieure de télécommunications qui forme des techniciens supérieurs et des ingénieurs. Récemment, nous avons révisé son programme d'enseignement pour y inclure l'enseignement de l'Intelligence Artificielle, du Big data, de la cybersécurité, du Cloud Computing. La volonté politique forte émanant du Président de la République, illustrée par la conduite de tous ces projets, devrait nous permettre de rattraper notre retard en termes de transformation digitale ■

Propos recueillis par Camille Dubruelh

ATDA
ASSISES DE LA TRANSFORMATION DIGITALE EN AFRIQUE

Assises de la Transformation Digitale en Afrique

12 ème édition

ANTANANARIVO
MADAGASCAR

19 ET 20
MAI 2023

Capital humain

Catalyseur d'un écosystème numérique africain performant

LA RÉFÉRENCE DU NUMÉRIQUE EN AFRIQUE
cio mag .com

MNDPT
MINISTÈRE DU DÉVELOPPEMENT NUMÉRIQUE, DE LA TRANSFORMATION DIGITALE, DES POSTES ET DES TÉLÉCOMMUNICATIONS

www.lesatda.com

MAROC
Le risque cyber, un enjeu stratégique pour la souveraineté numérique du royaume

Dans un monde marqué par l'essor des infrastructures numériques, la cybersécurité devient un enjeu majeur pour le développement de tous les pays du globe. Faisant face à une augmentation exponentielle des cyberattaques au cours des dernières années, le Maroc a pris la mesure des risques cyber qui pèsent sur ses institutions, en renforçant ses capacités techniques, réglementaires et humaines. Focus sur la stratégie du royaume en matière de souveraineté numérique.

Adil ABDELALI

Au Maroc, le centre de veille, de détection et de réponses aux cyberattaques, relevant de la Direction générale de la sécurité des systèmes d'information (DGSSI), a noté une augmentation annuelle de 50% des cyberattaques visant le royaume en 2021. Des attaques multiformes qui ciblent différentes organisations, telles que les entreprises privées et les institutions de l'État. Celles-ci sont particulièrement ciblées par les cybercriminels, à cause du caractère vital des secteurs visés. En 2021, la DGSSI a neutralisé 577 cyberattaques ayant pour cibles des ministères et des établissements publics du royaume.

En 2023, renforcer la sécurité des systèmes d'information n'est plus un luxe, mais une condition sine qua non au bon fonctionnement des organisations, qu'elles soient publiques ou privées. Pour le Maroc, la cybersécurité est érigée en priorité nationale dans le but de répondre aux défis de la transition numérique opérée par le royaume au cours des dernières années. D'où la mise en place d'un cadre juridique et réglementaire adapté aux défis actuels, à travers la loi 05-20 relative à la cybersécurité. L'adoption en 2021 de ce texte représente l'ultime étape d'une longue réflexion entamée au milieu des années 2000. La prise de conscience des pouvoirs publics a permis, entre autres, la mise en place d'une stratégie nationale de cybersécurité et de sécurité des systèmes d'information, l'installation de la DGSSI, relevant de l'administration de la défense nationale, ainsi que la création de la Commission nationale de contrôle de la protection des données personnelles (CNDP).

Toutes ces étapes ont permis au royaume de renforcer la maturité de son environnement cyber pour mieux appréhender les menaces liées à la cybercriminalité. Ainsi, dans le dernier rapport GCI (Global Cybersecurity Index), établi par l'Union internationale des télécommunications (UIT) et mesurant les engagements en matière de cybersécurité, le Maroc s'est hissé au 50e rang mondial sur 194 pays.

Verrouiller les données sensibles

Résolument engagé à renforcer sa souveraineté numérique, le Maroc a fait le choix stratégique de verrouiller l'accès aux données considérées comme sensibles, en interdisant l'hébergement de celles-ci dans des serveurs situés en dehors de ses frontières. À ce titre, il convient de distinguer deux types de données considérées comme sensibles, comme nous l'explique Taieb Debbagh, expert en cybersécurité et ancien membre de l'UIT : *« D'un côté, on parle de donnée personnelle sensible dans le cadre de la loi 08-09 relative à la protection des données personnelles. Cela concerne notamment les données de santé des citoyens ou leur appartenance politique ou syndicale. D'un autre côté, la loi 05-20 relative à la cybersécurité définit la donnée sensible comme une information nationale sensible, en lien avec les infrastructures d'importance vitale. Ce sont deux choses complètement différentes. »* Pour notre interlocuteur, l'interdiction de stockage à l'étranger vise, en priorité, les données et les informations en lien avec les infrastructures

d'importance vitale, comme les centrales de production d'énergie ou les infrastructures aéroportuaires. Ces données-là sont obligatoirement hébergées dans un Data Center national. En ce qui concerne les données sensibles des citoyens, les autorités peuvent faire preuve de souplesse. *« On peut demander une autorisation pour transférer ces données à l'étranger, à condition qu'il y ait une continuité juridique relative à la protection de cette donnée dans le pays de destination »,* précise l'expert.

Karim Hamdaoui, président de Morocco Trust (MorTrust), première association professionnelle de la cybersécurité au Maroc, estime pour sa part que l'interdiction d'héberger les données sensibles à l'étranger revêt une importance géostratégique pour le royaume. *« La carte géopolitique est en constante évolution sur la scène internationale. Rien ne nous garantit qu'un pays allié qui héberge aujourd'hui nos données ne se retournera pas demain contre nous. Pour éviter d'être pris en otage, il est obligatoire de stocker nos données sensibles dans des serveurs situés au Maroc. »* Quant à la capacité du royaume à assumer pleinement la responsabilité du stockage et de la gestion de toutes ces données, Karim Hamdaoui est plutôt confiant. Le Maroc dispose, selon lui, de centres de données qui répondent aux normes internationales ainsi que des prestataires cyber marocains qui peuvent assurer la sécurité de données. *« Cela étant dit, les organisations qui détiennent ces données doivent mettre en place des mesures de sécurité efficaces pour se prémunir des cyberattaques »*, nuance-t-il.

Former les talents et les retenir

La mise en place d'un cadre réglementaire dédié à la cybersécurité au Maroc a favorisé le développement d'infrastructures nationales, en phase avec les préoccupations des organisations. Néanmoins, le développement de ce chantier stratégique se heurte à plusieurs difficultés, notamment celle liée à la disponibilité des ressources humaines. Les institutions publiques et les entreprises privées peinent à recruter des experts en cybersécurité, malgré l'ouverture récente de nouveaux cursus académiques dédiés.

En 2010, alors qu'il était secrétaire général du ministère chargé des Technologies de l'information, Taieb Debbagh nous indiquait qu'il n'existait qu'une seule institution au Maroc qui offrait une formation de master en sécurité des systèmes d'information. *« Mais depuis, les choses ont évolué positivement. À titre d'exemple, la DGSSI a instauré un master au niveau de l'Institut national des postes et télécommunications (INPT). C'est également le cas dans des écoles publiques comme l'ENSA de Kénitra et celle de Marrakech ainsi que l'ENSIAS de Rabat, ou encore dans des institutions privées comme l'Université internationale de Rabat (UIR). Aujourd'hui, nous disposons, au moins, d'une quinzaine de masters dédiés à la cybersécurité »,* atteste notre interlocuteur. Néanmoins, Taieb Debbagh précise que l'offre de formation actuelle reste insuffisante pour combler la forte demande de profils spécialisés sur le marché.

