Recommandations essentielles pour la sécurité des Services Financiers Numériques

Recommandations essentielles pour la sécurité des Services Financiers Numériques.

Les lignes directrices de l'annexe 1 à 5 sont proposées pour adoption

Résumé des lignes directrices

1. Recommandations pour les régulateurs pour atténuer les vulnérabilités SS7: - détails sur les recommandations pour les régulateurs des services financiers numériques et les opérateurs de réseaux mobiles pour atténuer les effets des vulnérabilités SS7.

2. Recommandations pour protéger contre les risques de carte SIM des services financiers numériques et la fraude de remplacement de carte SIM: - guide et recommandations pour les régulateurs et les fournisseurs pour atténuer les vulnérabilités de carte SIM telles que les remplacements de carte SIM, le recyclage de carte SIM et les attaques sur les cartes SIM telles que les attaques binaires par voie hertzienne.

3. Meilleures pratiques de sécurité pour les applications mobiles: meilleures pratiques de sécurité pour les applications de services financiers mobiles que les régulateurs des services financiers numériques peuvent adopter en tant que lignes directrices.

4. Modèle de MOU entre le régulateur des télécommunications et la banque centrale sur la sécurité des services financiers numériques: - comprend des clauses qui abordent la sécurité des services financiers numériques que les régulateurs devraient considérer pour adoption ou intégrer dans des MOU existants.

5. Cadre de compétence pour les consommateurs des services financiers numériques: Le Cadre de compétence pour les consommateurs des services financiers numériques fournit des orientations aux décideurs politiques, aux régulateurs nationaux et aux fournisseurs de services financiers numériques lors de l'élaboration de programmes de sensibilisation et de littératie des consommateurs en tant que partie de la stratégie des services financiers numériques/inclusion financière. Voir le document complet via: https://figi.itu.int/wp-content/uploads/2022/06/22-00239_DFS-Consumer-Competency-Framework_F.pdf

Voir les détails des documents mentionnés de 1 à 4 dans l'annexe.

Annexe 1 .

1 Recommandations pour les régulateurs pour atténuer les vulnérabilités SS7

Les canaux de communication USSD et SMS avec lesquels l'utilisateur communique avec le fournisseur de services financiers numériques reposent sur le protocole hérité de Signaling System 7, qui a depuis longtemps été "brisé" et avec de nombreuses vulnérabilités publiées, certaines datant de plus de 20 ans, ce qui permet aux attaquants de commettre des fraudes, de compromettre les services financiers numériques et de voler des fonds par des prises de contrôle de compte, des interceptions de services financiers numériques, des attaques de déni de service, etc.

Les Rapport technique sur les failles du SS7 et les mesures d'atténuation applicables aux transactions des services f inanciers numériques contiennent des détails sur les recommandations pour les régulateurs de services financiers numériques et les opérateurs de réseaux mobiles pour atténuer les vulnérabilités SS7. Ces recommandations sont résumées ci-dessous.

1.1 Orientations réglementaires pour faire face aux vulnérabilités causées par SS7

a) **Coordination réglementaire: un** memorandum d'entente (MOU) bilatéral relatif aux services financiers numériques (SFN) devrait être mis en place entre le régulateur des télécommunications et la Banque centrale sur SS7. Un exemple de MOU est inclus à l'Annexe B du rapport technique sur les vulnérabilités de SS7 et les mesures de mitigation pour les transactions de services financiers numériques. Le MOU devrait inclure les modalités de création d'un Comité de travail conjoint sur la sécurité et les questions liées aux risques des SFN qui abordent SS7.
b) **Inciter l'industrie:** créer des programmes d'incitation avec l'industrie pour promouvoir le développement de contre-mesures dans le domaine de la lutte contre la fraude Telcom-SFN.
c) **Inciter les opérateurs et les fournisseurs:** établir une réglementation qui transfère les dommages financiers de la fraude SFN aux fournisseurs SFN et aux télécoms, créant ainsi un incitant financier à agir.
d) **Éducation pour les régulateurs des télécommunications et des services financiers sur les vulnérabilités de SS7 et leur impact sur les SFN:** les régulateurs des télécommunications et financiers du monde entier doivent être conscients des risques et surtout être conscients qu'il existe des solutions pour atténuer ces risques.
e) **Passerelle de validation IMSI:** une passerelle de validation IMSI peut être utilisée pour valider aux SFNP et aux banques que le véritable client enregistré utilise le système via USSD pour que les SFNP puissent détecter l'interception USSD.
f) **Les régulateurs des télécommunications doivent établir des mesures de sécurité de base pour chaque catégorie (2G/3G/4G/5G):** les régulateurs des télécommunications sont encouragés à établir des mesures de sécurité de base pour chaque catégorie (2G/3G/4G/5G) qui doivent être mises en œuvre par les opérateurs de télécommunications pour garantir un environnement d'interconnexion plus sécurisé.
g) Les opérateurs de réseaux mobiles et les opérateurs SFN devraient prendre en compte les contrôles décrits dans les sections 1.2 et 1.3 ci-dessous.

