Organisation de l'aviation civile internationale

AN-Conf/13-WP/42
28/8/18

NOTE DE TRAVAIL

TREIZIÈME CONFÉRENCE DE NAVIGATION AÉRIENNE

Montréal (Canada), 9 – 19 octobre 2018

COMITÉ A

Point 5 : Questions émergentes
5.4 : Cyberrésilience

RENFORCEMENT DES CONCEPTS DE CYBERSÉCURITÉ DANS LE DOMAINE DE L'AVIATION

(Note présentée par l'Autriche au nom de l'Union européenne et de ses États membres[1], par les autres États membres de la Conférence européenne de l'aviation civile[2] et par EUROCONTROL)

RÉSUMÉ ANALYTIQUE

La présente note propose un aperçu des raisons pour lesquelles les organisations devraient gérer leurs risques, produits et services en matière de cybersécurité au moyen d'un système de gestion de la sécurité de l'information (ISMS) qui tient compte des risques liés à leurs interactions avec d'autres organisations ou avec les systèmes qu'elles exploitent.

La note met aussi l'accent sur la fiabilité et explique pourquoi elle est un élément nécessaire et décrit les avantages que procure l'utilisation d'un ISMS aux organisations. Elle montre en outre qu'un niveau équivalent de cybersécurité des systèmes connectés, quels que soient l'heure et l'endroit, est un préalable essentiel et fournit les éléments de sa réalisation pour les opérations sol-sol ou air-sol.

Elle présente également l'importance critique d'une perspective commune en matière d'aviation ainsi que les avantages découlant de l'échange d'informations.

Suite à donner : La Conférence est invitée à approuver les recommandations figurant au paragraphe 3.

[1] Allemagne, Autriche, Belgique, Bulgarie, Chypre, Croatie, Danemark, Espagne, Estonie, Finlande, France, Grèce, Hongrie, Irlande, Italie, Lettonie, Lituanie, Luxembourg, Malte, Pays-Bas, Pologne, Portugal, République tchèque, Roumanie, Royaume-Uni, Slovaquie, Slovénie et Suède.

[2] Albanie, Arménie, Azerbaïdjan, Bosnie-Herzégovine, Géorgie, Islande, L'ex-République yougoslave de Macédoine, Monaco, Monténégro, Norvège, République de Moldova, Saint-Marin, Serbie, Suisse, Turquie et Ukraine.

1. INTRODUCTION

1.1 Afin de garantir la sécurité et la sûreté de l'aviation civile, un secteur confronté à une numérisation croissante, il est fondamental de disposer d'informations exactes et de systèmes essentiels pour la sécurité pleinement opérationnels. Vu le haut degré d'intégration du système aéronautique et la diffusion de l'information au niveau mondial, les initiatives de cybersécurité dans le secteur aéronautique doivent s'appuyer sur une approche intégrée et de bout en bout.

1.2 La présente note fait ressortir les avantages de l'introduction de systèmes de gestion de la sécurité de l'information (ISMS) dans le secteur aéronautique. Ces systèmes, de préférence harmonisés ou combinés avec les systèmes de gestion des risques en aviation déjà en place, aident les organisations et le secteur dans son ensemble à mieux se préparer pour faire face aux menaces à la sécurité de l'information.

1.3 Une approche commune des systèmes de gestion permet de coordonner les mesures dans l'ensemble du secteur, compte tenu du fait que l'information est partagée, que les mêmes systèmes sont utilisés par de nombreux acteurs du secteur et que les risques sont partagés.

1.4 Outre l'approche ISMS, la présente note approfondit également la notion de confiance. En effet, dans le secteur de l'aviation, la confiance entre partenaires – en plus de la fiabilité – est primordiale. Pour cela, un système solide combinant formation, certification, contrôle, surveillance et contre-vérification permet d'instaurer pour chaque vol une confiance mutuelle entre tous les partenaires, qui peuvent ainsi s'acquitter consciencieusement et correctement de leurs tâches respectives dans la chaîne du transport aérien.

