E-KARANGÉ

RENCONTRE...

FRANK NZOUETOM

Frank William Nzouetom est un ingénieur spécialiste de la gestion des systèmes d'information et de la gestion des risques opérationnels. Diplômé de l'école d'ingénieurs ESIGELEC (Rouen), il a enrichi sa formation initiale de certifications en management des processus informatiques, en audit et sécurité des systèmes d'information, et a obtenu un certificat Economics for Managers à Harvard Business School. Il a travaillé en France et à l'international, dans des cabinets de conseil tels qu'EY, Mazars ou encore Wavestone. Son implication dans la vie associative professionnelle l'a porté dans de prestigieuses associations spécialisées dans l'intelligence économique, ou il joue toujours un rôle actif sur des questions liées au numérique. Aujourd'hui, Frank est Directeur au sein des activités Conseil de Grant Thornton France et auteur du Lexique Cyber 2022, paru aux éditions Baudelaire.

POURQUOI LES RENCONTRES D'E-KARANGE ?

Les Rencontres d'E-Karangé sont des occasions d'explorer les enjeux de cybersécurité et de protection des données personnelles en Afrique, à travers des discussions avec des experts de la diaspora africaine dans ces domaines.

A chaque épisode, nous rencontrons un acteur de la diaspora qui partage son expertise et son expérience en matière de cybersécurité et de protection des données personnelles en Afrique. Nous discutons des défis actuels et des tendances émergentes dans ces domaines, ainsi que des perspectives et des solutions pour faire face aux menaces et aux risques potentiels.

Nous abordons des sujets tels que la protection des données des utilisateurs, la sécurité des réseaux informatiques, les risques liés aux transactions en ligne, la protection de la vie privée et bien d'autres. Nous explorons également les implications de la cybersécurité et de la protection des données pour le développement économique et social en Afrique.

Rejoignez-nous pour découvrir les enjeux passionnants de la cybersécurité et de la protection des données personnelles en Afrique, et pour découvrir les points de vue de nos invités experts de la diaspora à travers notre podcast E-Karangé disponible sur Spotify et Anchor.

Bonne lecture !

Pourriez-vous nous expliquer ce qu'est la cyber sécurité de manière simple pour des non experts ?

La cybersécurité peut s'expliquer par un exemple très simple. Que nous soyons une personne physique ou morale, nous avons un certain nombre d'informations à protéger, celles relatives à notre vie privée, celles stratégiques et donc relatives à notre entreprise ou business etc. Nous avons aussi une certaine exposition en ligne, sur internet, car nous disposons par exemple de messageries, consultons et interagissons via des sites web etc. En réalité c'est cet ensemble d'informations et de données que nous devons protéger, tant dans l'espace numérique que dans le monde réel.

C'est cette protection qui est appelée la cybersécurité, c'est-à-dire la sécurité dans le monde cyber, face aux menaces potentiels.

Comment se présente l'écosystème africain en termes de cyber sécurité à l'heure actuelle ?

Nous pouvons en effet donner une image représentative de la cybersécurité en Afrique. Commençons par l'un des piliers de base, qui est le pilier légal.

En Afrique, quel que soit le pays visé, il est à noter que la quasi-totalité des pays se sont doté de cadre juridique en matière de cybersécurité. Dans ce cadre juridique il est indiqué un certain nombre de comportements considérés comme délictuels et assortis de sanctions imposés par les pouvoirs publics ; Par exemple il n'est pas autorisé de se connecter à un système d'information sans l'autorisation du responsable.

Nous avons également le pilier relatif à la formation, bien qu'étant encore embryonnaires, il y a quelques initiatives mis en place, comme au Sénégal avec l'université numérique du Sénégal qui propose un certain nombre de formation en la matière, tout comme au Gabon, en Côte d'Ivoire et au Cameroun. Il y a donc de belles initiatives en marche. Au delà, il y a le pilier de la sensibilisation, avec deux volets, la sensibilisation du grand public et celui des entreprises. En ce qui concerne la sensibilisation des personnes morales, il y a des actions faites notamment au sein des grandes entreprises disposant de chartes et gouvernances qui prennent en compte la sensibilisation et formation des collaborateurs aux risques cyber. En ce qui concerne le grand public, force est de constater qu'il y a une grande disparité entre les pays. Il existe des pays dans lesquels il n'y a aucune stratégie de sensibilisation matérialisée. A contrario d'autres pays s'activent vraiment dans cette lancée.

