République du Cameroun
Paix- Travail - Patrie
Ministère des Postes et Télécommunications

Republic of Cameroon
Peace- Work- Fatherland
Ministry of Posts and Telecommunications

TROISIÈME FORUM NATIONAL SUR LA CYBERSÉCURITÉ ET LA LUTTE CONTRE LA CYBERCRIMINALITÉ.

Thème:

Mécanismes de Gestion de La Sécurité des Données des Clients dans les Systèmes Bancaires

ADOLPHE NKENNI
Chef de Département Sécurité

AFRILAND FIRST BANK

SOMMAIRE

Catégories de données sensibles collectées par le secteur bancaire

Concepts normatifs généraux de traitement des données

Rôle du Core Banking dans la protection des données

Mesures spécifiques pour sécuriser les données bancaires

Recommandations pour les utilisateurs des services financiers.

Enjeux de la protection des données à l'ère de l'open Banking

LES CATÉGORIES DE DONNÉES SENSIBLES COLLECTÉES PAR LE SECTEUR BANCAIRE

- **Informations personnelles :**
  - **Nom, prénom, adresse, numéro de téléphone.**
  - **Informations d'identité nationale (CNI, passeport).**

- **Données financières :**
  - **Détails des comptes bancaires.**
  - **Historique des transactions et revenus.**

- **Données biométriques :**
  - **Empreintes digitales, reconnaissance faciale.**

- **Données réglementaires :**
  - **Statut fiscal, justificatifs d'origine des fonds.**

CONCEPTS NORMATIFS GÉNÉRAUX DE TRAITEMENT DES DONNÉES

- **Principes fondamentaux :**

- Légalité : Respect des lois en vigueur (Loi n° 2010/012).

- Transparence : Informer les clients sur l'utilisation de leurs données.

- Consentement : Recueillir l'approbation explicite avant le traitement.

- **Droits des utilisateurs :**

- Accès, rectification et suppression des données.

- Opposition à certaines utilisations des données.

- **Normes internationales appliquées : PCIDSS, RGPD, ISO 27001.**

RÔLE DU CORE BANKING DANS LA PROTECTION DES DONNÉES

- Qu'est-ce que le core Banking ?

- Une plateforme centrale pour la gestion des opérations bancaires.

- Contributions à la sécurité :

- Cryptage des données en temps reel et au repos

- Centralisation et gestion des accès pour réduire les risques.

- Évolutions récentes :

- Ajout de systèmes de détection des fraudes.

- Conformité accrue avec les réglementations locales.

MESURES SPÉCIFIQUES POUR SÉCURISER LES DONNÉES BANCAIRES

- **Infrastructure :**

- Serveurs sécurisés avec des pare-feu robustes nouvelle generation.
- Systèmes de sauvegarde et de récupération des données.

- **Cybersécurité :**

- Détection proactive des menaces.
- Authentification multi-facteurs pour les utilisateurs.

- **Formation et audits :**

- Sensibilisation du personnel aux bonnes pratiques.
- Audits réguliers des systèmes pour identifier les vulnérabilités.

ENJEUX DE LA PROTECTION DES DONNÉES À L'ÈRE DE L'OPEN BANKING

- **Opportunités :**

- Facilitation des partenariats entre banques et fintechs.

- Personnalisation des services grâce à une meilleure compréhension des données.

- **Risques :**

- Cibles privilégiés des cybercriminels

- Vulnérabilités accrues en cas de partage mal sécurisé.

- Gestion complexe des consentements clients.

- **Exigences :**

- Utilisation d'API conformes et sécurisées.

- Surveillance continue des flux de données entre partenaires.

RECOMMANDATIONS POUR LES UTILISATEURS DES SERVICES FINANCIERS

- **Sécurité Personnelle :**

- Créer des mots de passe complexes et les changer régulièrement.

- Ne jamais partager ses identifiants ou codes avec des tiers.

- **Vigilance en ligne :**

- Vérifier l'authenticité des plateformes bancaires.

- Éviter les réseaux Wi-Fi publics pour effectuer des transactions sensibles.

- **Collaboration avec les banques :**

- Activer les alertes de transactions.

- Signaler immédiatement toute activité suspecte.

CONCLUSION :

- **Synthèse :**

- La protection des données est essentielle pour maintenir la confiance.

- Les banques doivent s'adapter aux évolutions technologiques.

- **Perspectives :**

- Investissement dans des technologies avancées.

- Collaboration entre parties prenantes pour des normes renforcées.

- **Appel à l'action :**

- Sensibiliser les utilisateurs sur leur rôle dans la sécurité des données.