Organisation de l'aviation civile internationale

NOTE DE TRAVAIL

A41-WP/241
EX/108
2/8/22

ASSEMBLÉE — 41e SESSION

COMITÉ EXÉCUTIF

Point 14 : Sûreté de l'aviation — Politique

SÉCURISER L'AVIATION PAR L'APPROCHE DE LA CONFIANCE ZÉRO

(Note présentée par l'Afrique du Sud)

RÉSUMÉ ANALYTIQUE

Le secteur de l'aviation est parfois tributaire de grandes chaînes d'approvisionnement englobant des industries variées, ce qui augmente l'étendue des menaces dans le secteur. L'adoption de systèmes fondés sur le protocole Internet (IP) pour améliorer l'efficacité exige l'adoption d'approches proactives nécessaires à la protection des systèmes actuels et anciens.

Le plan d'action pour la cybersécurité de l'OACI souligne la nécessité de centrer les ressources et les actions pour parvenir à une approche systématique de gestion de la cybersécurité dans l'aviation, l'objectif étant l'élaboration d'une approche systémique qui permette à l'aviation de s'adapter en temps utile et de résister aux menaces nouvelles.

La présente note décrit le concept de confiance zéro, que les États et d'autres acteurs de l'aviation pourraient adopter comme principe d'atténuation. L'incorporation de la confiance zéro peut renforcer les capacités actuelles en matière de protection de la cybersécurité par l'application de systèmes de bout en bout. Elle s'éloigne de la sécurité périmétrique traditionnelle en mettant en œuvre des dispositifs de sécurité à la périphérie ou plus près des installations de contrôle du trafic de l'utilisateur final et des sites distants (radar) des données d'aide à la navigation au sol.

Suite à donner : L'Assemblée est invitée à :

a) reconnaître l'avantage de la mise en œuvre d'approches souples et adaptatives d'évaluation continue adaptative du risque et de la confiance (CARTA : *Continuous, Adaptive Risk, and Trust Assessment*) dans le cadre de la protection des activités aéronautiques ;
b) demander à l'OACI, par le biais du Groupe d'experts de la cybersécurité, d'élaborer des éléments indicatifs techniques pour aider les États à inrégrer la confiance zéro dans les systèmes de management de la sécurité de l'information (SMSI) ;
c) exhorter les États à envisager d'incorporer les principes de la confiance zéro dans leur SMSI.

Objectifs stratégiques :	La présente note de travail se rapporte à l'objectif stratégique *Sûreté et facilitation*
Incidences financières :	Pas d'incidences financières supplémentaires, car les activités auront lieu dans les limites du budget alloué à l'OACI.
Références :	*Plan d'action pour la cybersécurité*

	Doc 8973, *Manuel de sûreté de l'aviation*

1. INTRODUCTION

1.1 Ces dernières années, l'industrie de l'aviation a connu une transformation favorisée par l'adoption de technologies et, par suite, une augmentation des cyberrisques qui appelle l'attention. Ce gigantesque bond en avant technologique sans précédent nécessite l'adoption constante d'approches et de modèles d'évaluation continue adaptative du risque et de la confiance (CARTA).

1.2 L'industrie de l'aviation était jusqu'à présent vue isolément. Mais l'interdépendance et la convergence des technologies de l'information (TI) et des technologies opérationnelles (TO) dans l'écosystème de l'aviation ont amené sur la scène des parties prenantes diverses qui ne sont pas régies par les mécanismes de conformité de l'aviation. Cela a augmenté la surface de cyberattaque possible et nécessite la révision de certains concepts traditionnels.

1.3 Auparavant, la gestion et la maintenance du matériel et des logiciels aéronautiques pouvaient se faire par le biais d'un accès à distance sécurisé RVP, et, dans le monde actuel, ce type de connexion a compromis la sécurité des systèmes.

1.4 Les cybermenaces telles que les rançongiciels, le vol de données et les attaques par hameçonnage sont devenues chose courante dans l'industrie de l'aviation, affectant les environnements informatiques (accès ERP, services de collaboration, services de courrier électronique) et les environnements technologiques opérationnels (SCADA, PLC) en ciblant les zones de contrôle dans et autour des aéroports et des centres de données.

2. ANALYSE

2.1 La chaîne d'approvisionnement étendue de l'aviation est susceptible d'introduire des cybermenaces, ce qui rend d'autant plus nécessaire l'adoption d'approches novatrices et nouvelles pour répondre à ces menaces. Cela est dû au fait que l'aviation dépend de multiples parties prenantes dont les différents systèmes, applications et technologies doivent s'intégrer les uns aux autres.

2.2 Il convient également de noter que la mise en œuvre de ces opérations peut nécessiter un soutien à distance de la part de ressources situées à l'intérieur et à l'extérieur des frontières nationales, ce qui expose davantage la chaîne des valeurs du transport aérien aux cybermenaces.