C'est une problématique à laquelle est confronté régulièrement Karim Hamdaoui, en tant que président fondateur de LMPS Group, acteur marocain et panafricain de la cybersécurité. *« La difficulté à recruter des profils spécialisés concerne directement les prestataires de services, mais c'est un défi également pour les utilisateurs des systèmes d'information tels que les banques et les assurances qui ont du mal à attirer des spécialistes en cybersécurité, qui se font de plus en plus rares sur le marché »,* constate-t-il. Aussi, Karim Hamdaoui insiste sur la nécessité de former davantage d'ingénieurs et de techniciens et de favoriser les synergies entre le monde professionnel et académique. *« Il faut multiplier les partenariats entre les entreprises et les établissements d'enseignement pour définir des cycles de formation en cybersécurité »*, préconise-t-il.

Créer un écosystème

Par ailleurs, les rares diplômés marocains en cybersécurité trouvent facilement des propositions d'emplois plus avantageuses à l'étranger, alimentant ainsi l'inexorable fuite des cerveaux hors du pays. *« On n'y peut rien ! »,* déplore Taieb Debbagh tout en avançant certaines pistes de réflexion pour combler ce manque. *« Au-delà de la multiplication des cursus de formation, il faut favoriser l'émergence de centres R&D pour créer un écosystème qui permettrait d'attirer des profils spécialisés, tout en leur fournissant des conditions de travail optimales »,* explique l'expert. Même son de cloche pour Karim Hamdaoui qui milite pour retenir le plus grand nombre de compétences formées localement. Toutefois, il concède qu'une bonne partie de ces profils aspirent, tôt ou tard, à poursuivre leur carrière à l'étranger. *« En fin de compte, on ne peut pas empêcher quelqu'un de quitter le pays, mais les entreprises et les autorités doivent tout mettre en œuvre pour réussir ce défi »,* précise-t-il.

Dans le sens inverse, embaucher des talents étrangers qualifiés en cybersécurité s'avère fastidieux pour les organisations marocaines. *« Contrairement à la France, qui, grâce au passeport talent, arrive à recruter des profils en un temps record, nous avons du mal à embaucher des profils dans les pays d'Afrique subsaharienne, à cause de la lourdeur des procédures administratives. Par exemple, ramener au Maroc une recrue du Cameroun peut nous prendre des mois »,* déplore Karim Hamdaoui, qui appelle les autorités du royaume à fluidifier le processus de recrutement à l'étranger ■

Orange, opérateur Multiservice en Afrique et au Moyen-Orient

Présent dans 18 pays, nous proposons des services qui apportent des réponses concrètes aux attentes des populations dans la santé, l'éducation, l'énergie, l'agriculture et les services financiers.

Vous rapprocher
de l'essentiel

orange™

RDC
Une stratégie cybersécuritaire sur les rails

La République démocratique du Congo a enregistré quelques avancées en matière de cybersécurité depuis la mise en place, en 2020, du Plan national du numérique - Horizon 2025. Celles-ci, parmi lesquelles la validation de la Stratégie nationale de cybersécurité, placent le pays sur une bonne voie, bien que beaucoup restent à faire.

Enock BULONZA

Entre initiatives privées et publiques, la République démocratique du Congo ne croise pas les bras face aux enjeux et menaces cyber multiformes. En 2020, les autorités congolaises ont mis en place le Plan national du numérique - Horizon 2025, un vaste programme ayant pour objectif de faire du numérique congolais *« un levier d'intégration, de bonne gouvernance, de croissance économique et de progrès social ».*

Ce programme institutionnel tient compte aussi des nouvelles menaces liées à la cyberdépendance, à la cybercriminalité, aux malveillances informatiques de tout genre, aux atteintes à la vie privée, à l'ordre public, aux activités des entreprises, aux données personnelles et aux intérêts des États.

Deux ans plus tard, le président de la République a exprimé sa volonté de doter le pays d'un écosystème cybersécuritaire solide, capable de faire face aux menaces. Félix-Antoine Tshisekedi a, à cet effet, mis en place une commission technique pour la cybersécurité, attachée à la présidence de la République. Cette commission inter-institutionnelle a pour charge d'élaborer et valider la Stratégie nationale de la cybersécurité. Et à mettre en œuvre la création d'une agence nationale de cybersécurité.

Ainsi, les initiatives des autorités congolaises vont dans le sens d'une construction d'un écosystème cybersécuritaire solide, pour un pays en pleine transformation technologique. Elles permettront aussi à la Rdc de ratifier la Convention de Malabo, un cadre légal et règlementaire de la protection des données en Afrique, adopté le 23 juin 2014 par les Chefs d'État et de gouvernement de l'UA.

Des efforts restent à faire

En dépit des efforts fournis, le pays doit penser au renforcement de son arsenal juridique sur la protection des données à caractère personnel et au développement de ses infrastructures numériques.

En décembre 2022, l'Assemblée nationale a ainsi déclaré recevable le projet de loi portant sur le code du numérique de la RDC. Présenté et défendu par le ministre Eberande Kolongele, ce projet de loi se veut un cadre juridique de régulation, entre autres, de l'économie numérique, de la protection des données et de la vie privée. Après avoir été déclaré recevable, ce projet a été envoyé à la commission Aménagement du territoire, Infrastructures et Nouvelles technologies de l'information et de la communication pour un examen approfondi. L'adoption dudit projet de loi doit permettre au pays de franchir un pas important en matière de cybersécurité.

Des initiatives privées à l'assaut du système éducatif

En plus des initiatives institutionnelles, certains privés se démarquent par leurs actions en faveur de la construction de l'écosystème cybersécuritaire.

À titre d'exemple, l'Institut africain de Cybersécurité et Sécurité des Infrastructures (Institut CSSI) est la première école privée spécialisée dans la cybersécurité et la sécurité des infrastructures, disposant d'un programme sur l'apprentissage des technologies numériques et l'acquisition de compétences en management d'équipes et management de l'innovation. L'I-CSSI a ouvert ses portes à Kinshasa en octobre 2021 sous l'égide de Nathalie Kienga, spécialiste en stratégie de sécurité numérique.

À travers ses programmes, cette institution veut contribuer à la formation d'une élite capable d'évaluer les tendances de sécurité, reconnaître les meilleures pratiques, comprendre les risques et les menaces de sécurité informatique.

Certes, ces initiatives privées et publiques aideront le pays à répondre aux défis de cybersécurité, mais pour maintenir cet élan, la RDC devra fournir d'énormes efforts pour faire face à des menaces de plus en plus nombreuses et multiformes ■

Philippe Wang, vice-président exécutif de Huawei Northern Africa

INTERVIEW

STRATÉGIE

« En Afrique, nous accompagnons nos clients à améliorer leur cyber résilience »

Entre janvier et août 2020, l'Afrique a été la cible de 28 millions de cyberattaques. Cette même année, le marché de la cybersécurité s'élevait sur le continent à 2 milliards de dollars. C'est la preuve du potentiel stratégique que représente ce secteur pour la croissance et le développement socio-économique de l'Afrique. Huawei apporte également son expertise pour améliorer la cyber résilience des États africains. Philippe Wang, Vice-président exécutif de Huawei Northern Africa, en fait cas dans cette interview.

Cio Mag : Quel constat faites-vous sur la souveraineté numérique en Afrique et ses enjeux ?

Philippe Wang : La croissance numérique que connaît le continent africain depuis de nombreuses années témoigne d'une réelle prise de conscience des enjeux que représente la transition numérique pour le développement socio-économique des États africains. Avec l'accélération de la diffusion des technologies de l'information et de la communication (TIC) et de leur usage depuis la fin des années 1990, l'Afrique a embrassé un tournant numérique caractérisé par un accroissement des données. Le trafic de ces dernières a davantage explosé en plein cœur de la pandémie de la Covid-19, les mesures de confinement et de distanciation sociale ayant considérablement limité les interactions sociales.