1.2 Contrôles MNO pour faire face aux vulnérabilités SFN causées par SS7

a) **Chiffres GSM sécurisés pour le trafic de réseau radio:** L'opérateur mobile doit veiller à l'utilisation d'un chiffrement radio sécurisé entre les appareils des utilisateurs et les stations de base.

b) **Délai de session:** utiliser un délai de session pour USSD et STK pour réduire les risques d'attaques de l'homme du milieu.
c) **Masquage du PIN USSD:** Déployez le masquage du PIN USSD chaque fois que possible.
d) **Sécuriser et surveiller le trafic du réseau central:** Utiliser un TLS v1.2 ou supérieur pour sécuriser la connexion entre le SMSC GW, USSD GW et le serveur d'application SFN.
e) **Limiter l'accès aux traces et journaux:** Assurez-vous qu'un processus auditable est en place pour examiner l'accès aux traces et journaux sur les interfaces qui utilisent des protocoles intrinsèquement insécurisés. Les PINs USSD ne doivent pas être enregistrés dans les enregistrements de données d'événements.
f) **Filtrage SMS:** Les attaquants à distance comptent sur les réseaux mobiles pour livrer des SMS binaires aux téléphones des victimes et vice versa. Les opérateurs mobiles doivent mettre en œuvre le blocage de la capacité à envoyer et à recevoir des messages binaires tels que les SMS OTA. De tels SMS ne doivent être autorisés que depuis des sources autorisées.
g) **Routage SMS domestique:** il s'agit de l'interdiction de tous les SMS sortants et entrants, à l'exception de ceux acheminés via les hôtes du réseau domestique. Les messages OTA avec codage STK des abonnés domestiques doivent être restreints pour être envoyés uniquement à/par la plate-forme MNO et non à d'autres abonnés.

1.3 Contrôles du fournisseur SFN pour faire face aux vulnérabilités SFN dues à SS7

Les opérateurs SFN devraient envisager d'adopter les contrôles suivants pour atténuer les risques SS7.

a) Délai de session: utiliser un délai de session pour USSD et STK pour réduire les risques d'attaques de l'homme du milieu, les messages OTP pour SFN devraient également avoir un délai de session.
b) Limites de transaction pour les canaux insécurisés: fixer des limites de transaction pour les retraits et les transferts de clients à travers des canaux insécurisés tels que USSD.
c) Éducation des utilisateurs: les utilisateurs SFN doivent être formés sur la manière de s'engager de manière s

Annexe 2 .

Recommandations de sécurité pour protéger contre les risques liés aux cartes SIM SFN et les fraudes de remplacement de SIM.

1 Les vulnérabilités de la SIM

Les institutions financières ont adopté des moyens numériques et continuent de proposer des produits financiers sur des applications mobiles telles que les services supplémentaires non structurés (USSD) et la banque STK, ce qui rend les services financiers disponibles n'importe où, n'importe quand à travers des séquences d'interactions via les données de services supplémentaires non structurés (USSD), le service de messagerie court (SMS) et internet. Les interactions entre l'utilisateur mobile et le réseau sont authentifiées avec la carte SIM. Cependant, il y a eu une augmentation des risques de fraude sur les SIM en raison des menaces provenant notamment des échanges de SIM, des attaques de SIM jacker et du recyclage et du transfert de numéros de SIM.

1.1 Fraude d'échange de SIM

La fraude d'échange de SIM est devenue une tactique courante utilisée pour prendre le contrôle des comptes. Dans une fraude d'échange de SIM, un fournisseur de téléphonie est trompé pour émettre un remplacement de la SIM d'une victime à un fraudeur, ce qui leur permet de prendre le contrôle d'un compte SFN qui se fonde sur le mot de passe à usage unique par SMS (OTP) ou USSD pour l'authentification.

