PROTECTION DES SYSTEMES INFORMATIQUES ET DE COMMUNICATION CRITIQUES EN AVIATION CIVILE

Mr. Safiou SOULE

Directeur Inspection et Qualité à l'ANAC
Inspecteur et Instructeur AVSEC

SOMMAIRE

INTRODUCTION

Depuis 2019, le Togo s'est lancé dans le processus de digitalisation des services publics et privés, ainsi la sécurisation desdits services contre les cyberattaques devient impérative ; cette sécurisation tient compte des changements majeurs notamment :

- **l'inauguration de la nouvelle aérogare (2016)** : sécurisation les systèmes aéroportuaires / protection les données passagers;
- **les cybermenaces (2018)** : protection des infrastructures critiques contre les ransomwares et piratages;
- **la protection des données (2019)** : Assurer la confidentialité des données personnelles;
- **Impact COVID-19 (2020)** : Accélération de la digitalisation nécessitant un renforcement de la cybersécurité pour la continuité des services.

- **l'économie numérique (2020) :** Renforcement des infrastructures numériques pour attirer les investisseurs.
- **la confiance numérique (2020) :** Sécurisation des transactions électroniques pour la confiance des utilisateurs.
- **les standards internationaux et OACI :** Alignement avec les normes de la CEDEAO, de l'Union africaine, et les exigences de l'OACI pour assurer la cybersécurité dans le secteur de l'aviation et des infrastructures critiques.

CADRE LEGAL ET REGLEMENTAIRE DE LA CYBERSECURITE AU TOGO

- **Loi n°2018-026** du 07 décembre 2018 sur la cybersécurité et la lutte contre la cybercriminalité : Crée un cadre légal pour la protection des systèmes d'information et la répression des actes cybercriminels.

- **Loi n°2019-014** du 29 octobre 2019 sur la protection des données à caractère personnel : Assure la protection des informations personnelles en conformité avec les standards internationaux.

- **Décret N°2019-022/PR du 13 février 2019** portant attributions, organisation et fonctionnement de l'agence nationale de la cybersécurité (ANCy)

- **Arrêté n°2022-040/PMRT** du 29 juin 2022 : Fixe les règles de cybersécurité applicables aux opérateurs de services essentiels (OSE) pour protéger les infrastructures critiques.

L'AGENCE NATIONALE DE LA CYBERSECURITE (ANCy)

- **Création et mandat** : L'ANCy a été créée pour superviser et coordonner les efforts de cybersécurité au Togo, en protégeant les systèmes d'information contre les cybermenaces.

- **Missions principales** :
  - Développer la stratégie nationale de cybersécurité;
  - Mettre en place de politiques de cybersécurité pour les OSE;
  - Coordonner avec les acteurs internationaux;
  - Contrôler la conformité par la réalisation des audits annuel des infrastructures essentielles, mené avec **Cyber Defense Africa**.

ADOPTION DES REGLES DE CYBERSECURITE

L'ARRÊTÉ N°2022-040/PMRT DU 29 JUIN 2022

- **Objectifs de l'arrêté** : Garantir un niveau de sécurité minimal pour les systèmes d'information des OSE afin de protéger les infrastructures critiques du pays;
- **Champ d'application** : Tous les opérateurs de services essentiels, y compris les secteurs de l'énergie, des télécommunications, du transport aérien, et des services financiers;
- **Obligations légales des OSE** : Mise en place d'un Plan de Sécurité d'Opérateur (PSO) et réalisation d'audits réguliers.

L'Arrêté n°2022-040 PMRT

L'arrêté impose aux Opérateurs de Services Essentiels (OSE) plusieurs mesures de cybersécurité :

➢ Contrôle techniques de sécurité :

1. **Contrôle d'accès** : Authentification forte (multi-facteur) pour protéger les systèmes critiques;
2. **Gestion des actifs** : Inventaire et surveillance des actifs matériels et logiciels;
3. **Sécurité des communications** : Chiffrement des données pour protéger les communications;
4. **Sécurité opérationnelle** : Surveillance continue et mises à jour pour corriger les vulnérabilités;
5. **Gestion des incidents** : Réponse rapide aux cyberattaques avec des équipes CERT;
6. **Continuité des activités** : Plans pour la reprise après une cyberattaque ou incident majeur.

