.

ORGANISATION DE L'AVIATION CIVILE INTERNATIONALE

Vingt-quatrième réunion du Groupe régional Afrique – Océan indien de planification et de mise en œuvre (APIRG/24)

(Réunion virtuelle, 2 au 4 novembre 2021)

Point 4 de l'ordre du jour : Autres initiatives de navigation aérienne

Cybersécurité dans l'ATM

(Présenté par l'ASECNA)

SUMMARY	
Dans sa conclusion 23/25 sur la cybersécurité et la résilience des systèmes de navigation aérienne, afin d'accroître les capacités des États et des organisations en matière de cybersécurité, il a été convenu que l'OACI, avec la collaboration de l'industrie dans le cadre du mécanisme APIRG, augmente son soutien aux activités visant à sensibiliser à la cybersécurité et à la résilience des NSA par le biais de webinaires / ateliers / séminaires sur la cybersécurité et la résilience des systèmes ANS pour la région AFI. Ce document met en évidence la vision de l'ASECNA, face au défi organisationnel et opérationnel de la cyber-résilience ANS dans son domaine de responsabilité. Il met également en évidence les défis rencontrés en mettant l'accent sur toutes les données utilisées / stockées / échangées, pas seulement l'infrastructure (protection des données). Les mesures à prendre par la réunion sont indiquées au paragraphe 3	
Objectifs stratégiques	A B

1 INTRODUCTION

Le système mondial de l'aviation est l'un des systèmes les plus complexes et les plus intégrés des technologies de l'information et de la communication (TIC) au monde. Par conséquent, le système ATM est une cible potentielle pour une cyberattaque à grande échelle. En fait, les systèmes ATM, en tant que partie importante de l'infrastructure de transport, sont une cible attrayante pour les cyberattaques en raison de leur importance et de leur importance. Les réseaux et systèmes, interconnectant les différents ANSP sont basés sur IP et sont exposés à plusieurs niveaux aux cyberattaques. Les cybermenaces sont réelles et peuvent prendre plusieurs formes selon les moyens des hackers. Par conséquent, les organisations doivent identifier leurs systèmes d'information critiques et mettre en œuvre des mesures de cybersécurité appropriées, au niveau opérationnel.

2 DISCUSSION

2.1 L'interconnectivité croissante de la gestion du trafic aérien (ATM) signifie que l'impact d'une cyberattaque peut s'étendre à un nombre croissant de systèmes interconnectés. Compte tenu du très haut niveau d'interconnexion des systèmes CNS / ATM, dans le même écosystème opérationnel de collecte, de transmission et de traitement des données en interne, que par le biais de liens bilatéraux, il existe un réel besoin d'une cyber-stratégie harmonisée dans la région AFI.

2.2 Le fait d'avoir des connexions bilatérales sous protocole TCP/IP est désormais une nécessité, afin de pouvoir établir par exemple, des connexions AMHS, de partager des données de surveillance, ou de déployer SWIM dans quelques années. Dans ce contexte, les enjeux de cybersécurité deviennent de plus en plus des enjeux collectifs, car il s'agit d'une **responsabilité partagée**, d'où la nécessité d'accords bilatéraux de coopération entre les Etats et les fournisseurs de service, afin d'évaluer concrètement toutes les questions de cybersécurité telles que les procédures communes d'identification des menaces, la formation, l'évaluation des performances des systèmes, l'évaluation des risques, les analyses de sécurité informatique, les audits et le contrôle, les exercices de tests d'intrusion, etc.

2.3 Il n'est plus indiqué aujourd'hui de ne se contenter que de séminaires et d'ateliers, certes forts utiles, le moment est venu de prendre des dispositions concrètes et pratiques.

2.4 En termes de ressources humaines, il ne faut plus hésiter à ouvrir le champ des profils et des compétences nécessaires pour renforcer l'ATSEP, dans ce domaine extrêmement sensible et spécialisé, l'idée étant de construire un réseau mixte d'experts capables de faire face aux cyber challenges de l'ATM.

2.5 En outre, afin d'atténuer les risques de cybersécurité, liés au partage d'informations au-delà de sa « sphère de diffusion » prévue, les documents d'orientation sur l'utilisation du Protocole sur les feux de signalisation (TLP), publiés en septembre 2021 sous l'autorité du Secrétaire général de l'OACI, ont été adoptés et des mesures ont été prises pour inclure l'utilisation du TLP dans sa politique de communication et la rendre applicable dans l'ASECNA à partir du début de l'année prochaine.

3 SUITE A DONNER PAR LA REUNION

3.1 La réunion est invitée à :

1. Prendre note des informations contenues dans la note de travail
2. Formuler des recommandations pertinentes viser à créer les meilleures conditions possibles pour la mise en œuvre de procédures opérationnelle sur les menaces de cybersécurité, telles que des tests d'intrusion réguliers, le partage d'informations classifiées et des meilleures pratiques, formalisées dans des lettres d'accord techniques dans le domaine de la cybersécurité.
3. Encourager les États et les organisations à travailler de manière décisive dans le cadre de l'approche coopérative pour définir et mettre en œuvre les plans d'action réactifs et proactifs nécessaires pour relever le défi de la cybersécurité en élaborant des plans conjoints de reprise des activités et de continuité des activités en cas de cyberattaque.
4. Soutenir le matériel d'orientation et élaborer et mettre en œuvre des politiques pour l'utilisation du Protocole sur les feux de circulation par les États et les organisations.

Annexe 1:

La Cybersécurité est une responsabilité partagée