1.2 Risques de recyclage de SIM

Les risques de recyclage de SIM sont liés à la dépendance des numéros de téléphone, Mobile Station Integrated Services Digital Network (MSISDN) en tant que numéros de compte SFN primaires. Les fournisseurs de téléphonie réassignent les numéros de téléphone qui sont en sommeil ou considérés comme ayant été abandonnés (non utilisés dans une période spécifique). La réassignment du numéro de téléphone peut effectivement conduire à une prise de contrôle du portefeuille SFN associé au numéro si le fournisseur SFN n'est pas informé du changement de propriété.

1.3 Attaque Binary Over the Air (SIM jacker)

L'attaque SIM jacker exploite une vulnérabilité dans une bibliothèque de cartes SIM appelée le navigateur S@T. Un message texte binaire formaté spécialement est envoyé au téléphone de la victime, qui contient un ensemble de commandes à exécuter par l'environnement navigateur S@T sur la carte SIM. Les commandes peuvent instruire le téléphone d'exfiltrer ces informations, de forcer l'appareil mobile à initier une demande USSD, de faire un appel téléphonique ou d'envoyer un message.

2 Orientations réglementaires pour atténuer les risques de SIM (remplacement de SIM, clonage de SIM, recyclage de SIM et attaques par l'air binaire):

a) **Coordination réglementaire: -** Une entente bilatérale de compréhension (MOU) liée à la SFN devrait être en place entre le régulateur des télécommunications et la banque centrale sur les remplacements de SIM. Un exemple de MOU est inclus à l'annexe B du rapport technique sur les vulnérabilités SS7 et les mesures de mitigation pour les transactions de services financiers numériques.

b) **Les opérateurs de réseaux mobiles devraient considérer adopter les contrôles suivants pour atténuer les risques de SIM et la fraude, comme décrit en 2.1 ci-dessous.**

2.1 Contrôles des opérateurs de réseau mobile pour atténuer les risques de SIM et la fraude:

a) Normalisation par les régulateurs des règles de remplacement de SIM parmi les MNOs / MVNOs par le régulateur, y compris les remplacements de SIM menant au transfert de numéros vers d'autres MNOs / MVNOs.

b) Lorsque le remplacement de SIM est effectué par une personne tierce, l'MNO / MVNO ou ses agents doivent capturer une image biométrique, faciale de la personne tierce qui doit être conservée pendant une période spécifiée.

c) Les MNOs doivent informer les fournisseurs de services financiers numériques sur les SIM remplacées, les numéros transférés et recyclés.

d) Vérification biométrique du remplacement de SIM: Les fournisseurs de services mobiles devraient adopter la vérification biométrique avant qu'un remplacement de SIM soit effectué.

e) Validation de l'utilisateur à plusieurs facteurs avant le remplacement de SIM: Les fournisseurs de services mobiles doivent utiliser une combinaison de ce qu'ils sont, de ce qu'ils ont ou de ce qu'ils connaissent pour authentifier les utilisateurs avant un remplacement de SIM. Les défis d'authentification de l'utilisateur doivent inclure la vérification des détails personnels (adresse, adresse e-mail, date de naissance), des informations sur le compte (date d'activation, dernier paiement, type de service), des informations sur l'appareil (IMEI, ICCID), des informations d'utilisation (numéros récents), de la connaissance (code PIN ou mot de passe, question de sécurité), de la possession (OTP par e-mail, OTP par SMS).

f) Partage d'informations avec le fournisseur SFN sur les échanges de SIM et le recyclage de SIM: L'opérateur mobile doit concevoir un processus de recyclage de numéros mobiles qui implique une communication avec les fournisseurs SFN sur les numéros d'identification de l'abonné mobile (MSIDN) qui ont été modifiés ou recyclés. (Dans ce contexte, le recyclage de numéro est lorsque l'opérateur mobile réattribue un numéro d'identification de l'abonné mobile (MSISDN) inactif/dormant à un nouveau client). Lorsqu'une SIM est recyclée, l'opérateur mobile signale le nouveau IMSI associé au numéro de téléphone du compte. Le fournisseur SFN doit bloquer le compte jusqu'à ce que l'identité de la nouvelle personne qui détient la carte SIM soit vérifiée en tant que titulaire du compte.