2. ANALYSE

2.1 **Comment tirer avantage d'un ISMS.** Les concepts actuels en matière d'ISMS se limitent intrinsèquement aux organisations individuelles. Or, l'aviation civile est un tel système de systèmes étroitement imbriqués, composé de produits, de personnes et de processus interdépendants, et présentant même des connexions avec des systèmes militaires[3], qu'on ne peut plus l'envisager uniquement du point de vue d'une organisation individuelle. Ainsi, l'aviation civile devra introduire l'ISMS en y intégrant l'idée de gestion inter-organisationnelle de la cybersécurité.

2.2 Une stratégie ISMS coordonnée à l'échelle mondiale représente donc un instrument clé pour le secteur de l'aviation civile. Un tel cadre mondial faciliterait la mise en œuvre cohérente de plusieurs concepts auxiliaires, comme une infrastructure de communication interopérable et sécurisée à l'échelle mondiale, ainsi qu'un cadre de confiance, ou tout autre concept, propices à la mise en place d'un futur système fondé sur l'échange fiable d'informations. Sachant qu'on ne construit pas l'avenir en un jour, il sera nécessaire de faciliter l'évolution individuelle des organisations, États ou régions. La mise en place de l'ISMS dans toutes les organisations sera une condition préalable à la concrétisation de ces concepts. En outre, sa mise en œuvre devra s'aligner sur les systèmes actuels de gestion de la sécurité (p. ex. Annexe 19 — *Gestion de la sécurité*), la gestion des risques en matière de sûreté aérienne, les dispositions de l'OACI et les normes de l'industrie, ainsi que sur des mécanismes de surveillance efficaces.

2.3 **Le concept de fiabilité.** Au fil des décennies, l'aviation civile s'est dotée d'un cadre de confiance solide. Aujourd'hui, la fiabilité est un concept officiel grâce auquel une organisation, ou un système qu'elle exploite, peut s'appuyer sur les propriétés relatives à la cybersécurité d'une autre

[3] Voir la note AN-Conf/13-WP/39.

organisation ou d'un système qu'elle utilise[4]. La confiance n'étant jamais absolue, le concept propose plusieurs niveaux de fiabilité en fonction de l'incidence (sécurité ou continuité du service, p. ex. acheminement rapide de la circulation aérienne dans une région) qu'il aura sur la partie impliquée.

2.4 Par exemple, dans le domaine de la certification des aéronefs, la confiance en matière de navigabilité découle en grande partie de l'assurance que les mesures appropriées ont été prises et ont produit des résultats acceptables. Ces mesures ont été conçues pour gérer la gravité des incidences des risques de sécurité. Ainsi, des niveaux de gravité des incidences plus élevés nécessiteront des examens encore plus poussés pendant la phase de développement. Un concept similaire est proposé pour les propriétés relatives à la cybersécurité et vise à montrer l'efficacité de la protection contre les cybermenaces. En substance, c'est la confiance dans l'absence d'erreurs de développement et de vulnérabilités ainsi que dans les organisations qui protègent correctement l'aviation civile qui préparera le futur pour voler en toute sécurité. Il conviendrait d'intégrer le concept de fiabilité dans l'ISMS, qui serait à son tour harmonisé ou combiné avec les systèmes de gestion existants.

