GUIDE DES BONNES PRATIQUES EN CYBERSÉCURITÉ EN AFRIQUE

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

SOMMAIRE

KSN TECHNOLOGIES +33 07 81 44 64 35 www.ksn-technologies.com

Introduction

La révolution numérique en Afrique transforme les économies, la gouvernance et la société :

- Croissance des services financiers mobiles (ex. M-Pesa, Mobile Money).
- Digitalisation des administrations publiques (e-gov).
- Développement rapide des PME technologiques et start-ups.
- Accès massif aux smartphones et à Internet.

Mais cette évolution s'accompagne de menaces : phishing, ransomwares, fraudes bancaires, espionnage, cyberattaques sur les infrastructures critiques (énergie, santé, transports).

Ce manuel vise à fournir des bonnes pratiques opérationnelles et adaptées au contexte africain, pour les entreprises, administrations et citoyens.

🔑 1. Gestion des accès et identités

Bonnes pratiques

- Utiliser des mots de passe robustes : au moins 12 caractères, mélange de lettres, chiffres, symboles.
- Éviter de réutiliser les mêmes mots de passe.
- Mettre en place une authentification multi-facteurs (MFA).
- Créer des profils utilisateurs selon le principe du moindre privilège (chaque utilisateur n'accède qu'à ce dont il a besoin).
- Désactiver immédiatement les comptes d'anciens employés.

Exemple africain

Dans plusieurs administrations africaines, des comptes génériques (« admin », « test ») sont exploités par les cybercriminels. La mise en place d'une politique stricte de gestion des identités permet de réduire ce risque.

🖥️ 2. Protection des systèmes et infrastructures

Bonnes pratiques

- Installer régulièrement les mises à jour de sécurité (Windows, Linux, applications métiers).
- Utiliser un antivirus et un pare-feu adaptés.
- Segmenter le réseau (séparer bureautique, serveurs critiques, Internet invité).
- Sécuriser les accès Wi-Fi (WPA2/WPA3, pas de mots de passe par défaut).
- Utiliser des solutions de surveillance et détection d'intrusion (IDS/IPS).

Exemple africain

- Dans certaines universités, les réseaux Wi-Fi ouverts sont utilisés pour lancer des attaques. Une segmentation réseau et un contrôle d'accès réduisent ces risques.

📩 3. Prévention du phishing et des fraudes

Bonnes pratiques

- Vérifier l'adresse e-mail d'expédition avant de cliquer.
- Ne jamais ouvrir une pièce jointe suspecte.
- Se méfier des messages demandant un transfert urgent d'argent.
- Former régulièrement les employés à reconnaître les techniques d'ingénierie sociale.
- Mettre en place des filtres anti-phishing sur la messagerie.

Exemple africain

Les fraudes au mobile banking sont fréquentes (SMS ou appels frauduleux). Les campagnes de sensibilisation (ex. banques au Kenya, Nigéria) ont réduit les pertes.

🔐 4. Sauvegarde et continuité d'activité

Bonnes pratiques

- Effectuer des sauvegardes régulières (quotidiennes pour les données critiques).
- Stocker les sauvegardes sur un support externe ou dans le cloud sécurisé.
- Tester la restauration des données tous les 3 à 6 mois.
- Définir un Plan de Continuité d'Activité (PCA) et un Plan de Reprise après Sinistre (PRA).

Exemple africain
Lors d'une attaque par ransomware sur une mairie en Afrique de l'Ouest, seules les données sauvegardées sur disque externe ont pu être récupérées.

📱 5. Sécurité mobile et finance numérique

Bonnes pratiques

- Protéger son smartphone par code ou biométrie.
- Ne pas installer d'applications hors stores officiels.
- Ne jamais partager ses codes de Mobile Money.
- Activer le chiffrement du téléphone.
- Utiliser des applications bancaires officielles uniquement.
-

Exemple africain

Les fraudes par SIM swap (vol de carte SIM pour détourner les comptes bancaires) sont en forte hausse en Afrique australe. L'authentification forte et la vigilance des opérateurs télécoms réduisent ces risques.

👥 6. Gouvernance et sensibilisation

Bonnes pratiques

- Nommer un responsable cybersécurité (CISO ou référent).
- Mettre en place une politique écrite d'usage des systèmes d'information.
- Organiser des sessions de sensibilisation régulières (phishing, bonnes pratiques).
- Intégrer la cybersécurité dès la conception des projets numériques.

Exemple africain

Au Maroc, plusieurs ministères ont mis en place des formations obligatoires en cybersécurité pour leurs agents, ce qui a permis de réduire fortement les incidents.

🤝 7. Cadre légal et coopération

Bonnes pratiques

- Respecter les lois locales et régionales :
- NDPR (Nigeria Data Protection Regulation).
- PDPL (Kenya).
- RGPD (pour échanges avec l'UE).
- Collaborer avec les CERT/CSIRT nationaux (Computer Emergency Response Teams).
- Participer à des exercices régionaux de cyberdéfense.
- Échanger des informations sur les menaces entre entreprises, États et ONG.

Exemple africain

L'Union Africaine a adopté la Convention de Malabo (2014) sur la cybersécurité et la protection des données personnelles, mais son application reste encore inégale selon les pays.

Conclusion

La cybersécurité en Afrique est une condition essentielle du développement numérique. Chaque citoyen, entreprise et administration a un rôle à jouer :

- Les utilisateurs doivent adopter de bons réflexes.
- Les organisations doivent sécuriser leurs infrastructures.
- Les États doivent renforcer la coopération et le cadre légal.

En appliquant ces bonnes pratiques, l'Afrique peut bâtir un écosystème numérique sûr, résilient et souverain, garantissant la confiance des citoyens et des investisseurs.

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 électroniques.
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.