g) Notifications d'échange de SIM aux utilisateurs: Lors de la demande d'un échange de SIM, envoi de notifications via SMS, IVR ou Push USSD de la demande d'échange de SIM au propriétaire (actuel) du numéro/téléphone SIM, au cas où la SIM est encore active, puis en attendant une réponse positive du propriétaire pendant un certain temps avant de réaliser l'échange de SIM.

h) Protection sécurisée des données SIM: L'opérateur mobile doit protéger les informations personnelles pouvant être utilisées lors d'échanges de SIM et stocker en toute sécurité les données SIM telles que IMSI et les valeurs de clé secrète SIM (KI).

i) Temps de retenue avant activation d'une SIM échangée: Un temps général de retenue entre le moment de la demande de la carte SIM et la fourniture de la nouvelle carte SIM à la personne qui en fait la demande.

j) Formation des représentants du support client: Fournir une meilleure formation aux représentants du support client. Les représentants doivent parfaitement comprendre comment authentifier les clients et que les déviations des méthodes d'authentification ou la divulgation d'informations clients avant l'authentification sont impermissibles.

2.2 Contrôles des opérateurs SFN pour atténuer les risques et la fraude liés aux SIM

a) Détection en temps réel de l'IMSI / ICCID: les fournisseurs de services SFN et de paiement devraient être en mesure de détecter en temps réel chaque fois qu'une carte SIM associée à des services SFN est échangée ou remplacée. Une vérification supplémentaire avant d'autoriser toute transaction ou modification de compte avec la nouvelle SIM devrait être requise.

b) Détection en temps réel du changement d'appareil: l'authentification de l'appareil pour améliorer la sécurité de la fin de traitement en suivant les IMEI des appareils utilisés pour accéder aux services financiers. De cette façon, un compte qui change d'appareil peut être signalé par l'opérateur SFN.

c) Encourager l'utilisation d'un accès SFN sécurisé: offrir aux clients la possibilité de se désabonner des canaux USSD ou STK pour les transactions financières, en particulier ceux qui peuvent accéder au SFN en utilisant une application.

Les mesures recommandées ci-dessus pourraient également être adoptées en tant que réglementations par les régulateurs SFN.

Annexe 3 .

Modèle pour un protocole d'accord entre l'organisme de réglementation des télécommunications et la banque centrale sur la sécurité des SFN

1 Fondements du protocole d'accord

En reconnaissance de la convergence croissante des services de télécommunications et des services financiers au sein d'entités communes désignées par l'appellation "services financiers numériques" (SFN), les autorités ont identifié des besoins en matière d'interaction et de collaboration entre les différents organismes de réglementation, afin de garantir l'intégrité, la sécurité, la stabilité et la protection des parties prenantes et des utilisateurs finaux qui fournissent ou bénéficient de ces services.

la banque centrale et la banque centrale et l'organisme national de réglementation des télécommunications doivent coopérer pour assurer le contrôle et la surveillance des fournisseurs de SFN et des réseaux de communication des MNO – dans le respect de leurs mandats respectifs, tant sur le plan financier que sur le plan des télécommunications – de manière à garantir le plus haut degré d'exigence possible en matière de sécurité, de fiabilité, de protection des usagers, d'équité d'accès aux équipements et de confidentialité.

Par ailleurs, en reconnaissance du fait que la banque centrale et la banque centrale et l'organisme national de réglementation des télécommunications disposent chacun d'un champ limité en matière de contrôle et de surveillance des composantes des SFN, le présent protocole d'accord vise à établir des modalités communes de supervision et d'interaction sur les enjeux relatifs aux SFN inscrits dans les prérogatives et les mandats respectifs des deux autorités signataires, qui s'engagent ainsi à renforcer le cadre de réglementation, de contrôle et de surveillance des SFN en/au/aux/à [nom du pays] et à combler d'éventuelles lacunes.

Ce protocole d'accord est signé sur la base d'un respect mutuel, dans un esprit de bonne volonté et n'affecte en rien l'indépendance des deux autorités signataires.

Ce protocole d'accord vise à favoriser l'intégrité, l'efficience et l'efficacité des parties prenantes en optimisant la réglementation et en renforçant la supervision des SFN.

2 Domaines et stratégies de coopération dispositions générales

2.1 Les parties signataires acceptent de coopérer, en conformité avec leurs rôles respectifs, sur le traitement des enjeux suivants:

a) Les SFN en général;
b) L'accessibilité, l'équité d'accès, la sécurité et la fiabilité de l'ensemble des composantes des SFN en/au/aux/à [nom du pays];
c) La protection des usagers;
d) Tout autre domaine de collaboration possible entre les deux autorités signataires.