2.3 Les anciennes méthodes de sécurité périmétriques des réseaux, qui étaient utilisées pour répondre aux besoins de sécurité, se sont avérées inefficaces. L'augmentation des cyber-événements dans l'industrie de l'aviation en est la preuve. Une fois que les attaquants ont franchi le périmètre, les mouvements latéraux ultérieurs ne sont pas entravés.

2.4 Des concepts comme celui de la confiance zéro peuvent permettre de faire face aux menaces de nouvelle génération et sophistiquées qui prévalent aujourd'hui. Il s'agit de permettre à chaque demande de ressources de déclencher un processus d'évaluation de la posture, de validation de la posture et d'octroi de l'accès aux ressources au moyen de contrôles de sécurité réfléchis et efficaces

2.5 L'approche de confiance zéro fournit un ensemble de principes directeurs pour le flux de travail, la conception du système et les opérations, qui peuvent servir à améliorer la posture de sécurité des activités critiques et sensibles. Dans le but de prévenir les violations de données et de limiter les mouvements latéraux internes.

2.6 L'approche de confiance zéro part du principe que l'on ne peut faire confiance à personne, que ce soit à l'intérieur ou à l'extérieur de l'organisation. Cette approche vise à minimiser la surface d'attaque en se fondant sur les idées clés suivantes :

a) le périmètre n'existe pas. Élimination de l'hypothèse selon laquelle il faut faire confiance aux gens parce qu'ils ont pénétré dans un réseau d'entreprise ;

b) vérification des utilisateurs avant d'accorder l'accès et vérification de l'intégrité des dispositifs avant de se connecter au réseau ;

c) élimination de l'hypothèse selon laquelle les utilisateurs feront ce qu'il faut. Au lieu de cela, exiger des droits d'accès vérifiés pour chaque demande de service ;

d) plutôt que de traquer les mauvais actifs, mettre en place des obstacles pour ralentir la performance.

2.7 L'incorporation de la confiance zéro peut renforcer les capacités de la cybersécurité par une protection de bout en bout des systèmes. Elle s'éloigne de la sécurité périmétrique traditionnelle en mettant en place des dispositifs de sécurité à la périphérie ou plus près des installations de contrôle du trafic de l'utilisateur final et des sites distants (radar) et des données d'aide à la navigation au sol.

2.8 La mise en œuvre de la confiance zéro repose sur différentes technologies sous-jacentes qui offrent une protection sur plusieurs fronts :

a) la microsegmentation, le tout premier concept de la confiance zéro, est principalement conçu pour protéger contre les mouvements latéraux afin de minimiser l'incidence d'une violation. Le mouvement latéral pour capturer des informations sur les actifs clés du centre de données est un élément central de plusieurs attaques. La microsegmentation vise à limiter les communications non autorisées entre les charges de travail si ces dernières n'ont aucune raison opérationnelle de communiquer, en minimisant l'incidence de la violation. Contrairement à la protection nord-sud caractéristique des pare-feu, la microsegmentation s'intéresse à la sécurité est-ouest des charges de travail ;

b) l'accès au réseau de confiance zéro crée une frontière logique fondée sur le contexte pour l'accès aux applications. L'objectif est de minimiser l'accès aux applications et les abus en fonction du contexte de l'utilisateur et du dispositif. Il remet en question l'hypothèse selon laquelle l'emplacement d'une entité (par ex., à l'intérieur d'un réseau) doit se voir accorder automatiquement la confiance ;

c) la confiance zéro cache toutes les applications sur le réseau et autorise l'accès en fonction d'attributs tels que l'identité de l'utilisateur, le dispositif, la géolocalisation et la posture de sécurité. Cela signifie que les utilisateurs ont accès aux applications dont ils ont besoin, mais qu'ils ne voient rien d'autre sur le réseau ;

d) l'isolement du navigateur à distance part du principe que les utilisateurs finaux représentent les maillons les plus faibles de toute organisation et que l'accès à Internet est l'une des plus grandes surfaces d'attaque à l'origine des violations. Par conséquent, l'un des moyens les plus efficaces de minimiser la compromission du point final/de l'utilisateur final est d'isoler l'accès au web afin d'éliminer les attaques en ligne et des menaces comme les rançongiciels, les logiciels malveillants intégrés et l'hameçonnage.

3. CONCLUSION

3.1 Les principes de la confiance zéro peuvent être utilisés pour faire en sorte que l'aviation civile se renforce d'elle-même en adoptant une approche de « sûreté intégrée ». La sécurisation des éléments et processus critiques « dès la conception » s'est avérée efficace et change le paradigme de la sûreté, qui passe de réactif (boulonné) à proactif, et favorise le développement d'un système d'aviation civile qui se renforce lui-même - ce qui lui permet d'évoluer et d'améliorer sa résilience de manière plus automatisée.

— FIN —