De ce fait, il est nécessaire de les centraliser afin qu'elles soient valorisées et ainsi en mesure de créer des opportunités de développement pour les territoires. De ce point de vue, le chantier est encore conséquent, d'autant que la digitalisation des activités n'a pas terminé sa fulgurante progression, notamment à travers des secteurs porteurs ancrés au cœur de la quatrième révolution industrielle, à savoir le Cloud Computing ou encore l'Internet des Objets (IoT).

Par conséquent, afin que les usages liés à ces technologies de pointe puissent continuer d'émerger et de se démocratiser sur tout le continent, il est nécessaire que l'Afrique accélère la construction et l'installation de data centers sur tout le continent. C'est le cas par exemple de la blockchain, des cryptomonnaies ou encore de l'intelligence artificielle qui nécessitent à la fois des infrastructures réseau performantes et des capacités de stockage de données accrues.

Les ambitions de l'Afrique en matière de souveraineté numérique sont stratégiques et légitimes. Elles devront cependant s'opérer de façon cohérente avec les Objectifs de Développement Durable (ODD) et inclusifs

qui s'imposent au sein d'un continent où la fracture numérique demeure l'une des plus importantes au monde. En effet, alors même que plus de la moitié de la population subsaharienne (59%) vit en zone rurale, seuls 16% des habitants ont recours à l'internet mobile dans ces territoires isolés, comparé à un taux de 40% au sein des populations urbaines[1].

Cio Mag : Les attaques cyber se sont multipliées en Afrique durant la crise de la Covid-19, fragilisant de nombreuses structures publiques et privées. Avez-vous observé une réelle prise de conscience des autorités africaines depuis cette crise ?

P.W : À mesure que l'écosystème digital s'impose sur le continent, les autorités africaines sont conscientes des risques liés. C'est particulièrement le cas depuis la crise de la Covid-19 et l'émergence de nouveaux usages numériques tels que le télétravail, à l'origine d'une vulnérabilité grandissante des entreprises et structures publiques (administrations, hôpitaux etc.).

En tant que fournisseur leader d'infrastructures TIC et de dispositifs intelligents en Afrique, Huawei fait de la sécurité, de la fiabilité et de la protection de la vie privée l'un de ses principaux leitmotivs, en Afrique et dans le monde. Nous accompagnons donc nos clients sur le continent à améliorer leur cyber résilience en proposant des produits, des solutions et des services sécurisés et fiables. Je pense que des entreprises comme Huawei ont pour mission d'être de véritables facilitateurs pour fournir des solutions et du matériel efficace afin que les États puissent se prémunir des cyberattaques.

Cio Mag : Comment les entreprises peuvent-elles accompagner les États africains vers une souveraineté numérique pleine et entière ? Est-ce seulement une question d'investissements ?

P.W : Bâtir et installer durablement une souveraineté numérique sur le continent requiert bien entendu plusieurs ingrédients. En premier lieu, la conception, la construction et l'installation d'infrastructures nécessitent d'importants investissements dirigés en faveur de la R&D et de l'innovation. C'est la raison pour laquelle Huawei investit massivement dans la R&D et ce, depuis des années.

Au cours de la dernière décennie, nous avons consacré plus de 845,6 milliards de yuans (soit 126,21 milliards de dollars) dans la R&D orientée vers les innovations liées au cloud, à l'intelligence artificielle et aux terminaux intelligents.

La construction d'une souveraineté numérique africaine repose donc sur le déploiement de moyens financiers, mais aussi et surtout sur la mobilisation de ressources humaines. De plus en plus d'entreprises, conscientes de ces enjeux, accompagnent les autorités africaines dans ce sens. Chez Huawei, nous pensons qu'une grande place doit être accordée à la sensibilisation et à l'éducation des populations à un usage prudent des outils et solutions numériques.

A titre d'exemple, Huawei et l'École Nationale de l'Administration (ENA) du Sénégal ont signé un protocole d'accord en juin 2022 pour une durée de trois ans, afin de permettre aux élèves de l'ENA de se familiariser avec les nouvelles technologies nécessaires à une administration plus performante.

Du 29 août au 5 septembre 2022, les 39 étudiants de cette première cohorte ont ainsi pu bénéficier du programme de formation Seeds for the Future et se former aux technologies disruptives que sont la 5G et l'IA, ainsi qu'à la cybersécurité. Il leur a ainsi été possible d'acquérir des compétences leur permettant de relever les défis auxquels l'Afrique fait face pour améliorer sa digitalisation, et ainsi s'acheminer progressivement vers une souveraineté numérique pleine et entière.

En parallèle, ces partenariats et programmes de formation tels que la ICT Academy visent également à favoriser les transferts de compétences nécessaires pour accroître l'autonomie des États dans la gestion et le traitement de leurs données, et participent ainsi au développement des compétences essentielles pour assurer un fonctionnement pérenne des data centers locaux. L'objectif étant de permettre un transfert de compétences sur le long terme afin que les populations africaines soient elles-mêmes en mesure de prendre en main leur avenir numérique.

Cio Mag : L'Europe peine encore aujourd'hui à construire sa souveraineté numérique. En quoi cela peut-il être différent pour le continent africain ?

1 « The State of Mobile Internet Connectivity 2020 » GSMA, 2021

P.W : Quel que soit le continent, la digitalisation de nos sociétés se poursuit sur des modèles similaires et bouleverse les quotidiens des populations partout dans le monde. La question du modèle de souveraineté souhaité, quant à lui, découle de choix politiques propres. Chez Huawei Northern Africa, nous pensons qu'il est primordial de favoriser l'émergence d'acteurs locaux en accompagnant les stratégies digitales nationales ambitieuses mises en place par les différents gouvernements. Notre rôle est de fournir aux acteurs de l'écosystème, présents et futures, les dispositifs et infrastructures nécessaires au développement de leurs activités et à l'expression libre de leurs esprits innovants.

La souveraineté numérique africaine devra reposer sur un défi industriel, mais aussi réglementaire et les États africains ont déjà bien conscience de cela. Les États européens disposent déjà tous d'un modèle centralisé de gestion des données et ils sont confrontés à une problématique d'harmonisation à travers la construction d'un nouveau modèle réglementaire. À l'inverse, les États africains, dont les modèles de gestion de données fonctionnent encore en ordre dispersé, ont d'ores-et-déjà l'opportunité de construire une véritable souveraineté en mutualisant la structuration de leur modèle.

Lors du dernier Sommet de la Cybersécurité à Lomé, en mars 2022, le Président togolais Faure Gnassingbé, a déclaré qu'il était important que *« l'Afrique soit au rendez-vous, et même partie prenante du nouveau monde en construction (autour du numérique), afin de répondre de manière adéquate aux enjeux qu'ils comportent ».*

Cio Mag : Les principaux acteurs de l'écosystème s'accordent pour dire qu'il est urgent de renforcer les capacités de stockage des données sur le continent africain. Comment Huawei Northern Africa accompagne-t-il les États africains dans la construction de data centers ?

P.W : Donner à l'Afrique les moyens humains et matériels de développer et d'installer durablement une filière dans la gestion et l'hébergement de la data me semble être une priorité pour les années à venir. L'exploitation de la donnée représente un véritable levier de développement socio-économique pour le continent qui a réalisé au cours de ces deux dernières décennies, une transformation numérique sans précédent. Parce que nous sommes présents depuis plus de vingt ans dans la région, chez Huawei Northern Africa, nous sommes au fait des problématiques techniques liées au territoire, que rencontrent certains États africains. Parmi ces difficultés, nous pouvons citer l'instabilité de l'approvisionnement en électricité en raison de réseaux de distributions fragiles.

