ARTCI
AUTORITE DE REGULATION DES TELECOMMUNICATIONS/TIC DE COTE D'IVOIRE

SECURITE DES RÉSEAUX TELECOMS

TANOH BEUGRE Jacques

Chef de Département Audit SI et Sécurité des Réseaux

Définition de résilience et sécurité des réseaux

Résilience des réseaux de télécommunications

La réglementation ivoirienne, n'a pas encore prévu de définition de « résilience des réseaux de télécommunications ».

la notion de « continuité de service » qui est la capacité d'un organisme à poursuivre la fourniture des produits ou la prestation de services à des niveaux acceptables et préalablement définis après un incident perturbateur

Sécurité des réseaux de télécommunications

Processus consistant en la mise en œuvre de mesures organisationnelles et techniques visant à assurer qu'un système d'information est capable de résister à des évènements volontaires ou non, susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées ou transmises

La cybersécurité est l'ensemble des mesures et des actions destinées à protéger le cyberespace des menaces associées à ses réseaux et à son infrastructure informatique ou susceptibles de leur atteinte.

La cybersécurité vise à préserver la disponibilité et l'intégrité des réseaux et de l'infrastructure ainsi que la confidentialité des informations qui y sont contenues ; CID-T (confidentialité, intégrité, disponibilité – Traçabilité)

la définition de la « sécurité des réseaux de télécommunication » diffère de celle de « la cybersécurité », mais elle constitue un élément majeur de la cybersécurité

Cadre réglementaire d'amélioration de la résilience des réseaux

1. Plan National de Télécommunications en cas d'urgence et de catastrophes naturelles (PNTUC)

- Permanence et disponibilité/accessibilité du service ;
- Plan de continuité de services relatif aux incidents graves qui pourraient survenir sur leur réseau, conforme au référentiel établit par l'ARTCI

2. L'adoption de textes législatifs et règlementaires spécifiques aux télécommunications d'urgence

---

Cas de l'incendie d'un centre technique

- Conséquences: impacts importants sur les services de télécommunications,
- Mesures prises: l'ARTCI a lancé une campagne d'audit des plans de continuité de services de l'ensemble des opérateurs télécoms.

Obligations des opérateurs et actions du régulateur

1. Obligations des opérateurs

01 Mettre en place un Plan de Continuité de Service (PCS);

02 Élaborer un Plan annuel de sécurisation de leurs réseaux

03 Fournir un rapport annuel d'activité faisant le bilan des actions réalisées en matière de cybersécurité

04 Se conformer aux exigences du Référentiel général de Sécurité des Systèmes d'Information (RGSSI) et du Plan de Protection des Infrastructures Critiques (PPIC)

05 Réaliser une analyse des risques de sécurité tous les six (6) mois

06 Se soumettre à l'audit réglementaire périodique de sécurité de leurs réseaux et systèmes d'informations

2. Actions du régulateur

- L'audit du Plan de Continuité de Service (PCS) des opérateurs télécoms ;
- La vérification du respect par l'opérateur de ses obligations en matière de sécurité;
- La mise en demeure et la prise de sanction envers les opérateurs en cas de non-respect des exigences de sécurité.

Principaux enjeux de sécurité liés aux évolutions techniques et aux architectures réseaux

En raison de la croissance soutenue des réseaux,

- ✓ La protection des infrastructures critiques ;
- ✓ La protection des données personnelles, plus particulièrement liés aux technologies Cloud et Big Data ;
- ✓ La protection des objets connectés (IoT) dans la mise en œuvre des « smart cities ».

Méthodologie

1. Décrets sur l'audit de sécurité et la certification des systèmes d'information, et la protection des infrastructures critiques
2. Conduite des missions d'audit de sécurité chez les opérateurs, par des prestataires agréés
3. Homologation des équipements réseaux et de sécurité
4. Autorisations d'importation d'équipement qui fournit des services de cryptologie
5. Élaboration tous les 03 ans des analyses, des évaluations des menaces et des risques de sécurité sur le cyberespace ivoirien.

