

LE BIMESTRIEL D'UN CONTINENT EN MARCHÉ - N°17 - JANVIER / FÉVRIER 2019

LA AFRIQUE TRIBUNE



PROSPECTIVE 2019
DES PROJETS QUI FERONT
LA CROISSANCE DE DEMAIN

CONFESSIONNAL
À BÂTONS ROMPUS
AVEC ALAIN JUILLET

CHAMPIONS DU SUD
QUAND L'AFRIQUE OUTILLE
SES « BUSINESS LEADERS »

Péril digital Un front lucratif [POUR QUI ?]

M 03111 - 17 - F. 7,20 € - RD



ZONE CFA 4500 FCSA - MAROC 75 DHS

FAIRE DE LA CYBERSÉCURITÉ UN ATOUT DE L'ÉCONOMIE AFRICAINE

Les technologies de l'information permettent de s'affranchir des distances. Qu'il s'agisse de couvrir de vastes territoires ou de commercer avec des pays étrangers. Ainsi, le numérique fait partie des puissants leviers pour développer les économies africaines. On recense déjà plus de quatre cents millions d'internautes sur le Continent. Le e-commerce y progresse de plus en plus rapidement, avec un revenu de 16,5 milliards de dollars en 2017, selon le cabinet Statista, et les analystes de McKinsey & Company estiment que ce chiffre sera de 75 milliards de dollars en 2025. L'émergence d'une classe moyenne en Afrique participe à cette dynamique avec des usages numériques en nette progression. Pour faire en sorte que cette activité soit durable, elle devra intégrer de plus en plus les questions de cybersécurité. Là encore, la prise de conscience se renforce : la dernière édition (2017) de l'Indice mondial de la cybersécurité établi par l'Union internationale des télécommunications (UIT), l'agence spécialisée de l'ONU, recense une quinzaine de pays africains (Cameroun, Côte d'Ivoire, Maroc, Sénégal, Tunisie,...) parmi la catégorie des nations « matures » dans le domaine de la protection des actifs numériques. Cette évaluation se fonde sur vingt-cinq critères qui couvrent tant le cadre juridique, la maîtrise technologique que la désignation de services administratifs dédiés à la sécurité numérique.

C'est dans ce contexte porteur que les acteurs privés comme Orange Cyberdefense pourront faire bénéficier, notamment à partir de sa base marocaine, le tissu économique africain de son expertise opérationnelle, avec une gamme d'interventions qui va des missions d'audit, d'évaluation et de conseils jusqu'à la supervision de la sécurité des systèmes d'information par son réseau international de Security Operations Centers (SOCs). L'appartenance au réseau mondial des Centres de réponses à incidents (CERTs) d'Orange Cyberdefense constitue alors une source d'information précieuse sur les cyberat-



PHOTO DR

PAR NICOLAS
ARPAGIAN, DIRECTEUR
DE LA STRATÉGIE ET
DES AFFAIRES
PUBLIQUES, ORANGE
CYBERDÉFENSE



PHOTO DR

ET EMMANUEL
CHÉRIET, DIRECTEUR
D'ORANGE
CYBERDÉFENSE MAROC

taques en cours, afin de configurer sans délai les équipements en fonction des modes opératoires constatés chez les premières victimes.

RÉACTION RAPIDE ET MOBILISATION SUR LA DURÉE

La menace numérique ignore les frontières et cherche de plus en plus à viser les sous-traitants des grands groupes internationaux pour tenter de dissimuler leurs tentatives d'atteintes aux systèmes d'information. Le suivi des dispositifs juridiques propres à chaque pays du Continent, avec la présence d'Orange comme opérateur de référence dans nombre d'entre eux, permet à ses experts en cybersécurité de configurer dans les meilleures conditions leurs recommandations en matière de sécurité numérique. Cette capacité à pouvoir travailler avec des partenaires de confiance est particulièrement appréciable en cas de crise : il faut être en mesure de réagir rapidement et de mobiliser les spécialistes sur la durée, afin de préparer au mieux le retour à une situation normale. Ce savoir-faire est complété par un investissement conséquent dans le domaine de la formation pour faire en sorte que les équipes disposent de la maîtrise des nouvelles technologies.

Ce travail avec le monde académique, mais également avec les éditeurs techniques contribue à élaborer des réponses agiles pour faire face aux nouvelles formes de risques. Cette démarche a fait ses preuves au service de la cybersécurité des grands groupes internationaux et des entreprises de taille intermédiaire (ETI) en Europe. Elle sera également bénéfique aux sociétés africaines qui feront le choix d'intégrer le plus tôt possible les règles de la sécurité dans leurs processus.

C'est en adoptant cette stratégie de protection de son activité numérique que l'économie africaine pourra bénéficier dans les meilleures conditions de ces nouvelles formes de production, de commerce et d'organisation nées de la numérisation de l'activité des entreprises, des collectivités et des administrations. ■