Or, un approvisionnement continu en électricité est indispensable, non seulement pour le fonctionnement sans interruption des infrastructures d'hébergement de données, mais aussi pour le refroidissement de ces data centers. Il faut savoir que le refroidissement représente environ 40% de l'énergie consommée par les data centers.

Pour répondre à ces aléas, Huawei a proposé sur le marché l'an dernier une nouvelle génération de data centers intelligents et à faible émission carbone, à travers le lancement de PowerPOD 3.0. Ce nouveau système d'alimentation électrique permet de gagner du temps, de l'espace et de l'efficacité énergétique. Il permet ainsi de réduire le délai de livraison de composants électroniques de 2 mois à 2 semaines, l'encombrement de 40% et la consommation d'énergie de 70%. Cette nouvelle génération de data centers promet ainsi d'être durable, autonome et fiable, avec une architecture d'alimentation et de système de refroidissement simplifiés. En outre, ces data centers seront entièrement écoénergétiques en favorisant le recyclage de tous les matériaux nécessaires à leur fabrication, y compris les batteries, freinant ainsi l'épuisement des ressources minières sur la planète ■

Philippe WANG a rejoint le groupe Huawei en 2009. Il a successivement exercé les fonctions de Directeur de grand compte d'Orange, Directeur général de plusieurs pays (Togo, Bénin, Gabon, Guinée-Équatoriale), puis Vice-président Exécutif de la région Afrique de l'Ouest. Depuis octobre 2018, il est devenu Vice-président exécutif de Huawei Northern Africa.

BANQUES
Les hackers ont une longueur d'avance

La transformation numérique s'accompagne d'un important lot de désagréments. Les banques et institutions financières sont notamment les cibles privilégiées des hackers ces derniers temps. Au-delà de lutter contre ces attaques, les pays du continent doivent adopter une approche globale sur la cybersécurité. Analyse.

Enock BULONZA

D'après une étude de Kaspersky, durant les six premiers mois de 2022, plusieurs banques, des systèmes de paiement et des sites de commerce électronique ont été attaqués dans des pays d'Afrique subsaharienne. Quelque 100 192 attaques par hameçonnage ont été enregistrées au Kenya, soit une hausse de 201% par rapport au premier trimestre. Selon le document, ces attaques concernent essentiellement le commerce électronique et les banques.

Clément Domingo, spécialiste de la cybersécurité, croit connaître les raisons d'une telle situation. Selon lui, les attaques sur les banques sont plus récurrentes du fait d'un manque notoire de conformité aux exigences en matière de sécurité informatique. Pendant longtemps, les entreprises ont manqué de prendre très au sérieux la menace sécuritaire. Là où certaines se contentent de très peu, d'autres n'accordent presque pas d'importance à cet aspect. *« Il faut d'ailleurs noter une évolution des attaques. On parlait beaucoup de la fraude interne dans les banques. Mais dernièrement, il y a de plus en plus des cyberattaques, des ransomwares sur les banques. Les cybercriminels ont compris qu'il y avait de grosses failles dans les systèmes d'information des banques et que c'était peu ou pas corrigé »*, analyse-t-il. Une situation d'autant plus inquiétante que presque tous les pays du monde amorcent ou entament le dernier virage de la transformation digitale. Et le drame, selon notre analyste, c'est que même les plus grandes puissances ne sont pas épargnées.

Pour une approche plus globale, Clément Domingo, alias Saxx, estime important que les pays africains réactualisent la Convention de Malabo, qui date de 2014. *« Depuis qu'elle est entrée en vigueur, sur les 54 pays, il n'y en a que 23 qui l'ont ratifiée et seuls 5 ou 6 ont commencé à signer »*, a-t-il d'emblée déploré. Pour rappel, cet accord vise à *« renforcer et harmoniser les législations actuelles des Etats membres et des Communautés Economiques Régionales (CER) en matière de TIC »*, dans le respect des libertés fondamentales et des droits de l'Homme et des Peuples. Elle vise également à créer *« un cadre normatif approprié correspondant à l'environnement juridique, culturel, économique et social africain »* et souligne que la protection des données personnelles et de la vie privée est un *« enjeu majeur de la société de l'information »* ; tout traitement de données personnelles doit respecter un équilibre entre libertés fondamentales, promotion et usage des TIC, intérêts des acteurs publics et privés.

Saxx estime que la plupart des 44 points de la Convention sont en déphasage avec les enjeux de l'heure. « *Il y a besoin de remettre à jour cette Convention, en y ajoutant des aspects sur la cybersécurité, la cryptomonnaie, le blanchiment d'argent…*

C'est important de s'adapter aux enjeux sans cesse croissants », insiste-t-il.

Partage d'informations

Dans le même ordre d'idées, Clément Domingo estime que les pays doivent penser à des agences nationales de surveillance des systèmes d'information. Ce qui permet, selon lui, en cas de grandes attaques, d'alerter, de veiller et d'aider les entreprises à se préparer. *« Au niveau régional, il faudrait que chacun ait un point de contact qui permette le partage d'informations sur les menaces. Mais aujourd'hui, les gens ont peur de partager des informations. Il faut beaucoup de pédagogie. Les entreprises aussi, même si elles sont petites, doivent prendre ces enjeux très au sérieux et grandir avec. Pour Saxx, même le simple usager des réseaux sociaux n'est pas à l'abri. Car, estime-t-il, nous sommes tous sur les réseaux sociaux et ce sont des données personnelles qui sont concernées »*. Par ailleurs, il recommande aux gouvernements africains d'exiger un certain dispositif sécuritaire certifié aux entreprises, comme le Bénin est en train de le faire. « *L'État peut, par exemple, dire : ceux qui n'ont pas de certificat ne peuvent pas accéder à certains marchés. Il faut encourager la culture de la sécurité numérique, ensuite favoriser la formation du personnel pour élever le niveau de sécurité »*, explique-t-il.

Selon notre analyste, l'inquiétude est d'autant plus grande que sur le continent, les entreprises ne semblent pas avoir pris la pleine mesure des enjeux. En effet, déplore le spécialiste, dans de nombreux projets numériques, la dimension « données personnelles » est laissée en rade. Aujourd'hui, insiste le hacker, il faut sensibiliser et éduquer sur le numérique, comme cela a été fait avec la prévention routière. *« Les entreprises en Afrique n'ont pas encore inclus la dimension cybersécurité. Elles ne mettent pas le budget. Si vous regardez bien, de très grosses compagnies, qui ont pourtant mis des montants importants, se font attaquer. C'est le cas de Uber, par exemple. En Afrique, beaucoup de banques ont été victimes de cyberattaques. Au Sénégal, l'Autorité de régulation des télécommunications et des postes (Artp) a été victime d'une attaque virulente »*, fait-il remarquer.

Toutefois, même si des solutions ne manquent pas, Clément Domingo souligne que le combat est loin d'être gagné. Pour lui, entre les hackers et les entreprises, c'est le jeu du chat et de la souris. *« Les hackers ont toujours une longueur d'avance sur les entreprises »* ■

Pascal Naudin, directeur des Ventes B2B, Kaspersky Afrique du Nord, de l'Ouest et du Centre

« Les entreprises africaines doivent sérieusement réfléchir à leur stratégie »

Lancé dans un mouvement de digitalisation sans précédent, le continent africain fait aussi face à des menaces cyber de plus en plus grandes. Et la culture de la cybersécurité est bien loin d'être partagée, dans la société civile comme dans les entreprises. Pascal Naudin, Directeur des Ventes B2B, Kaspersky Afrique du Nord, de l'Ouest et du Centre, donne quelques pistes pour plus de résilience face à ces menaces.