➢ Contrôle physique de sécurité :

1. **Sécurisation des centres de données** : Accès contrôlé par badges, vidéosurveillance et biométrie.;
2. **Contrôle d'accès physique** : Protection stricte des infrastructures sensibles (énergie, télécoms, transports);
3. **Protection contre les risques environnementaux** : Solutions contre les catastrophes naturelles (incendies, inondations) et utilisation de générateurs de secours.

ROLES ET RESPONSABILITES DES OPERATEURS DE SERVICES ESSENTIELS(OSE)

1. Elaborer et mettre à jour un Plan de Sécurité d'Opérateur (PSO);
2. Réaliser des audits de sécurité annuels avec Cyber Defense Africa;
3. Adapter continuellement les mesures de sécurité face aux nouvelles menaces;
4. Mener des analyses de risques et élaborer des plans d'atténuation;
5. Notifier les incidents à l'ANCy;
6. Vérifier les antécédents des employés critiques;
7. Former et sensibiliser le personnel à la cybersécurité au moins une fois par an;
8. Sécuriser les interactions avec les tiers et sous-traitants.

OPERATEURS DE SERVICES ESSENTIELS(OSE) DE L'AIGE

SALT : GESTIONNAIRE D'AEROPORT

AUDIT DE SECURITE DE L'INFRASTRUCTURE DE LA SOCIETE AEROPORTUAIRE DE LOME TOKOIN (SALT)

Date de l'audit : 25 octobre 2023

Organisme : Cyber Defense Africa (CDA)

Objectif : Evaluer la sécurité du système informatique de l'administration de la SALT, notamment en matière de protection des données, de résilience face aux cyberattaques, et de conformité aux normes internationales de cybersécurité.

Portée : Analyse des systèmes de gestion des données, des contrôles d'accès, de la sécurité des réseaux, et de la conformité réglementaire.

RESPONSABILITES DE L' ANAC

- Elaborer et mettre en œuvre des mesures de protection pour les systèmes critiques.
- Encourager les acteurs à identifier les vulnérabilités et les menaces.
- Promouvoir une culture de cybersécurité dans l'aviation civile.

EXIGENCES DU PNSAC

1. Identifier les infrastructures critiques
2. Elaborer et mettre à jour des mesures visant à identifier les infrastructures critiques
3. Evaluer les risques cybermenaces et élaborer des plans d'atténuation.
4. Vérifier les antécédents des employés critiques.
5. Notifier les incidents et évènements de sûreté.

ACTIONS MENEES PAR ANAC

1. **ELEMENTS D'ORIENTATION : PROTECTION DES SYSTÈMES INFORMATIQUES CRITIQUES;**
2. **METHODOLOGIE DE GESTION DE RISQUES AVSEC ;**
3. **OUTIL POUR L' EVALUATION DE RISQUES CYBERMENACES POUR LES EQUIPEMENTS CRITIQUES;**
4. **EXERCICE DE TABLE .**

ELEMENTS D'ORIENTATION :

protection des systèmes informatiques critiques

Objectifs du guide:

- Etablir des critères pour la protection des systèmes et des données informatiques critiques;
- Renforcer la résilience des systèmes aéronautiques face aux cybermenaces;
- Garantir la confidentialité, l'intégrité et la disponibilité des systèmes de l'aviation.

Usagers de l'aeroport concernés:

- Systèmes critiques pour la sécurité aérienne (gestion du trafic aérien, systèmes de communication) : **ASECNA**
- Systèmes critiques pour la sûreté (contrôle d'accès, systèmes de surveillance) : **ASAIGE**
- Systèmes critiques pour la facilitation (réservation, enregistrement des passagers) : **SALT**.