Nous pourrions par ailleurs rajouter un dernier pilier qui est celui de la protection des données personnelles. Sur ce sujet, il y a deux vitesses, avec les pays de la CDEAO qui ont quasiment pour la plupart une loi encadrant la protection des données personnelles.
En Afrique centrale, nous avons quelques pays comme le Gabon et le Tchad qui sont également outillés en ce sens. Le Cameroun par contre n'est pas encore doté de ce type de dispositif juridique, ce qui peut paraitre surprenant au regard de la taille de la population dite « connectée » et la maturité intellectuelle de cette population, nous avons bon espoir que les choses vont évoluer dans un futur proche.
En définitive, et si on se limite à ces quatre piliers, nous pouvons constater que les choses sont en train de se mettre en place, que les vitesses ne sont pas les mêmes d'un pays à un autre. Mais il y a une prise de conscience qui est évidente tout au moins au niveau des pouvoirs publics.

Au regard des standards internationaux, l'Afrique a t-elle fait des progrès en général ?

S'il y a des progrès à souligner, c'est le nombre de cyberattaques frappant les entreprises implantées en Afrique. Le secteur financier par exemple est sujet de cyberattaques de plus en plus régulières. Cela a été le cas, en Angola (Banco Sol), en Afrique du Sud avec la NedBank, ou encore au Mali avec la cyberattaque de la BOA. Le problème que les spécialistes soulignent est le fait que les institutions, dès lors qu'elles sont victimes de ces incidents, nient leur survenance.

Cette démarche est très problématique pour la gouvernance d'ensemble de ce fléau. Nous comprenons bien les enjeux en termes de business, que cela implique mais cela dénote aussi du manque de préparation à la gestion de ces incidents. Partout dans le monde, sauf en Afrique, quant une entreprise est victime d'une cyberattaque, il est mis en place un canal de communication. Par exemple lorsque la cyberattaque a impacté des données personnelles de clients ou collaborateurs, il y a un cadre de communication mis en place. Et tout cela doit être prévu en amont.
Cependant en Afrique la pratique est plutôt de nier leur survenance alors que les spécialistes voient et parfois ont accès aux données ayant fuitées. C'est en cela qu'il y a un vrai travail à faire et un réel équilibre à trouver entre la communication de crise et la protection de l'image des institutions victimes de ces situations, notamment en Afrique francophone.

Identifiez-vous à l'heure actuelle des barrières à l'évolution de la cyber sécurité globalement sur le continent ?

Nous avons en effet la problématique de la sensibilisation. Par exemple quand des institutions financières limitent ou retardent leur communication vis-à-vis du grand public. Il faudrait montrer à ce grand public que les cyberattaques sont des fléaux réels et d'envergure croissante. Que l'on en est finalement victime comme pour une maladie, mais que nous avons les prédispositions pour y faire face. Ce manque de sensibilisation du grand public est un frein à la gestion d'une crise cyber. Le deuxième point est celui de densifier et massifier les offres de formation. La majorité des experts africains sont de la diaspora, quand bien même des initiatives sont lancées localement. Je prends pour exemple, le CESIA (Gabon) qui a lancé une initiative permettant de faire des reporting en matière de maturité cyber à des Etats africains.

Il y a aussi le Cyberobs qui est un carrefour de rencontre en Côte d'Ivoire d'experts en cybersécurité pour discuter des technologies, tendances et autres sujets en matière de cybersécurité. Et il y a enfin des réalisations plutôt littéraires, avec des œuvres comme le lexique cyber, dont je suis l'auteur et qui a pour objectif de partager au grand public les notions de base en termes de cybersécurité. Cet œuvre est en français pour palier à l'inaccessibilité de certaines productions en la matière, souvent en anglais et en des termes parfois techniques.

L'ensemble de ces actions doivent cependant être fédérées pour avoir l'effet escompté au niveau continental.

Quels sont les conseils pouvant permettre de transcender ces barrières propres à nos réalités/ contexte ?

