

CYBERSÉCURITÉ EN CENTRAFRIQUE : UN DÉFI NATIONAL ET UN LEVIER DE CONFIANCE

Protéger le présent, préparer l'avenir

Par **Sostene NGUEMBI**
*Consultant en Cybersécurité
Managing Director, KSN Technologies*

SOMMAIRE

- ✓ Un secteur en pleine mutation
- ✓ Les banques en première ligne
- ✓ Une volonté politique affirmée
- ✓ Des partenaires technologiques engagés
- ✓ Une priorité pour la confiance numérique

La République Centrafricaine est engagée dans une transition numérique qui touche aussi bien les institutions publiques que les entreprises privées. Mais cette évolution s'accompagne d'un défi majeur : la cybersécurité. Dans un contexte mondial marqué par la recrudescence des cyberattaques, protéger les données, les infrastructures et les communications est devenu une priorité nationale.

Un secteur en pleine mutation

Avec l'expansion des services mobiles et d'Internet haut débit, portée par des opérateurs comme Orange Centrafrique et Moov Africa et Telecel, la connectivité s'accroît rapidement dans le pays. Cette ouverture numérique favorise le commerce en ligne, les services bancaires digitaux et les démarches administratives dématérialisées. Mais elle expose aussi les utilisateurs et les entreprises à de nouveaux risques : piratage, fraude financière, vol de données personnelles, attaques par ransomware.

Les banques en première ligne

Les établissements financiers comme la Banque Populaire Maroco-Centrafricaine (BARC), Ecobank, la BSIC ou la CBCA ont été parmi les premiers à investir dans des solutions de cybersécurité pour protéger leurs transactions et rassurer leurs clients. La progression des services de Mobile Money et des paiements électroniques rend indispensable le renforcement des dispositifs de sécurité : authentification renforcée, chiffrement des données, surveillance en temps réel des opérations.

L'action des pouvoirs publics

Le Ministère des Postes, des Télécommunications et de l'Économie Numérique, en collaboration avec d'autres départements, travaille à l'élaboration d'une stratégie nationale de cybersécurité. Celle-ci doit fixer un cadre réglementaire pour la protection des données, encourager la coopération internationale et développer des compétences locales dans le domaine. Des discussions sont également en cours pour mettre en place un Centre national de réponse aux incidents de cybersécurité (CERT), afin de détecter et neutraliser rapidement les menaces.

Le rôle des acteurs technologiques

Des entreprises spécialisées comme KSN Technologies apportent leur expertise en accompagnant les institutions et les grandes organisations dans la mise en place de solutions de sécurité adaptées. Cela inclut la modernisation des infrastructures IT et télécoms, la mise en œuvre de solutions Microsoft Defender ou équivalentes, ainsi que la formation du personnel pour adopter les bonnes pratiques numériques.

Une priorité pour la confiance numérique

La cybersécurité en Centrafrique dépasse le simple aspect technique : elle est désormais un enjeu de souveraineté et de confiance. Sans infrastructures numériques fiables et sécurisées, il sera difficile d'attirer les investisseurs, de développer l'e-gouvernement ou de favoriser l'inclusion financière par le digital.

La mobilisation des opérateurs télécoms, des banques, du gouvernement et des partenaires technologiques est essentielle pour bâtir un écosystème numérique sûr et durable. C'est à ce prix que la République Centrafricaine pourra tirer pleinement profit des opportunités offertes par la transformation digitale tout en protégeant ses citoyens et ses institutions.

Protéger le présent, préparer l'avenir

Alors que le numérique devient un moteur de développement en Afrique, la République Centrafricaine vit une transformation profonde. L'essor d'Internet, des services mobiles et des paiements digitaux ouvre de nouvelles perspectives pour l'économie et l'administration. Mais cette ouverture expose aussi le pays à un défi majeur : la cybersécurité.

Une connectivité en plein essor

Avec des opérateurs comme Orange Centrafrique et Moov Africa, l'accès à Internet et aux services mobiles s'est considérablement développé ces dernières années. Les usages numériques explosent : réseaux sociaux, e-commerce, démarches administratives en ligne, sans oublier l'essor du Mobile Money.

Cependant, cette révolution numérique accroît aussi les risques : attaques par ransomware, fraudes bancaires, phishing, piratage de données sensibles. « Chaque nouveau service numérique doit s'accompagner d'une protection renforcée », rappelle un expert local en sécurité informatique.

Les banques en première ligne

Le secteur bancaire est particulièrement exposé. Des institutions comme la BARC, Ecobank, la BSIC ou la CBCA investissent déjà massivement dans la sécurisation de leurs systèmes. Authentification multi-facteurs, cryptage des données, surveillance des transactions en temps réel : autant de dispositifs devenus indispensables pour protéger la confiance des clients.

Une volonté politique affirmée

Le Ministère des Postes, des Télécommunications et de l'Économie Numérique prépare actuellement une stratégie nationale de cybersécurité. Celle-ci devrait inclure un cadre réglementaire adapté, la mise en place d'un Centre national de réponse aux incidents (CERT) et le développement de programmes de formation pour les fonctionnaires et les jeunes talents. « La cybersécurité n'est pas seulement une affaire de technologie, c'est une question de souveraineté nationale », souligne un haut responsable du ministère.

Des partenaires technologiques engagés

Aux côtés de l'État, des entreprises spécialisées comme KSN Technologies accompagnent les institutions et organisations dans leur transition numérique sécurisée. Déploiement de solutions de cybersécurité, infrastructures IT et télécoms modernisées, formations de haut niveau : autant d'initiatives pour renforcer la résilience face aux menaces.

Une priorité pour la confiance numérique

La cybersécurité est désormais un levier de confiance. Elle conditionne l'essor de l'e-gouvernement, l'inclusion financière par le digital et l'attractivité du pays pour les investisseurs.

La République Centrafricaine avance encore prudemment, mais les premiers jalons sont posés. Avec la mobilisation des opérateurs télécoms, des banques, des institutions publiques et des partenaires technologiques, le pays peut bâtir un écosystème numérique sûr et durable.



Sostene Nguembi
CEO / Managing Director
KSN Technologies

En charge de la stratégie et du développement de la société et du groupe, Sostène initie et conduit toutes les activités technologiques du groupe.

Ingénieur de Recherche et Développement en Microélectronique Radiofréquence et Hyperfréquence. Spécialiste en Conception et Procédés Technologiques des composants très hautes fréquences et nano électronique. Sostene est aussi responsable technique du Broadcasting, il dirige une équipe qui travaille sur la conception et réalisation des schémas de transmission et de diffusion innovante des signaux vidéos et audio basses/hautes fréquences (Hertzien, Satellitaire) et IP. Des activités menées et co développées avec nos partenaires Telcos et opérateurs de satellites.

Il accompagne et conseille plusieurs personnalités du premier rang sur des stratégies du développement et de transformation digitale ainsi que sur la communication digitale.

Aussi diplômé de Cyber University et Paris Sorbonne en tant que analyste et consultant en cybersécurité. Certifié Cisco SBTO (700-755) et Cisco ICS (700-150)...

Très grand passionné d'aviation, de basket ball et du cyclisme, il consacre ses temps libres dans du bénévolat et actions caritatives.