2.2 La coopération entre la banque centrale et la banque centrale et l'organisme national de réglementation des télécommunications se concentrera sur les enjeux et les processus suivants:

a) L'échange d'informations utiles;

b) Le renforcement mutuel des capacités;

c) L'ouverture d'une enquête en cas d'incident, de problème ou de situation relevant du champ d'application du présent protocole d'accord;

d) L'organisation d'auditions conjointes ou individuelles, selon les besoins;

e) L'utilisation de systèmes communs pour le suivi des transactions effectuées depuis les SFN;

f) L'action en faveur du respect de la concurrence et de l'égalité des chances pour toutes les parties prenantes de l'écosystème de SFN;

g) La résolution de conflits entre les fournisseurs et les utilisateurs finaux;

h) L'élaboration, le suivi et l'application, dans les lois, les réglementations et les directives, de dispositions relatives aux SFN;

i) Des consultations destinées à proposer, pour les différentes lois, réglementations et directives existantes, des amendements relatifs aux SFN;

j) Des consultations destinées à proposer de nouvelles lois, réglementations et directives relatives aux SFN;

k) Le recours à une expertise technique;

l) La gestion et l'exploitation de l'infrastructure de SFN;

m) La disponibilité des canaux de communication des opérateurs de réseau mobile (MNO) et l'équité d'accès pour tous les fournisseurs de SFN;

n) La disponibilité et l'équité d'accès pour les données des MNO juridiquement éligibles à une diffusion auprès des fournisseurs de SFN ou d'autres parties;

o) L'élaboration et l'application des normes techniques et opérationnelles minimales;

p) L'identification, l'atténuation, le traitement rapide et la maîtrise de l'ensemble des problèmes et incidents de sécurité;

q) Lorsque cela est nécessaire, la participation à l'élaboration des cadres de gestion des risques relatifs aux SFN;

r) Lutte contre le blanchiment d'argent, le financement du terrorisme et la fraude;

s) La protection générale des usagers;

t) La surveillance des systèmes et des réseaux à des fins de détection des violations de la sécurité et des intrusions susceptibles d'affecter les SFN, et leur signalement à l'autre autorité signataire;

u) Le soutien aux activités de l'autre autorité signataire relatives aux SFN et aux sujets connexes;

v) Le signalement rapide à l'autre autorité signataire de l'ensemble des problèmes, des processus et des événements susceptibles d'affecter le fonctionnement des SFN en/au/aux/à [nom du pays];

w) Toute autre stratégie entrant dans le champ d'application du présent protocole d'accord et jugée nécessaire et appropriée par les deux autorités signataire.

2.3 Fonctions assignées à l'autorité nationale des télécommunications

La banque centrale et l'organisme national de réglementation des télécommunications doit assurer la surveillance continue des fréquences agréées exploitées par les MNO, de façon à garantir qu'aucun appareil à radiofréquence non autorisé ne soit utilisé sur lesdites fréquences pour, entre autres, intercepter des informations sur les usagers ou perturber les communications entre les MNO et leurs abonnés.

Si nécessaire, cette surveillance peut être assurée conjointement par la banque centrale et l'organisme national de réglementation des télécommunications et les MNO. Toute intrusion ou violation susceptible d'affecter l'exploitation et la sécurité financière des SFN en/au [nom du pays] doit être signalée dans les meilleurs délais par la banque centrale et l'organisme national de réglementation des télécommunications à la banque centrale.

2.3.1 Dans le cadre de son mandat de surveillance et de supervision, la banque centrale et l'organisme national de réglementation des télécommunications agira pour garantir que les opérateurs détenteurs d'une licence offrent leurs services aux fournisseurs de SFN:

a) À un niveau technique élevé;

b) À un niveau de sécurité élevé;

c) À un niveau de disponibilité élevé pour garantir aux usagers des communications et/ou des transferts de données sans interruption;

d) De manière efficace et abordable;

e) De manière juste et équitable;

f) Sans abuser de la licence qui leur a été accordée pour l'exploitation des ressources de télécommunications et sans tirer avantage de la quantité limitée desdites ressources au détriment d'autres entités dont le fonctionnement en dépend;

g) De manière transparente;

