Organisation de l'aviation civile internationale

AN-Conf/14-WP/113[1]
28/6/24

NOTE DE TRAVAIL

QUATORZIÈME CONFÉRENCE DE NAVIGATION AÉRIENNE

Montréal (Canada), 26 août – 6 septembre 2024

Point 4 : Hyperconnectivité du système de navigation aérienne
4.2 : Cybersécurité et résilience des systèmes d'information

CYBERSÉCURITÉ – GESTION DES RISQUES ET INVENTAIRE DES CYBERACTIFS INFORMATIONNELS DES SERVICES DE NAVIGATION AÉRIENNE (ANS)

[Note présentée par le Chili, avec l'appui de 20 États membres de la Commission latino-américaine de l'aviation civile (CLAC)[2]]

RÉSUMÉ ANALYTIQUE

La présente note contient des orientations générales en matière de cybersécurité qui devraient être prises en considération par les services de navigation aérienne (ANS) afin de lutter contre les menaces qui pèsent actuellement sur les systèmes technologiques utilisés dans ce domaine. L'échange constant d'informations rend ces systèmes vulnérables aux cyberattaques.

Cette situation est attribuable à la structure fonctionnelle du système de l'aviation, qui comprend les autorités de l'aviation civile, les fournisseurs de services de navigation aérienne (ANSP), les exploitants d'aéroports et toute autre organisation concernée.

Suite à donner : La Conférence est invitée à :

a) promouvoir l'élaboration d'un plan de gestion des risques pour les ANS qui permette de cerner et d'atténuer toute menace en matière de cybersécurité à l'étape de la conception et de l'installation des réseaux et des systèmes requis et tout au long de leur exploitation ;
b) promouvoir les fonctionnalités qui facilitent la gestion des risques, telles que la mise en place d'un répertoire unique et intégré pour chaque cyberactif recensé nécessaire aux ANS, et qui permettent de cerner les menaces, et de hiérarchiser les priorités en ce qui concerne les actions, le maintien, et le rétablissement rapide du système, si nécessaire ;
c) renouveler son engagement d'amélioration continue des différents processus, y compris ceux désignés comme critiques, afin d'atteindre des niveaux de cybersécurité optimaux dans les ANS.

1. INTRODUCTION

1.1 Les changements technologiques mis en œuvre dans différentes organisations de la société ont accru leur exposition à la cyberdélinquance. Les services de navigation aérienne (ANS) n'échappent pas non plus à ce problème, et il y a donc une volonté de mettre au point des stratégies et d'établir des

[1] Version en espagnol fournie par le Chili.
[2] Argentine, Aruba, Belize, Brésil, Colombie, Costa Rica, Cuba, Équateur, El Salvador, Guatemala, Honduras, Jamaïque, Mexique, Nicaragua, Panama, Paraguay, Pérou, République dominicaine, Uruguay et Venezuela (République bolivarienne du).

barrières de protection contre cette menace latente et croissante, qui pourrait potentiellement avoir une incidence sur les niveaux optimaux de sûreté opérationnelle.

1.2 La nécessité d'élaborer des méthodes de gestion des risques pour cerner et atténuer les menaces de cybersécurité pesant sur les systèmes des ANS exige un engagement renouvelé en faveur de l'amélioration continue des différents processus, y compris ceux qu'une organisation juge critiques.

1.3 Toute politique sur la cybersécurité des ANS devrait prendre en considération l'ensemble du cycle de vie des systèmes de l'aviation et inclure des éléments tels que la culture de la cybersécurité, la promotion de la sûreté intégrée, la sûreté de la chaîne logistique pour les programmes et équipements informatiques, l'intégrité des données, un contrôle d'accès approprié, la gestion proactive des vulnérabilités, l'amélioration des délais de mise à jour des systèmes et l'incorporation de systèmes et de processus de contrôle des données.

2. ANALYSE

2.1 L'objectif d'un système de navigation interopérable à l'échelle mondiale suppose le partage des réseaux et des infrastructures informatiques, des architectures et des opérations réseaucentriques. Dans l'avenir, l'échange d'informations ne se limitera pas aux communications de point à point, mais reposera également sur l'architecture de systèmes ouverts et le flux d'informations provenant de l'Internet. Tout cela rend le système plus vulnérable aux cyberattaques.