2.5 **Conditions d'exploitation de la cybersécurité.** Pour tirer pleinement avantage du concept de fiabilité, il importe de traiter également de la dynamique de l'évolution des différentes organisations et des systèmes qu'elles exploitent, qui appartiennent à l'infrastructure sécurisée et interopérable à l'échelle mondiale. Des conditions d'exploitation prédéterminées de la cybersécurité seraient une façon de résoudre ce problème. Pour chaque connexion entre pairs, il faudra obligatoirement que les niveaux de fiabilité soient compatibles entre eux, d'où la nécessité ensuite de définir les appairages. Certaines paires de niveaux de fiabilité seront autorisées à se connecter dans la mesure où elles atteindront les objectifs de la cybersécurité avec des niveaux de risque acceptables. D'autres paires ne pourront peut-être pas atteindre les objectifs fixés. Cette situation encouragera les pairs à parvenir à un accord sur les conditions en matière de niveaux de fiabilité compatibles mais cependant différents, ce qui permettra à terme de définir des approches équilibrées. Il faut faire la distinction entre deux niveaux de migration des connexions entre pairs : celui concernant les organisations dont les systèmes sont connectés d'une part, et d'autre part celui entre les véhicules aériens ou spatiaux et les systèmes basés au sol, qui changent rapidement de connexions. La vitesse d'évolution de leurs conditions de cybersécurité joue un rôle clé dans cette distinction.

2.6 Évolution lente : d'une part, les systèmes basés au sol en général – et la gestion du trafic aérien (ATM) et les services de navigation aérienne (ANS) en particulier – évoluent relativement lentement. Les changements dans leurs conditions d'exploitation dépendent largement des modifications qui interviennent au niveau de leur propre situation de cybersécurité ou de celle des systèmes auxquels ils sont connectés. Ceci permet une adaptation étroitement coordonnée des propriétés en matière de cybersécurité afin que toutes les parties connectées répondent aux exigences générales de cybersécurité. Le concept de conditions d'exploitation assure le bon appairage des niveaux de fiabilité entre les organisations connectées.

2.7 Évolution rapide : d'autre part, les aéronefs se déplacent d'un endroit à un autre relativement rapidement, tout en se connectant de manière dynamique à un nombre élevé de pairs dans un court laps de temps. En général, les aéronefs ou les systèmes ATM/ANS ne sont pas dans un état de cybersécurité leur permettant de s'apparier un jour donné. Pour qu'ils demeurent opérationnels, la migration sera nécessaire de part et d'autre. L'adaptation du concept des conditions d'exploitation pourrait apporter une réponse à la question de la cybersécurité. Si l'on prend l'exemple du concept actuel des conditions d'exploitation, le respect des exigences en matière de séparation horizontale applicables dans un espace aérien requiert certains équipements au sol et à bord de l'aéronef. Le concept de

[4] La note d'information (AN-Conf/13-WP/160) expliquera les concepts et les principes de l'ISMS, les concepts de fiabilité et de conditions d'exploitation de la cybersécurité ainsi que les avantages du partage de l'information

conditions d'exploitation pourrait donc servir de guide en matière de cybersécurité, en répondant aux exigences en rapport avec les propriétés de la cybersécurité introduites par les niveaux de fiabilité. L'appariement adéquat des niveaux de fiabilité entre les ATM/ANS et les systèmes d'aéronefs permettrait une utilisation sûre et sécurisée de l'espace aérien.

2.8 **Échange d'informations sur les questions de cybersécurité.** L'échange d'informations pourrait également être traité comme un élément d'un ISMS. Un cadre d'ISMS à l'échelle mondiale pourrait en outre aider à créer un mécanisme d'échange d'informations plus cohérent sur les risques de cybersécurité. Le monde des technologies de l'information (TI) a créé le concept d'un centre de cybersécurité, chargé de « gérer » l'information relative aux incidents de cybersécurité, de recueillir et de tenir à jour les bases de données des incidents, menaces et vulnérabilités et de fournir des analyses et des orientations sur les pratiques éprouvées à même de contrer les incidents en question. L'ensemble de ces tâches participe de l'échange d'informations.