h) Sans opérer de distinction entre les différents fournisseurs de SFN ni entre les autres entités dont le fonctionnement dépend de ces ressources, que ce soit en matière de coût, d'accessibilité ou de qualité de service;

i) Sans retarder l'acheminement et la transmission d'aucun message de service;

j) Dans le respect des droits de propriété intellectuelle;

k) Tout en garantissant la disponibilité de l'accès au réseau selon les normes en vigueur;

l) Sans nuire au principe de libre concurrence;

m) Lorsque les détenteurs de la licence sont des MNO, ils doivent s'assurer que seules les personnes authentifiées et autorisées sont en mesure d'accéder aux cartes SIM des usagers – ou, le cas échéant, d'en fournir;

n) Selon les besoins, s'assurer que les opérateurs mettent en œuvre une politique constante de test, de filtrage des intrus et de surveillance des réseaux centraux, de l'infrastructure des stations d'émission-réception de base et des bandes de fréquences de téléphonie mobile agréées afin d'empêcher d'éventuelles tentatives d'accès, de perturbation ou d'utilisation non autorisées.

2.3.2 La surveillance et les tests relatifs aux questions spécifiées dans la section 2.4 ci-dessus et qu'il sera nécessaire, le cas échéant, de mettre en œuvre portent notamment, mais pas exclusivement, sur les points suivants:

a) L'accès non autorisé et l'usage de toute composante centrale de l'infrastructure d'un MNO basée sur l'ensemble de protocoles SS7;

b) L'usage de toute composante SS7 de l'infrastructure d'un MNO à des fins d'activité non autorisée ou frauduleuse ;

c) L'accès non autorisé et l'usage de toute composante centrale de l'infrastructure d'un MNO basée sur la norme LTE;

d) Dans la mesure du possible et en fonction des capacités techniques, la détection des appareils à radiofréquence non autorisés exploités par des acteurs non autorisés et susceptibles d'être conçus pour perturber les activités des MNO détenteurs d'une licence et/ou pour accéder frauduleusement au téléphone fixe, à la carte SIM et aux données des usagers, ainsi qu'à leurs droits d'accès aux équipements de MNO et de SFN.

2.3.3 La banque centrale et l'organisme national de réglementation des télécommunications doit également s'assurer que les opérateurs détenteurs d'une licence et l'ensemble des entités qu'il supervise:

a) Transmettent à la banque centrale et l'organisme national de réglementation des télécommunications des rapports relatifs aux tests de pénétration liés à la sécurité de leurs systèmes. Le cas échéant, ces rapports doivent notamment mentionner les actions correctives entreprises;

b) Transmettent à la banque centrale et l'organisme national de réglementation des télécommunications des rapports relatifs aux incidents liés aux autorisations d'accès à leurs systèmes et à leurs données. Ces rapports doivent notamment mentionner les pertes de données et les violations des mesures de protection des données des usagers, qu'elles soient effectives ou potentielles, ainsi que les actions correctives entreprises;

c) Appliquent dans les meilleurs délais les normes internationales les plus récentes en matière de technique et de sécurité;

d) Offrent aux utilisateurs finaux des SFN le plein accès aux différents fournisseurs de SFN et la possibilité de choisir, sans aucune restriction, discrimination ni traitement de faveur.

2.4 Fonctions assignées à la banque centrale

2.4.1 La banque centrale doit assurer la surveillance constante des entités qu'elle supervise.

2.4.2 Dans le cadre de son mandat de surveillance et de supervision, la banque centrale agira pour garantir que les opérateurs détenteurs d'une licence et les entités qu'elle supervise:

a) Offrent leurs services aux fournisseurs de SFN:

i. À un niveau technique élevé;

ii. À un niveau de sécurité élevé;

iii. À un niveau de disponibilité élevé pour garantir aux usagers des communications et/ou des transferts de données sans interruption;

iv. De manière efficace et abordable;

v. De manière juste et équitable;

vi. Sans abuser de la licence ou de l'autorisation d'exploitation qui leur a été accordée au détriment d'autres entités dont le fonctionnement dépend des ressources concernées;

vii. De manière transparente;

viii. Sans opérer de distinction entre les différents fournisseurs de SFN, que ce soit en matière de coût, d'accessibilité ou de qualité de service;

ix. Sans retarder l'acheminement et la transmission d'aucun message de service;

x. Dans le respect des droits de propriété intellectuelle;

xi. Tout en garantissant la disponibilité de l'accès au service selon les normes en vigueur.