2.2 La mise en œuvre de la cybersécurité dans les ANS doit tenir compte de la protection et de la résilience des réseaux et des systèmes et de la continuité de leur fonctionnement, ainsi que de la confidentialité, de l'intégrité et de la disponibilité de l'information. Ce dernier point exige une analyse des incidences opérationnelles et du cycle de vie du système.

2.3 Un cyberincident s'entend de tout événement compromettant la disponibilité, l'authenticité, l'intégrité ou la confidentialité des systèmes, ou des données stockées, transmises ou traitées, ou des services correspondants offerts au moyen de systèmes d'information et de leur infrastructure, et susceptible d'affecter leur fonctionnement normal.

2.4 Les ANS sont exposés à une série de cybermenaces telles que les inondations d'information, l'interception passive d'informations, l'interception active d'informations, la modification de configurations de systèmes ou de données, la destruction de configurations de systèmes, les attaques par interruption de service ou par déni de service, et d'autres encore.

2.5 Les fournisseurs de services de navigation aérienne (ANSP) devraient recenser les supports logiques et physiques des systèmes d'information critiques qu'ils utilisent et tenir compte du niveau d'incidence sur ces systèmes en cas d'endommagement ou d'interruption.

2.6 Les mesures de protection des systèmes d'information critiques devraient être mises en œuvre le plus tôt possible au moment de la conception afin qu'elles puissent offrir la meilleure résilience possible pour résister aux cyberattaques.

2.7 Les mesures de sûreté de l'infrastructure devraient tenir compte de la sûreté intégrée, de la séparation de réseau et de l'accès à distance.

2.8 Les mesures de sûreté applicables aux supports physiques et logiques de la chaîne logistique devraient tenir compte de la mise à jour périodique des systèmes de technologie de l'information

et des communications (TIC) nécessaires à l'aviation en raison de l'évolution des exigences opérationnelles et de la modernisation des supports logiques.

2.9 Pour mettre en œuvre un plan de gestion des risques pour les ANS, il faudrait au moins faire l'inventaire des cyberactifs associés à la gestion du trafic aérien (ATM) et définir les niveaux de classification des incidents, des dangers et des incidences sur les systèmes.

	DESCRIPTION OF PROCESSES							
Strategic product	Process	Sub-process	Asset name	Identifier or Code	Type	Location	Person responsible / Owner	Support

				CRITICALITY ANALYSIS			
Storage medium	Retention time	Disposal	Search criterion	Confidentiality	Integrity	Availability	Criticality