METHODOLOGIE DE GESTION DE RISQUES

Objectifs du guide

- Evaluation des risques (Menace, Vulnerabilités et consequences);
- Conception des scenarios de menaces AVSEC (cybersecurite, drones, ManPADs);
- Outils pour la conception de la cartographie de risques (excel).

Usagers de l'aeroport concernés

- Comite Local de Gestion de Risques (CLGR) : Evaluation de risques cyber;
- Senario de menace et evaluation de risques systeme de titres d'acces: ASAIGE.

APPROCHE D'ELABORATION DE LA CARTOGRAPHIE DE RISQUES

- **Etapes clés** :

1. Identification des systèmes critiques et des menaces.
2. Evaluation de la probabilité et de l'impact de chaque scenario de menace.
3. Carthographie de Risques
4. Elaboration de stratégies pour réduire ou éliminer les risques.
5. Mise en place de mesures correctives.

SCENARIOS DE MENACES

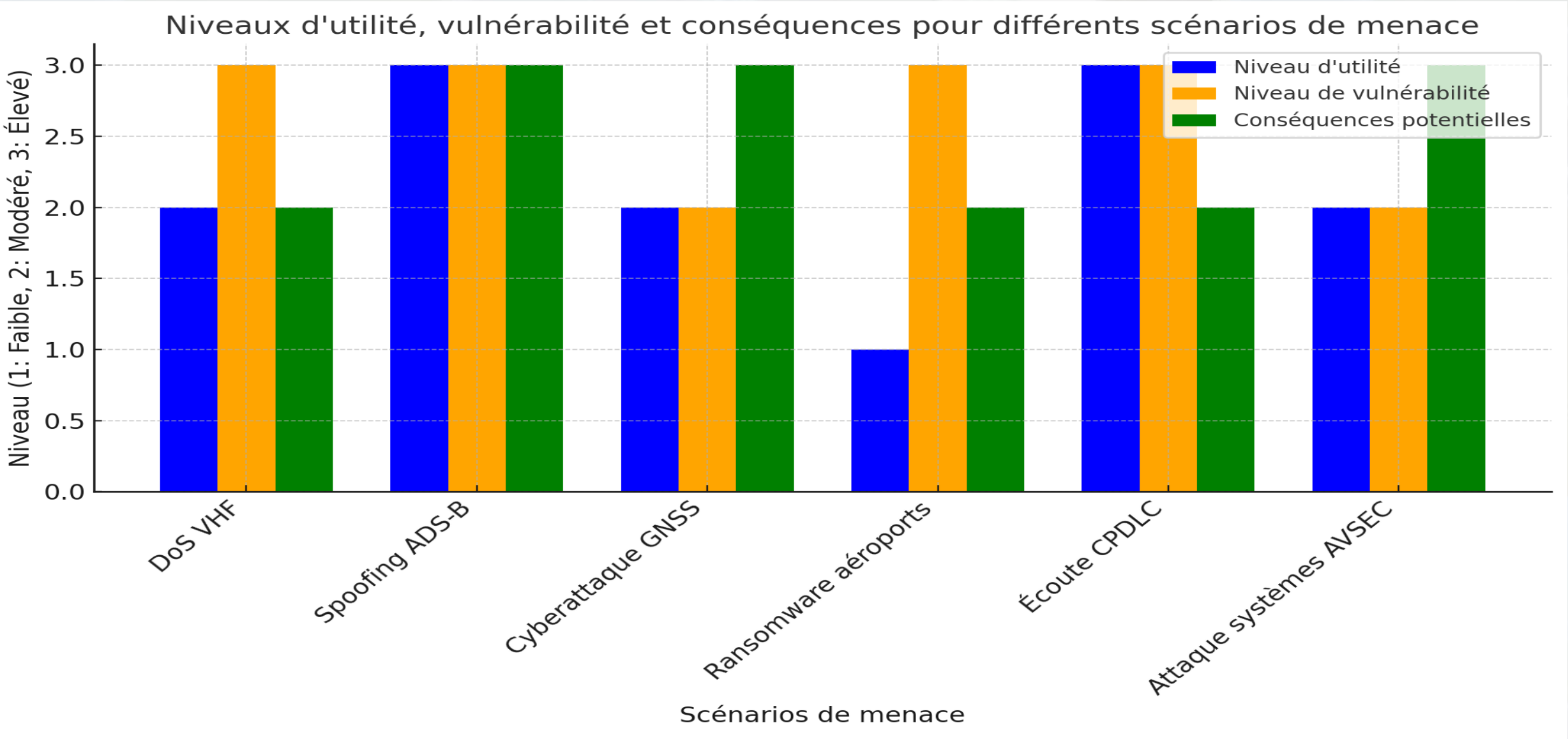
anticiper les risques, évaluer les vulnérabilités et renforcer la cyber-résilience des systèmes critiques dans l'aviation