INTERVIEW

Cio Mag : Le continent africain est-il plus vulnérable face aux menaces cyber et pourquoi ? Quelles sont les attaques les plus courantes sur le continent et les nouvelles tendances en ce début d'année 2023 ?

Pascal Naudin : Le continent africain n'est pas plus vulnérable que le reste du monde face aux menaces cyber. Simplement, avec la digitalisation croissante - sans nulle autre pareille dans le monde - des entreprises et des administrations africaines, le terrain d'exploitation des vulnérabilités cyber est croissant. Comme dans le reste du monde, les entreprises africaines vont plus que jamais devoir réfléchir à une stratégie de cybersécurité pour l'intégrer au cœur de leur développement économique et de leur digitalisation.

Pendant l'année 2022, nous avons découvert de plus en plus de nouveaux fichiers malveillants (URL, sites web, malwares, etc.) avec une moyenne de 400 000 nouveaux fichiers malveillants par jour, ce qui représente une augmentation de 5% par rapport à 2021.

Au total, les systèmes de Kaspersky ont détecté environ 122 millions de fichiers malveillants en 2022, soit 6 millions de plus que l'année précédente. En Afrique de l'Ouest, nos récentes observations tendent vers une croissance des attaques via le Web, sur les entreprises.

Lorsque l'on s'intéresse aux types de menaces, on remarque qu'elles sont variées et peuvent provenir d'Internet (URL malveillante, clic sur lien malveillant, infection en téléchargement, cheval de Troie, etc.), du réseau local par un appareil amovible type clé USB infectée par exemple. En matière de types d'attaques, elles aussi varient beaucoup et tout dépend de l'objectif recherché par le cybercriminel. Il peut s'agir d'objectifs d'espionnage, de destruction, de sabotage ou d'extorsions de données, de demande de rançon, etc. Plus rares, mais dont on parle le plus dans les médias, ce sont les attaques en provenance de groupes APT, perpétrées par des Etats ou sponsorisées par des Etats avec des modes opératoires bien plus sophistiqués. Le ransomware reste toutefois une grosse menace à craindre pour les entreprises.

Nos chercheurs ont également travaillé sur des prédictions ciblées, notamment en matière d'APT, et d'ailleurs une vidéo en français est disponible pour bien comprendre l'évolution des menaces et les impacts des conflits internationaux sur la cybersécurité.

Cio Mag : Il existe aujourd'hui une nette différence entre les entreprises multinationales qui appliquent leurs standards de cybersécurité en Afrique et les entreprises locales qui semblent ne pas avoir encore pris la mesure de la question. Comment faire pour dispenser une « culture » de la cybersécurité à grande échelle ?

P.N : De manière générale, nous avons tendance à dire que les entreprises de toutes les tailles doivent concevoir la cybersécurité comme une priorité stratégique à l'heure où les usages du numérique et la valeur des informations partagées via ce biais ne cessent de croître. Les problèmes que l'on rencontre aujourd'hui en Afrique sont les mêmes que dans le reste du monde : nous manquons de ressources, de budget bien souvent et de compétences. Les responsables de la sécurité informatique peinent parfois à se faire entendre, lorsqu'ils existent ! Il est nécessaire que la question de la cybersécurité soit intégrée aux prises de décision de l'entreprise, que ces sujets soient abordés aux comités de direction et soient intégrés dans les conversations sur l'avenir et le développement de l'entreprise.

Ensuite, il s'agit d'intégrer la culture de la cybersécurité au sein de la société, d'une part, en poussant les jeunes à s'intéresser à ces métiers, en sensibilisant aux bonnes pratiques cyber dès les premiers usages du numérique, des smartphones, etc. Et au sein des entreprises, d'autre part, afin que chaque employé puisse être non pas une porte ouverte aux cyber-risques, mais le premier rempart contre ces attaques.

Enfin, sans doute, qu'en instaurant des sortes de normes sur l'intégration de la sécurité directement dans la conception des appareils, qu'ils soient industriels, IoT ou grand public, cela permettrait de faire accepter à chacun le fait que l'usage du numérique offre un grand nombre d'opportunités mais que, mal utilisées, les technologies peuvent aussi comporter quelques dangers et qu'il est ainsi nécessaire d'adopter de bonnes habitudes (vérifier les paramètres de confidentialité, utiliser un VPN sur les réseaux publics/ouverts, utiliser des solutions de sécurité, même sur mobile, changer ses mots de passe, détecter les mails de phishing, ne pas utiliser de clé USB suspecte, etc.)

Cio Mag : Comment renforcer la capacité de résistance et de résilience des entreprises et organisations africaines aux cyberattaques et mettre fin au « tabou » ?

P.N : La résilience est exactement le mot adapté pour aborder la réalité de l'écosystème cyber aujourd'hui. Il est plus que primordial que les entreprises aient un temps d'avance vis-à-vis de la menace puisque la question n'est plus de savoir " si elles seront attaquées " mais plutôt " quand et par quel vecteur ". Il faut savoir s'informer, faire de la veille et comprendre comment les informations peuvent être transformées en action. Nous en sommes persuadés, les années à venir seront celles de la threat intelligence, encore plus que des technologies de détection et de réponse, aussi avancées soient-elles. Les capacités automatisées disponibles dans les technologies offertes, notamment par Kaspersky, permettent, en effet, aux entreprises d'être plus résilientes vis-à-vis de la menace, mais cela ne fait pas tout. Il faut que les entreprises soient en capacité d'opérer ces technologies, de les paramétrer, de faire les bonnes mises à jour mais également de former leurs salariés à quelques règles de cyber-hygiène de base. Projetons-nous dans l'avenir des villes connectées. On aura beau avoir un immeuble perfectionné, ultra-sécurisé, avec toutes les technologies embarquées et toute la sécurité possible, si l'habitant n'a pas les clés pour pénétrer dans cet environnement ultra-sécurisé et passe par la fenêtre, ou pire, casse une fenêtre, cela remet en question la sécurité de tout l'immeuble, pas seulement la sienne. En cybersécurité, il ne faut rien laisser au hasard et surtout pas la sensibilisation et l'accompagnement de toutes les parties prenantes d'un système.

Cio Mag : Les hackers sont de plus en plus professionnels sur le continent. Comment faire face aux nouvelles menaces ? Quelles solutions propose Kaspersky pour limiter les risques ?

P.N : Si l'on doit parler technique et outils, Kaspersky fournit tout un panel de solutions et de services cybersécurité, permettant aux entreprises de se protéger contre les menaces avancées et les attaques ciblées. Notre offre repose sur un modèle à 3 niveaux :

- La couche fondation : le must have pour toute

entreprise, et le niveau de sécurité minimal permettant la protection des postes de travail, des réseaux et des données. Il s'agit des technologies permettant la mise en place des mesures de protection préventives, et la matérialisation technique de la politique de sécurité des systèmes d'information de l'entreprise. Les solutions proposées dans la gamme Fondation sont : la protection du poste de travail, la protection de la messagerie, la sécurisation de la navigation web, la sécurité des stockages, etc. On parle ici de solutions de type Kaspersky Endpoint Security Cloud, Kapersky Secure Mail Gateway, Kaspersky Security for Microsoft 365, etc.

- La sécurité Optimum : l'offre Optimum est une suite de technologies et de services permettant l'identification des attaques avancées, l'outillage nécessaire pour la réponse aux incidents, ainsi que la formation des collaborateurs sur les risques et enjeux de la sécurité des systèmes d'information. C'est l'évolution logique pour les clients disposant des solutions de sécurité périmétriques et désirant augmenter leur niveau de résilience face aux menaces complexes grâce à l'EDR, le MDR, la sensibilisation, etc. Ici on proposera du coup des solutions de type EDR Optimum, mais aussi MDR ou Kaspersky Automated Security Awareness Platform.