2.9 Sur le plan international, les équipes d'intervention en cas d'urgence informatique (CERT) et les équipes d'intervention en cas d'incident lié à la sécurité informatique (CSIRT) ont créé une communauté appelée *Forum for Incident Response and Security Teams (FIRST) (Forum des équipes de sécurité et d'intervention en cas d'incident)*. La communauté de l'aviation pourrait se servir de ce forum aux fins d'une approche concertée de l'échange d'informations à l'échelle mondiale, dans le but non seulement de réagir aux incidents mais également de faire échec aux nouvelles attaques. En dévoilant de nouvelles vulnérabilités, les informations recueillies par les CSIRT permettront dans une certaine mesure d'anticiper les risques émergents et par là même de prendre des mesures préventives pour limiter les effets néfastes sur l'aviation civile. En résumé, l'objectif est de mieux sensibiliser aux cybermenaces et aux vulnérabilités affectant les systèmes aéronautiques. Lorsque la coordination des CSIRT aéronautiques et de leurs membres respectifs sera effective, il sera possible d'harmoniser au niveau international les mesures d'atténuation et de défense pour contrer les cybermenaces.

2.10 Les menaces contre la cybersécurité ne se limitent pas à l'aviation, puisqu'elles touchent d'autres secteurs du transport ainsi que des secteurs autres que le transport (système bancaire, industrie nucléaire). Ces secteurs ont souvent des technologies et des implémentations en commun, d'où les menaces et les vulnérabilités qui en découlent. Il est donc fondamental de partager les politiques, les renseignements et les meilleures pratiques avec les organisations de ces secteurs. Une approche de la cybersécurité dans l'aviation civile pourrait ainsi s'enrichir d'autres approches et expériences intersectorielles nationales ou régionales. Par ailleurs, une étroite collaboration avec les entités gouvernementales engagées dans la cybersécurité d'autres secteurs permettra d'augmenter les retombées positive*s* pour les autorités de l'aviation civile des États.

3. CONCLUSION

3.1 La conférence est invitée à approuver les recommandations suivantes :

Il est recommandé que la Conférence :

a) prie instamment l'OACI d'aider les États à exiger des organisations qu'elles se chargent de la gestion des risques de cybersécurité qui menacent leurs activités, produits et services, ainsi que les interfaces avec les pairs, par l'entremise d'un système de gestion de la sécurité de l'information (ISMS) fondé sur des normes internationales de l'industrie et, de préférence, harmonisé et combiné avec les systèmes de gestion déjà en place ;

b) demande à l'OACI d'encourager les États à prendre les mesures appropriées afin de mettre en place une infrastructure interopérable à l'échelle internationale, qui soit résiliente face aux cyberattaques. Celle-ci devra répondre aux critères d'interopérabilité et de cybersécurité de manière à renforcer tant les objectifs globaux que ceux de niveau supérieur relatifs à la sécurité et à l'acheminement rapide de la circulation aérienne ;

c) prie instamment l'OACI d'élaborer, selon une approche pluridisciplinaire, des dispositions aux fins de la confiance inter-organisationnelle, s'inscrivant dans le cadre d'un dispositif de confiance plus large, et d'encourager leur mise en œuvre ;

d) demande à l'OACI d'encourager les États à prendre des mesures, comme celle qui vise à ce que les exploitants aériens instaurent et facilitent l'échange d'informations opérationnelles en matière de cybersécurité par les voies appropriées qui auront été désignées, comme un réseau mondial d'« organisations de confiance » ;

e) prie instamment l'OACI de faciliter l'élaboration de dispositions relatives à la fiabilité et aux conditions d'exploitation de la cybersécurité de sorte que cette structure interopérable à l'échelle internationale soit exploitée de manière sécurisée ;

f) demande à l'OACI d'encourager les États à étendre la portée des canaux de communication existants consacrés à la cybersécurité, ou à en créer de nouveaux, afin de mieux faire face aux risques en matière de sécurité et de sûreté de l'aviation et d'assurer l'acheminement rapide de la circulation aérienne ;

g) demande à l'OACI d'appeler les États à promouvoir la collaboration intersectorielle gouvernementale et non gouvernementale sur la cybersécurité entre les secteurs de l'aéronautique et les autres secteurs.

— FIN —