En mon sens il faut faire évoluer l'offre de formation de nos états pour l'arrimer aux enjeux de nos économies, en préparant les jeunes filles et femmes pour transcender la question du genre dans le numérique et surtout cyber, tout en mettant en place des opportunités de formation à distance.

Il faut aussi faire appel à la diaspora, qui a énormément de chose à apporter, en termes de stratégie, de formation ou d'expérience. Partant de la réalité de nos états, il n'y a pas lieu d'écarter d'options qui peuvent être bénéfiques pour tous.

Enfin il faut au niveau de nos Etats, de véritables stratégies de sécurisation de nos systèmes d'informations.

Que pensez-vous de l'impact de la régulation harmonisée (notamment la convention de Malabo) sur l'avancée de la cyber sécurité sur le continent ?

Il existe en effet des dispositifs supranationaux en Afrique, comme la convention de Malabo. Cette convention date des années 2014, qui est édicté par l'UA, avec pour vocation d'encadrer la sécurité des systèmes d'informations au niveau de nos pays, moyennant ratification.

Malheureusement, à ce jour la ratification de ce texte n'est pas encore universelle. Ces régulations sont pourtant très importantes, quand il y a par exemple une cyberattaque en Côte d'Ivoire, rien n'indique que les malfaiteurs sont en Côte d'Ivoire.
Il faut donc organiser les représailles et si des textes ne facilitent pas la collaboration des états pour les poursuites et l'application des peines, ces actions seront difficilement mises en œuvre. Le maître mot est d'harmoniser les règles pour faciliter la collaboration et la coopération dans la lutte contre ces cybercriminels.

En cela j'appelle de tous mes vœux l'Union Africaine à renforcer son leadership en termes de cybersécurité, car il en va de la sécurité de nos économies.

Pouvez-vous nous rappeler les enjeux et avantages pour le continent à se positionner comme un cadre « cyber-sécure » ?

Au-delà des enjeux traditionnellement connus, je vais souligner les enjeux économiques. Aujourd'hui, l'Afrique est une terre de croissance pour les pays tiers.

Par exemple, beaucoup d'entreprises européennes sous-traitent une partie de leurs activités en Afrique ou tout simplement viennent s'y installer.

L'élément fondamental dans ces circonstances, est que compte tenu du cadre de protection des données qui prévaut en France notamment, l'entreprise française va exiger un minimum de maturité sécuritaire aux entreprises qui vont soumissionner (assurances cyber, désignation de responsable de SI), et il est certain que c'est le soumissionnaire le mieux outillé qui sera retenu.

Ainsi la cybersécurité est un outil de marketing, un avantage de compétitivité sur le marché économique pour nos entreprises africaines.

Il faut donc que nous ayons un cadre juridique clair, pour donner la chance à nos entreprises et startups de se faire une place sur le marché économique international.

Comment pensez-vous que les experts de la diaspora peuvent contribuer à l'évolution de la cyber sécurité en Afrique ?

En effet les experts de la diaspora ont leur rôle à jouer, mais ce qui va potentiellement leur manquer, c'est avoir les moyens d'impacter à une échelle assez importante.

Pour avoir cet impact, il faut une rampe de décollage qui ne peut leur être offert que par les dirigeants et nos institutions africaines. Par exemple aujourd'hui, il y a un vrai sujet pour nos startups relativement à la sécurisation de leurs données et secrets d'affaires, dans un monde d'intelligence économique accru.

Ces startups ont besoins de moyens pour y parvenir dont un financement, une infrastructure et un accompagnement.
Nous devons être force de propositions et acteurs de ces évolutions.

PERSPECTIVES

> "IL Y A ÉNORMÉMENT À FAIRE, ET DE LA PLACE POUR TOUT LE MONDE !"

Nous devons continuer nos actions de relais, de communication et d'évangélisation autour de la cybersécurité en Afrique.

J'ai bon espoir que par ce biais, nous ferons de nos apports, en plus de l'existant, quelque chose de stable, fiable et bénéfique à tout le continent !

Il y a énormément à faire, et de la place pour tout le monde !

Frank NZOUETOM

E-Karangé

NOS RÉSEAUX :
www.ekarange.com
E-KARANGÉ
E-KARANGÉ
E-KARANGÉ

CONTACTS :
contact@ekarange.com
+33 (0)7 53 67 22 64
+221 78 181 30 92