- Sécurité Expert : destinée aux équipes de cybersécurité matures et aux entreprises ayant des systèmes d'information évolués et complexes, l'offre Expert est constituée également des services et technologies les plus avancées. Grace à la technologie XDR (EDR Expert), les attaques ciblées et les menaces évasives pourront facilement être identifiées et bloquées sur le système d'information. Il s'agit d'une visibilité complète sur les menaces, avec des technologies combinant l'IA et les moteurs de détection les plus avancés du domaine. Ces technologies sont enrichies avec de la threat intelligence (renseignement sur les menaces), afin de contextualiser les incidents, et permettre aux équipes sécurité, de prévenir les attaques et cela, bien avant qu'elles ne se produisent grâce à l'intelligence de l'anticipation (voir Threat intelligence Portal de Kaspersky pour plus d'information).

Enfin, nous proposons des services cybersécurité, permettant aux entreprises d'évaluer la résilience de leur système d'information, et former les équipes sur des thématiques poussées de la sécurité (analyse de malware, investigation numérique, réponse aux incidents…)

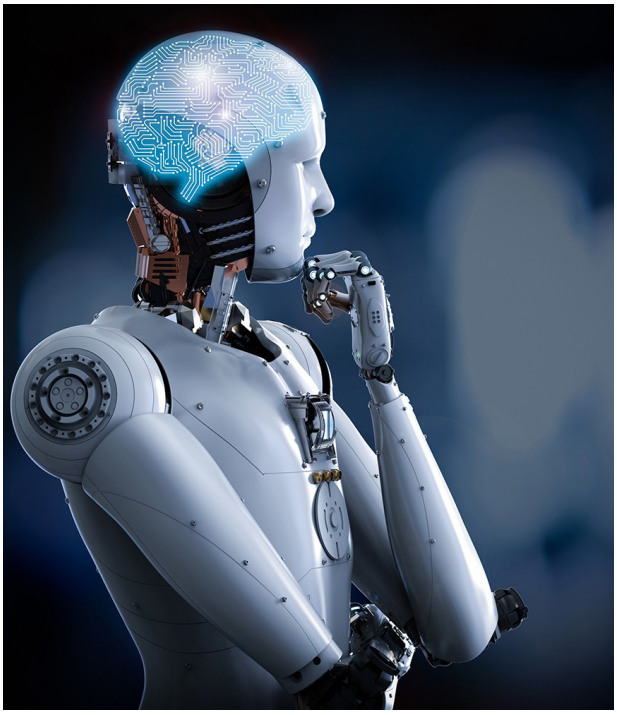
Cio Mag : En termes de compétences, lutter contre les menaces cyber nécessite-t-il des formations de haut niveau ou peut-on former l'ensemble des citoyens/employés afin de réduire les risques ?

P.N : Pour lutter au quotidien contre les menaces et ainsi bénéficier de tout ce que le numérique a à offrir (en termes de productivité, de connectivité, de partage, de stockage, etc.), il faut que tous les maillons de la chaine de valeur soient protégés. Cela passe par des technologies, certes, mais aussi par des compétences. Il est donc nécessaire d'avoir des professionnels formés pour être capables de répondre aux incidents, d'opérer la sécurité du système, de réagir en cas de problème, de prendre les bonnes décisions, etc. Il s'agit d'avoir des compétences techniques, compétences que nous offrons chez Kaspersky avec nos formations expertes de type CITO ou x-training – mais il est également impératif que l'ensemble des salariés et des citoyens soient formés, sensibilisés et développent de bonnes pratiques.

Enfin, au quotidien, et dès le plus jeune âge, il est possible d'intégrer les bonnes pratiques de sécurité au cœur de l'éducation par le biais d'outils type Kaspersky Safe Kids ou par le biais du dialogue, de l'échange… ou d'outils pédagogiques dédiés, mis à disposition par les institutions, les académies ou même les éditeurs de sécurité. Là encore, il s'agit d'un travail collectif qui requiert d'avancer tous dans la même direction : vers un monde numérique plus sûr ■

Propos recueillis par Camille Dubruelh

Après avoir passé plusieurs années chez différents intégrateurs IT, **Pascal Naudin** a débuté sa carrière africaine chez un distributeur il y a plus de 15 ans en faisant la promotion des solutions Kaspersky. Il a ensuite rejoint la marque comme Key Account Manager pour ensuite prendre la responsabilité de la région North, West et Central Africa. Avec une équipe dédiée de 6 personnes, ils rayonnent sur 27 pays afin d'assurer de la promotion du catalogue des solutions au travers d'un écosystème de partenaires locaux.



INTELLIGENCE ARTIFICIELLE
Une clé pour lutter contre les vulnérabilités

Parler de vulnérabilité dans la cybersécurité, c'est faire allusion à une faille ou à une faiblesse dans un système, une application ou un réseau, qui peut être identifiée et exploitée par des cybercriminels pour accéder à des informations sensibles ou pour causer des dommages. Dans ce sillage, comment des solutions basées sur l'Intelligence artificielle (IA), incluant des fonctionnalités de gestion des vulnérabilités, peuvent-elles permettre d'analyser et de prédire les risques parmi des milliers de vecteurs d'attaque et de menaces ? Des spécialistes se prononcent

Anselme AKEKO

Principales priorités des professionnels de la sécurité informatique, les vulnérabilités doivent être hiérarchisées et corrigées avant que les attaquants ne puissent les trouver et les exploiter. Solution architect sur des projets de prévention et de détection de fraudes et des anomalies basées sur l'IA et le Big data Analytics, Paterne Bazebizonza énumère quelques origines parmi les plus courantes des vulnérabilités. Selon lui, il peut s'agir de systèmes et d'applications mal configurés (erreurs de configuration) ; de vulnérabilités introduites involontairement par des développeurs dans le code qu'ils écrivent pour leurs applications (failles de sécurité) ; de défauts de conception dans les systèmes d'exploitation ; de logiciels non mis à jour (obsolètes ou non maintenus) ; ou encore de vulnérabilités introduites dans l'environnement de l'entreprise par des employés qui ne suivent pas les politiques de sécurité.

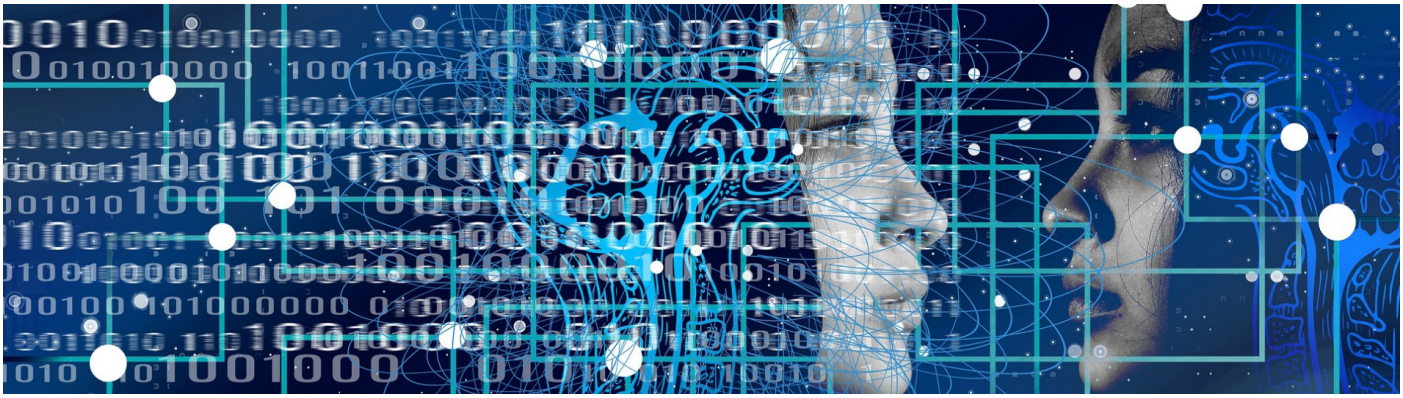
MBA Cybersecurity de l'Ecole de guerre économique du Maroc et Directeur général d'un groupe africain de cybersécurité, Cyprien Ekra ajoute que les équipes de sécurité utilisent traditionnellement des outils d'évaluation des vulnérabilités mais ils ne sont pas *« très efficaces avec les environnements distribués, en particulier les environnements hybrides, avec des appareils mobiles et IoT (Internet des objets, ndlr) ».*