b) Ne nuisent pas au principe de libre concurrence;

c) Selon des besoins, mettent en œuvre une politique constante de test, de filtrage des intrus et de surveillance des infrastructures afin d'empêcher d'éventuelles tentatives d'accès, de perturbation ou d'utilisation non autorisées; et, dans les meilleurs délais:

i. Transmettent à la banque centrale des rapports relatifs aux tests de pénétration liés à la sécurité de leurs systèmes. le cas échéant, ces rapports doivent notamment mentionner les actions correctives entreprises;

ii. Transmettent à la banque centrale des rapports relatifs aux incidents liés aux autorisations d'accès à leurs systèmes et à leurs données. Ces rapports doivent notamment mentionner les pertes de données et les violations des mesures de protection des données des usagers, qu'elles soient effectives ou potentielles, ainsi que les actions correctives entreprises;

iii. Appliquent les normes internationales les plus récentes en matière de technique et de sécurité;

d) Offrent aux usagers des SFN la possibilité de choisir entre différents fournisseurs, sans aucune restriction, discrimination ni traitement de faveur.

Annexe 4 .

Mobile Application security best practices.

Le modèle pour la sécurité des applications propose les meilleures pratiques que les régulateurs des services financiers numériques qui pourraient être incluses dans un document de politique de sécurité des applications par les fournisseurs SFN. Le modèle prend strictement en compte l'application mobile sur l'appareil, sauf indication contraire, et les sous-sections décrivant les recommandations traitent de divers aspects de l'opération ou de la politique sous-jacente relative à l'application mobile. L'accent est principalement mis sur les applications Android compte tenu de leur part de marché importante, bien que de nombreuses recommandations soient applicables à tous les systèmes d'exploitation mobiles. Ce modèle est extrait de la section 9 de la Cadre de garantie de la sécurité des services financiers numériques.

1 Lignes directrices relatives aux bonnes pratiques en matière de sécurité des applications d'argent mobile

Nous présentons un modèle de cadre de sécurité pour les applications d'argent mobile, en nous concentrant sur de bonnes pratiques générales et non sur des technologies spécifiques, sauf lorsqu'elles sont explicitement mentionnées. Pour ce modèle, nous nous inspirons de travaux d'analyse récents sur les applications de SFN du point de vue des applications d'argent mobile. Ces travaux incluent l'étude de la Global System Mobile Association (GSMA) sur les bonnes pratiques en matière de sécurité des applications d'argent mobile[1], les lignes directrices de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) pour le développement sécurisé de smartphones[2], ainsi qu'un cadre de sécurité pour les applications de paiement mobiles élaboré par la Banque d'État du Pakistan[3]. Ce modèle peut également être utilisé par les fournisseurs de SFN pour étayer leur politique en matière de sécurité des applications.

Cette section vise à synthétiser les recommandations afin de fournir aux organismes de réglementation ou aux examinateurs de la sécurité applicative un point de départ pour leurs évaluations de la sécurité. Le modèle porte strictement sur l'application mobile installée sur l'appareil, sauf indication contraire, et les sous-sections décrivant les recommandations traitent de divers aspects de l'exploitation ou de la politique sous-jacente relative à l'application mobile. L'accent est principalement mis sur les applications Android étant donné leur part de marché importante, bien que de nombreuses recommandations s'appliquent à l'ensemble des systèmes d'exploitation mobiles. Bien que la confidentialité constitue également un facteur important, ces recommandations concernent avant tout la sécurité.

1.1 Intégrité des appareils et des applications

i. Les appareils les plus sûrs pour effectuer des transactions financières sont ceux qui n'ont jamais subi de débridage ou de rooting, car il peut être difficile, voire impossible, d'évaluer la sécurité du système d'exploitation sous-jacent s'il a été remplacé ou exploité. Les applications doivent donc utiliser les services de la plate-forme mobile pour déterminer que la plate-forme sous-jacente et elles-mêmes n'ont pas été modifiées.

[1] GSMA, "Official Document MM.01 – MM App Security Best Practices, Version 1.0", 29 juin 2018.
[2] ENISA, "Smartphone Secure Development Guidelines", 10 février 2017.
[3] Banque d'État du Pakistan, *Mobile Payment Applications (App) Security Framework* (PROJET DE DOCUMENT, version 1.0), avril 2019.

ii. Il convient de supprimer tout code superflu éventuellement ajouté à l'application pendant le développement, comme les fonctionnalités qui ne sont pas conçues pour les plates-formes d'appareils sur lesquelles l'application sera déployée ou les fonctionnalités de développement/débogage, afin de réduire la surface d'attaque du code de production déployé.
iii. Côté serveur, il convient de déterminer si l'application s'exécute dans un état d'intégrité élevée grâce à la validation de signature, au hachage sur l'application ou à certains blocs de fonction du programme.

