SYMPOSIUM SUR UNE APPROCHE INTEGREE DE LA CYBERSECURITE
28 – 30 SEPTEMBRE 2021
NOOM HOTEL ABIDJAN
COUNTRY UPDATE: CÔTE D'IVOIRE

NB : *Chaque équipe nationale disposera de 5 minutes pour faire le point sur la cybersécurité dans son pays.*

- *Pour chaque élément de la liste ci-dessus, l'équipe nationale doit indiquer la situation actuelle (pleinement opérationnel, en cours ou inexistant) et la vision pour l'année 2022*

I. Stratégies nationales de cybersécurité (SNCS)

- **EN COURS**
  - Restitution de la stratégie nationale de cybersécurité
- **VISION 2022**
  - Diffuser et mettre en œuvre la stratégie nationale de cybersécurité

II. Équipes d'intervention en cas d'incident de sécurité informatique

La vision : Renforcer le rayonnement du CI-CERT et améliorer le niveau de sécurité des systèmes d'information des infrastructures critiques nationales ;

- **PLEINEMENT OPÉRATIONNEL**

- **CSIRT national** :
  - Un décret a été adopté en 2020, définissant officiellement le CI-CERT comme CSIRT national avec des missions, l'autorité et le champ d'action
  - Staff technique opérationnel pour les services de base
  - Trois catégories de services de base (pro-actifs, réactifs et management de la qualité de la sécurité) sont offertes aux parties prenantes par le CI-CERT
  - Le CI-CERT est membre plein du FIRST, OIC-CERT, AfricaCERT, Groupe de travail régional des CSIRT nationaux Africains

- **EN COURS**

- ***Formalisation et implémentation des procédures et du cadre organisationnel du CI-CERT***
  - Développer, mettre à jour et formaliser les procédures et processus par la Direction du CI-CERT ;
  - Mise en œuvre du cadre d'évaluation de la maturité du CI-CERT, conformément aux dispositions du model SIM3 (Security Incident Management Maturity Model)
- ***Développement et mise en œuvre d'un plan national de réponse aux cyber crises majeurs ;***
- ***Formalisation du réseau national de points de contacts cybersécurité du secteur public***

- **INEXISTANT**

- ***Centre des Opérations de sécurité (SOC) national***
  - Création et mise en services du SOC national
  - Monitoring des infrastructures critiques nationales
- ***CSIRT Sectoriels.***

III. Protection des infrastructures critiques (PIC)

- **EN COURS**
  - Diffusion de la politique de protection des infrastructures critiques
- **VISION 2022**
  - Mettre en œuvre de la politique de protection des infrastructures critiques

IV. Législation et cadres juridiques relatifs à la cybersécurité

- **PLEINEMENT OPÉRATIONNEL**

  - Loi N°2013-451 du 19 Juin 2013 relative à la lutte contre la cybercriminalité
  - Loi N°2013-450 du 19 Juin 2013 relative à la protection des données à caractère personnel

V. Sensibilisation à la cybersécurité, compétences et développement des ressources Humaines

La vision : Développer la confiance numérique, renforcer la lutte contre la cybercriminalité, la protection de la vie privée des usagers et des données personnelles et les capacités en matière de cybersécurité par la sensibilisation et la formation.

- **PLEINEMENT OPÉRATIONNEL**

- **Sites web et médias sociaux dédiés à la sensibilisation**
  - Diffusion par le CI-CERT de contenus informatif lié à sensibilisation à la sécurité numérique à destination du grand public et des professionnels de la cybersécurité
  - Site web national de sensibilisation dédié à la protection des enfants en ligne
- **Cyberdrill**
  - Participation aux Cyberdrill régionaux et internationaux (FIRST, AfricaCERT, UIT)
  - Organisation de Cyberdrill nationaux, destinés aux acteurs locaux
- **Formation universitaire et supérieures en matière de cybersécurité**
  - L'Ecole Supérieure Africaine des Technologies de l'Information et de la Communication (ESATIC) est un établissement Public d'enseignement supérieur qui propose des curricula de formation en cybersécurité dans le secteur des TIC.
  - L'Institut Polytechnique Houphouët Boigny (Centre INP-HB / Cnam) propose un certificat de compétence Analyste en Cybersécurité.

- **EN COURS**

- **Finalisation d'un programme de sensibilisation et formation à la sécurité numérique**
  - Développement des outils didactiques et mise en place du programme DIGISEC (Digital Security Classroom) par le CI-CERT
  - Implementation du NCSAM (National Cybersecurity Awareness Month)

- **INEXISTANT**

- Modules de formation à la cybersécurité dans les cursus des écoles nationales (ENA, INFJ, Ecoles Nationales Police, Gendarmerie, Douanes, etc.) et écoles de formation des fonctionnaires et agents d'état.
- Cursus de formation universitaires en cybersécurité
- Centre de recherche en cybersécurité
- Forum national sur la cybersécurité