D'après l'analyste, les outils de vulnérabilité traditionnels ignorent également les vecteurs d'attaque sophistiqués, tels que les problèmes d'identification ou le phishing. Quant aux solutions existantes, elles ne hiérarchisent pas les vulnérabilités, laissant les équipes de sécurité gérer plusieurs listes de vulnérabilités sans contexte. En la matière, il n'existe pas de stratégie parfaite pour déterminer la gravité d'une vulnérabilité. Face à la complexité de la tâche, Paterne Bazebizonza propose une approche basée sur trois piliers : *« Un en amont durant le BUILD, le second en aval durant le RUN et le troisième en Continuous improvement, à cheval entre le BUILD et le RUN »,* utilisant l'IA.

DevOpsSec et cybersécurité

Premier des trois piliers énoncés par Paterne, le DevOpsSec. Une approche qui peut aider à lutter contre les vulnérabilités en cybersécurité en intégrant les pratiques de sécurité dans les processus de développement et de livraison de logiciels. *« C'est en effet, vraiment en amont, qu'il faut concevoir (BUILD) et livrer des produits ou systèmes robustes, offrant la surface d'attaque la plus réduite possible, voire aucune. En utilisant des techniques telles que l'automatisation des tests de sécurité, l'intégration de la sécurité dans les processus de développement, la collaboration entre les équipes de développement et de sécurité, la surveillance continue et la mise en place de normes de sécurité, le DevOpsSec permet de mieux intégrer la sécurité dans toutes les étapes du processus de développement, depuis la conception jusqu'à la mise en production »*, explique-t-il.

Une fois le produit ou le système déployé dans l'entreprise (RUN), *« c'est au tour de la stratégie Cybersécurité de prendre la*



main », soutient le spécialiste. Expliquant que la cybersécurité utilise des outils tels que les scanners de vulnérabilités, les logiciels de gestion de vulnérabilités et les systèmes de gestion de sécurité des réseaux (SIEM) pour identifier les vulnérabilités dans les systèmes et mettre en place des solutions pour les atténuer.

IA et apprentissage automatique

Poursuivant, notre expert en IA et Big data Analytics affirme que l'IA peut être utilisée *« en mode Continuous improvement »*, pour prévenir, détecter et bloquer les attaques basées sur les vulnérabilités, aussi bien en BUILD qu'en RUN. *« En utilisant des techniques telles que l'analyse de comportement, l'apprentissage automatique, l'analyse de données, la reconnaissance de motifs et les systèmes d'Intrusion Detection and Prevention (IDPS), l'intelligence artificielle peut détecter les vulnérabilités plus rapidement et avec plus de précision que les méthodes traditionnelles »*, déclare Paterne Bazebizonza. Il ajoute que les systèmes d'IA peuvent également apprendre continuellement et s'adapter aux nouvelles vulnérabilités en utilisant des techniques d'apprentissage automatique (Machine Learning/Deep Learning).

« L'intelligence artificielle, en particulier l'apprentissage automatique, analyse les données en temps réel, en hiérarchisant les vulnérabilités en fonction du niveau de risque. Les solutions basées sur l'IA incluent des fonctionnalités de gestion des menaces et des vulnérabilités qui peuvent analyser et prédire le risque parmi des milliers de vecteurs d'attaque et de menaces. Facilitant ainsi le travail de classification des analystes et réduisant les temps de réponse aux incidents », renchérit Cyprien Ekra.

En effet, l'apprentissage automatique, ajoute Paterne, permet de créer des modèles qui peuvent identifier les vulnérabilités en analysant les données de sécurité, comme les journaux d'événements et les données de réseau, pour identifier les comportements anormaux et les menaces potentielles. Selon lui, la reconnaissance de motifs peut être utilisée pour détecter les vulnérabilités en recherchant des modèles récurrents dans les données de sécurité. Cela permet aux systèmes d'IA de devenir de plus en plus efficaces à mesure qu'ils reçoivent plus de données et d'expérience.

« Les vulnérabilités sont une plaie pour l'économie numérique »

Pour les spécialistes, c'est en combinant ces différentes méthodes et technologies que les entreprises peuvent atténuer les vulnérabilités et se protéger contre les cyberattaques. Toutefois, l'approche ne peut pas à elle seule garantir une protection à 100%. Aussi est-il important de maintenir et de superviser régulièrement les systèmes d'IA pour éviter les erreurs ou les biais dans les résultats. Ou encore de mettre en place une stratégie de cybersécurité globale mêlant sensibilisation, formation, politiques et procédures de sécurité, surveillance et détection des menaces, et gestion des incidents de sécurité. Ce qui est particulièrement utile, connaissant le coût économique des atteintes à la sécurité des actifs informatiques et technologiques. En 2020, ce coût était estimé entre 4 000 et 6 000 milliards de dollars, soit environ 4 à 6 % du PIB mondial, rappelle Cyprien Ekra.

« L'une des façons dont les vulnérabilités peuvent impacter l'économie numérique d'une Nation est de permettre le vol de propriété intellectuelle (PI) ou l'accès non autorisé aux systèmes qui stockent ou transmettent la PI, explique Cyprien Ekra. *De plus, les vulnérabilités peuvent permettre le détournement d'ordinateurs et la transmission de logiciels malveillants. »* Ces types de vulnérabilités peuvent, selon lui, avoir un impact dévastateur sur l'économie d'un pays, car les entreprises peuvent perdre des revenus en raison du vol de leur PI, et les individus peuvent être affectés par la perte d'informations personnelles.

« Les vulnérabilités sont une plaie pour l'économie numérique », confirme Paterne Bazebizonza. Ajoutant que les cybercriminels peuvent les utiliser pour prendre le contrôle des systèmes et des réseaux d'entreprises, et causer des perturbations des activités commerciales, des pertes de données, des perturbations de la confidentialité et des coûts de récupération ■

Dr. Jaleel Polin, NetSuite Practice Lead

ENTREPRISE
« Les PME attendent expertise et conseils sur les meilleures pratiques »

Leader des applications de gestion et de la cybersécurité, Catalyst Business Solutions s'est illustré comme un fournisseur d'audit, et dans la mise en œuvre, la mise à niveau, la formation, le support, la revente et la gestion des licences pour les applications commerciales et la cybersécurité. L'entreprise est également fournisseur de solutions NetSuite grâce auxquelles elle assiste les PME et les start-ups dans leur croissance. Dr. Jaleel Polin, NetSuite Practice Lead, nous donne plus de détails.

INTERVIEW

Cio Mag : En quoi consiste les activités de Catalyst Business Solutions ?