Prérogatives du régulateur en matière de cybersécurité

01 GOUVERNANCE

02 JURIDIQUE

03 TECHNIQUE

L'ARTCI joue le rôle de coordinateur principal du plan de protection des infrastructures critiques, en étroite collaboration avec les instances compétentes, notamment les comités stratégiques sur la cybersécurité, groupes de travail. Le rôle consiste essentiellement à définir en collaboration avec l'ensemble des acteurs impliqués, les lignes directrices et les principes de gestion du plan de protection des infrastructures critiques.

Côte d'Ivoire Computer Emergency Response Team en abrégé CI CERT est l'équipe de réponse aux incidents et de protection du cyberespace national qui a été mise en place en 2009 par l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire.

- Décret N°2020-128 du 29 Janvier 2020, portant création, organisation et fonctionnement du centre de veille et de réponses aux incidents de sécurité informatique dénommé Côte d'Ivoire Computer Emergency Réponse Team.

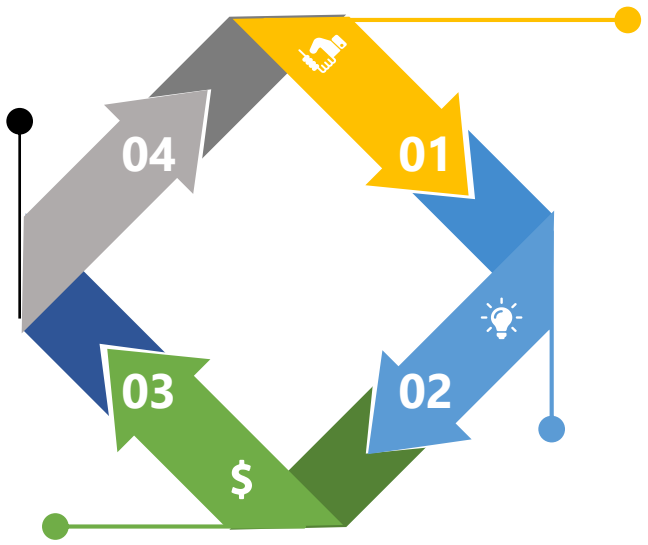
Mesures pour réduire les risques de cyberattaques

Adoption par décret 2021-916 du 22 Décembre 2021 du « Plan de Protection des Infrastructures Critiques

Précise que L'ARTCI identifie des infrastructures d'information critiques, fixe des priorités de protection et désigne les opérateurs ou gestionnaires d'infrastructures d'information critiques

Adoption par décret 2021-916 du 22 Décembre 2021 du Référentiel général de Sécurité des Systèmes d'Information (RGSSI)

Décret fixant les règles et exigences auxquelles les organismes et entreprises visés à l'article 3 doivent se conformer.



Adoption par décret 2021-915 du 22 Décembre 2021 de la politique de sécurité des systèmes d'information de l'administration publique.

Les organismes publics sont tenus de se conformer à la politique de sécurité des systèmes d'information de l'administration publique

Décret 2021-917 du 22 Décembre 2021 portant procédure d'audit contrôle et de certification des systèmes d'information

les systèmes d'information des administrations, des organismes et entreprises relevant du secteur public et privée établies en Côte d'Ivoire sont soumis à l'audit de sécurité périodique obligatoire.

Audit des opérateurs sur la résilience et sécurité des réseaux

1. Conduire des audits auprès des opérateurs sur la résilience des infrastructures et/ou la sécurité, conformément à la règlementation en vigueur;

1. Réaliser plusieurs audits de sécurité des systèmes d'information des organisations d'États. Cependant, nous n'avons pas entamé des audits auprès des opérateurs sur la sécurité de leurs infrastructures. Ceux-ci seront conduits par des prestataires d'audits de sécurité agréés par l'ARTCI.

2. Conduire les audits des plans de continuité de services des opérateurs tous les 02 ans pour s'assurer de leur résilience.

MERCI DE VOTRE ATTENTION