1. **Denial of Service (DoS)** : Perturber les communications VHF, bloquant les échanges critiques entre pilotes et contrôleurs.
2. **Spoofing ADS-B** : Créer des faux avions ou modifier les trajectoires avec de fausses informations de localisation.
3. **Cyberattaques sur les systèmes GNSS (GPS)** : Brouiller les signaux GPS, compromettant la navigation aérienne.
4. **Ransomware sur les systèmes de gestion aéroportuaires** : Verrouiller les systèmes, causant des retards et des interruptions d'opérations.
5. **Écoute clandestine (eavesdropping)** : Intercepter des communications sensibles entre les contrôleurs et les pilotes.

IDENTIFICATION DES CIBLES CONCERNEES ET LES METHODES D'ATTAQUES

- **Systèmes de communication VHF** : Perturbation des communications entre pilotes et contrôleurs;
- **Système de surveillance ADS-B** : Injection de fausses données de vol, créant des avions fantômes;
- **Systèmes GNSS (GPS)** : Brouillage ou usurpation des signaux de navigation.
- **Systèmes d'information SWIM** : Perturbation des échanges de données critiques entre les acteurs de la navigation aérienne;
- **Systèmes de gestion des aéroports** : Verrouillage des systèmes par ransomware, paralysant les opérations;
- **Systèmes de communication CPDLC** : Interception des communications entre pilotes et contrôleurs aériens;
- **Systèmes de gestion de la sécurité AVSEC** : Désactivation des systèmes de surveillance et de détection.

ANALYSE DES COMPOSANTES



SOLUTIONS POUR LA CYBERSECURITE AERIENNE

- **Mesures de protection** :
  - **Cryptographie** : Sécurisation des communications par le chiffrement.
  - **Contrôles d'accès** : Limitation de l'accès aux systèmes critiques.
  - **Redondance** : Utilisation de systèmes de secours en cas de panne ou d’attaque.
  - **Surveillance proactive** : Systèmes de détection des intrusions pour identifier rapidement les anomalies.

DEFIS

1. Formation et sensibilisation des acteurs
2. Compétences pour évaluer l'efficacité des mesures et leur mise en œuvre
3. Activités de supervision : inspections / audits
4. Tests de pénétration des systèmes
5. Coopération : Internationale / Nationale, Universitaire / Aéroportuaire
6. Budget de fonctionnement : Prévision d'un budget annuel pour couvrir les coûts liés aux activités de formation, de supervision, de tests de sécurité et de coopération.

CONCLUSION

- La cybersécurité est un enjeu crucial pour la sûreté et la sécurité des vols.
- L’identification des risques, l’application de mesures de protection, et la réactivité en cas d’incident sont essentiels.
- La collaboration entre les acteurs de l'aviation est nécessaire pour une défense robuste.

JE VOUS REMERCIE POUR VOTRE ATTENTION