Dr. Jaleel Polin : Catalyst est une société de conseil numérique dont le siège se trouve au cœur de la Silicon Valley à San Jose, CAlifornie. Nous sommes présents dans plus de 15 pays dans la région EMOA (Europe, Moyen-Orient et Afrique). Nous aidons nos clients à transformer et à protéger leurs organisations. Nous offrons des services dans les domaines des Applications de Gestion, de la Cybersécurité et de l'Adoption du Cloud. En particulier, Catalyst assiste les PME et les start-ups dans leur croissance grâce à la solution NetSuite.

Nous sommes partenaire Platinum Oracle depuis 2002. Nous couvrons principalement la zone EMOA (Europe, Moyen-Orient et Afrique), et en particulier l'Afrique, les Emirats Arabes Unis et la France. Nous sommes NetSuite Solution Provider (SP) et notre équipe certifiée NetSuite est distribuée dans nos différents bureaux à l'Ile Maurice, en Égypte, au Maroc, au Sénégal, au Cameroun et aux Emirats Arabes Unis.

Cio Mag : Quelles sont les solutions que vous proposez dans le cadre de votre activité NetSuite ?

Dr. J.P : Les solutions Oracle NetSuite sont suffisamment flexibles pour s'adapter aux entreprises de toutes tailles et de tous secteurs. Ces dernières années, notre équipe mondiale a mis en œuvre avec succès des projets ERP dans des secteurs tels que le commerce de gros et de détail, la Fintech, les mines et le commerce électronique, entre autres. Nous avons réussi à numériser les processus financiers, de vente, d'achat, de stocks et de production de nos clients, quels que soient leur secteur d'activité et leur situation géographique.

Cio Mag : Quels sont les services spécifiques que vous fournissez à ces clients ?

Dr. J.P : Nous avons constaté que les petites et moyennes entreprises attendent de nous non seulement une expertise sur l'ERP (NetSuite en l'occurrence) mais aussi des conseils sur les meilleures pratiques adoptées dans leur secteur d'activité.

C'est pourquoi Catalyst met à la disposition de

ses clients une équipe d'experts financiers et d'experts du secteur. Nous disposons d'une équipe de comptables à la fois expérimentés dans plusieurs législations de la région EMOA et experts sur NetSuite Finance. Ils fournissent une assistance approfondie dans la mise en place de plans comptables pour répondre aux normes OHADA, IFRS et GAAP, entre autres.

Ils sont également impliqués dans la configuration des taxes conformément aux réglementations locales. Une fois le système opérationnel, nous assistons nos clients dans divers domaines. Nous les aidons à optimiser l'instance ; et nous nous assurons que le client utilise les KPI, les tableaux de bord et toutes les fonctions analytiques de NetSuite.

Ensuite, nous aidons le client à maintenir les meilleures pratiques d'affaires. Comme toutes les mises à jour de NetSuite sont fournies automatiquement et qu'elles sont gratuites, nous effectuons des contrôles réguliers et proposons de nouvelles fonctionnalités au client.

Enfin, nous nous assurons que la configuration actuelle en place leur permet de relever les nouveaux défis commerciaux et nous leur apportons des améliorations si nécessaire.

Cio Mag : Outre les solutions technologiques, quelles facilités fournissez-vous aux PME pour soutenir leur croissance ?

Dr. J.P : Notre longue expérience dans le monde des affaires nous a permis de comprendre les difficultés quotidiennes des PME à travers le monde. Nous sommes conscients que les investissements informatiques sont coûteux et risqués, et que la gestion de la trésorerie est un défi pour les PME.

Aussi, nous proposons les incitations telles que des tarifs très compétitifs et des facilités de paiement. Nous permettons à nos clients de démarrer le projet avec des exigences minimales, un petit nombre d'utilisateurs clés et les modules essentiels pour gérer leur entreprise.

De même, nous planifions l'implémentation en différentes phases pour faciliter la trésorerie de nos clients et garantir un retour sur investissement rapide. Nous avons la connaissance de nombreuses législations et nous avons l'expérience d'intégration de NetSuite avec de nombreux autres systèmes, qu'il s'agisse de gestion de points de vente, de la paie, de commerce électronique, de système pont bascule, etc.

Par ailleurs, nos équipes sont francophones, anglophones et arabophones et nous sommes disponibles 24/24h et 7/7j grâce à notre présence globale.

Cio Mag : Quel conseil donneriez-vous aux entreprises qui hésitent à investir dans une solution ERP ?

Dr. J.P : Un projet d'implémentation réussi doit être réalisé par une équipe possédant le bon ensemble de compétences, ainsi qu'une compréhension approfondie du contexte local du client.

Nous avons récemment rencontré un client confronté à de nombreux défis après l'échec de la mise en œuvre d'une solution concurrente. Nous avons rétabli la confiance du client dans l'utilisation d'une solution ERP grâce à notre capacité à tenir nos engagements. Nous recommandons qu'au-delà du choix d'une solution technologique, le client s'assure de disposer d'un partenaire expert pour les accompagner dans leur transformation numérique.

Pour plus d'informations sur nos solutions et services, visitez notre site web www.catalyst-us.com ou contactez notre équipe via marketing@catalyst-us.com ■

Propos recueillis par Michaël Tchokpodo

Qui est Dr. Jaleel Polin ?

Dr. Jaleel Polin a plus de 17 ans d'expérience dans la transformation numérique. Il a eu l'occasion de travailler au sein de nombreux environnements, cultures et contextes d'entreprise à travers le monde, principalement en Afrique, au Moyen-Orient, en Europe, en Australie et en Amérique du Nord. Il a participé à plus de 60 projets de mise en œuvre en tant que consultant ERP, chef de projet et directeur de projet.

Aujourd'hui, **Dr. Jaleel Polin** dirige la practice NetSuite chez Catalyst Business Solutions. Il a un profil académique très riche avec une certification NetSuite d'Oracle et un certificat PMP du PMI, USA. **Dr. Polin** a obtenu une maîtrise en stratégie commerciale et informatique de l'université de Portsmouth, au Royaume-Uni, et un doctorat en administration des affaires de l'université Leeds Beckett, au Royaume-Uni.

Il termine actuellement un diplôme en droit à l'Université de Central Lancashire, au Royaume-Uni.

CALENDRIER ÉDITORIAL 2022

LA RÉFÉRENCE DU NUMÉRIQUE EN AFRIQUE

ciomag.com

DOSSIERS THÉMATIQUES NUMÉRIQUES

78 **Février-Mars**

Cybersécurité : lutter contre les vulnérabilités pour impulser l'économie numérique

79 **Mars-Avril**

Agritech : la technologie au service de la souveraineté alimentaire de l'Afrique

80 **Mai-Juin**

Formation et capital humain : les talents et les métiers de demain

Focus : Madagascar, l'île aux grandes ambitions numériques

81 **Juillet-Août**

Commerce électronique : un véhicule pour stimuler l'intégration régionale

82 **Septembre-Octobre**

Identité et gouvernance électronique : bâtir les smart nations africaines

83 **Novembre-décembre**

Fintech : les technologies financières, vecteur de développement du continent

10 AU 14 JUILLET 2023

CIO Mag, en partenariat avec

The Fisher Center For Business Analytics

organise une Expedition Learning dans le cadre prestigieux de

l'Université de Berkeley

Un certificat décerné par le Fischer Center for business Analytics de l'Université de Berkeley

Cette formation certifiante sera assurée par d'éminents professeurs sur le thème :

OpenAI, ChatGPT, éthique, cybersécurité et EGov

cio mag.com — LA RÉFÉRENCE DU NUMÉRIQUE EN AFRIQUE

The University of California Berkeley — Let There Be Light — 1868

The Fisher Center For Business Analytics
Berkeley Haas School of Business

Renseignement et inscription : **info@cio-mag.com**