1.2 Sécurité des communications et gestion des certificats

i. Les applications doivent utiliser des bibliothèques cryptographiques normalisées. Pour la communication avec les services internes, elles doivent également appliquer un chiffrement de bout en bout en bout en utilisant des protocoles normalisés, en particulier TLS. La version minimale recommandée du protocole TLS est la version 1.2.
ii. Les certificats TLS ne doivent pas être expirés et doivent présenter des suites de chiffrement robustes, notamment le chiffrement AES-128 et SHA-256 pour le hachage. Nous recommandons l'utilisation de modes d'opération de chiffrement authentifiés tels que le Galois/Counter Mode (GCM).
iii. Il faut limiter la durée de vie des certificats émis à 825 jours, conformément aux bonnes pratiques préconisées par le Certification Authority Browser Forum.
iv. Il convient de vérifier la fiabilité de l'autorité de certification et de prévoir un plan d'urgence si celle-ci n'est plus fiable.
v. La configuration de TLS doit être effectuée de manière sécurisée et des mesures doivent être prises pour éviter les problèmes de configuration qui pourraient entraîner l'échec de l'authentification ou une mauvaise sélection de l'algorithme.
vi. L'épinglage des certificats est recommandé pour empêcher leur remplacement.
vii. Il convient de s'assurer que les certificats de serveur sont validés correctement au niveau des appareils côté client.

1.3 Authentification des utilisateurs

i. Les codes PIN et les mots de passe doivent être difficiles à deviner; il convient également d'interdire les identifiants faibles. Cependant, il ne faut pas forcer les utilisateurs à changer régulièrement de mot de passe.
ii. Nous recommandons fortement l'utilisation de l'authentification à facteurs multiples avant toute action financière ou sensible.
iii. Pour envoyer des mots de passe à usage unique, il faut privilégier les applications d'authentification pour smartphone, car le canal SMS est vulnérable au piratage du protocole SS7 et à d'autres menaces en matière de sécurité.
iv. Si des informations biométriques sont utilisées pour l'authentification, des mesures de sécurité adéquates doivent être prévues pour leur stockage, par exemple en les chiffrant dans le magasin de clés Android ou en utilisant du matériel de confiance.

1.4 Traitement sécurisé des données

i. Les appareils mobiles doivent stocker les informations confidentielles en toute sécurité, par exemple à l'aide du cadre Android KeyStore.
ii. Il convient, si possible, d'utiliser du matériel de confiance pour stocker les informations sensibles sur les smartphones des clients.
iii. Il faut éviter de stocker des informations dans un dispositif de stockage externe. Le cas échéant, il faut s'assurer d'effectuer une validation forte des données entrantes avant de les utiliser.

iv. Il convient de supprimer les données confidentielles des caches et de la mémoire après leur utilisation et évitez d'exposer les informations de manière générale. La mémoire doit être nettoyée avant de quitter l'application.
v. Il convient de limiter la quantité de données partagée avec d'autres applications en utilisant des autorisations granulaires. Il faut également limiter autant que possible le nombre d'autorisations demandées par l'application et s'assurer que lesdites autorisations correspondent aux fonctionnalités nécessaires au bon fonctionnement de l'application.
vi. Les informations sensibles (mots de passe ou clés de passe, par exemple) ne doivent pas être codées en dur dans le code source de l'application.
vii. Toute entrée provenant du client qui doit être stockée dans les bases de données doit être validée pour éviter les attaques par injection SQL.

1.5 Développement d'applications sécurisé

i. Les applications doivent être développées selon les pratiques et les normes de programmation sécurisée reconnues par le secteur.
ii. Il convient de s'assurer d'être en mesure de mettre à jour les applications en toute sécurité et de veiller à ce que toutes les bibliothèques et tous les modules dépendants soient sécurisés. Les mises à jour pour ces éléments doivent être mises à disposition dès que nécessaire.
iii. Le code doit être testé et évalué de manière indépendante par des équipes de réviseurs internes ou externes.