Figure 1. Tableau d'inventaire des cyberactifs associés à l'ATM

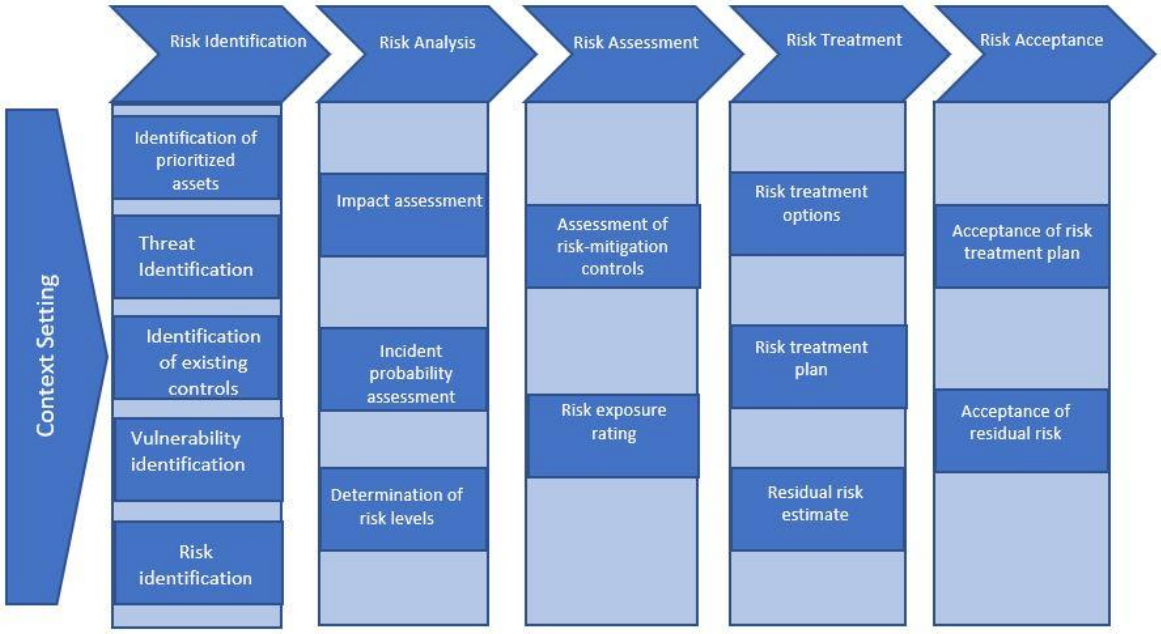

Figure 2. Diagramme de gestion des risques

		Susceptibilty						Risk																	
								Probability of occurrence									Impact								
								Threat agent factors				Vulnerability factors					Technical factors					Business fac			
ASSET ID	Vulnerability	Identity fraud (Authenticity)	Manipulation (Integrity)	Rejection (No Rejection)	Information disclosure (Confidentiality)	Denial of service (Availability)	Privilege escalation (Authorization)	Skill level	Motivation	Opportunity	Size	Ease of discovery	Ease of exploitation	Awareness	Intrusion detection	**Total probability of occurrence**	Loss of confidentiality	Loss of integrity	Loss of availability	Loss of responsibility	Overall technical impact	Financial loss	Reputational damage	Non-compliance	
ASST 17	Description of vulnerability	S	T	R	I		E	9	4	4	3	4	3	3	4	**4.25**	2	2	2	2	**2**	6	3	3	
ASST 17		S	T			I	D	E	4	4	7	4	4	4	7	4	**4.75**	4	4	3	3	**3.5**	3	4	4	
ASST 17		S	T	R	I	D	E	4	4	7	9	9	9	9	3	**6.75**	7	7	0	0	**3.5**	0	0	0	
ASST 16 & 17		S	T	R	I	D	E	4	4	7	9	9	9	9	3	**6.75**	2	2	2	2	**2**	2	2	2	
ASST 17		S	T			I	D	E	0	0	0	0	0	0	0	0	**0**	0	0	0	0	**0**	0	0	0	
ASST 16 & 17		S	T			I	D	E	0	0	0	0	0	0	0	0	**0**	0	0	0	0	**0**	0	0	0	

Figure 3. Analyse des risques et tableau des vulnérabilités des actifs recensés

2.10 Tout plan de gestion des risques devrait permettre d'anticiper les conséquences découlant de menaces telles que les cyberattaques et les cyberincidents non hostiles sur la base d'une analyse et d'une évaluation des risques auxquels les réseaux et systèmes sont exposés, afin de les éviter ou d'en réduire le nombre. Afin d'atténuer les incidences possibles, il faut déterminer les actions immédiates et les mesures d'amélioration progressive ainsi que leurs indicateurs, contrôles et documents correspondants.

2.11 Pour faciliter la gestion des risques, il conviendrait notamment d'envisager la création d'un répertoire unique pour chaque cyberactif associé à l'ATM. Cela permettrait :

a) de regrouper les cyberactifs de même type et/ou disposant d'un même cycle de vie ;

b) d'assurer l'intégrité des données ;

c) de promouvoir le succès des actions visant à conserver la résilience du système ;

d) de prévenir la duplication ou l'obsolescence des éléments ;

e) de réduire l'effort requis pour l'analyse et la prise de décision.

3. CONCLUSION

3.1 La nécessité de mettre en œuvre des stratégies de cybersécurité pour contrer les menaces numériques qui pèsent sur les ANS exige que les fournisseurs de ces services élaborent des plans et des protocoles de travail pour protéger les systèmes et l'infrastructure connexe, et s'assurer qu'ils sont suffisamment résilients pour conserver *la confidentialité, l'intégrité et la disponibilité* des informations.

3.2 Compte tenu de ce qui précède, et dans le contexte du Plan d'action de l'OACI pour la cybersécurité, la Conférence est invitée à convenir :

que les fournisseurs de services de navigation aérienne devraient :

a) élaborer un plan de gestion des risques liés aux cybermenaces qui comprend au moins l'inventaire des cyberactifs associés à la gestion de trafic aérien (ATM), la classification des incidents et des niveaux de danger, le niveau d'incidence sur le système et des protocoles de rétablissement du système ;

b) envisager d’inclure dans la gestion des risques des facteurs habilitants, tels que la conception d’un répertoire unique pour chaque cyberactif associé à l’ATM interopérable ;

c) renouveler leur engagement d’amélioration continue des différents processus, y compris ceux désignés comme critiques, afin d’atteindre des niveaux de cybersécurité optimaux dans les services de navigation aérienne.

— FIN —