Organisation de l'aviation civile internationale

NOTE DE TRAVAIL

AN-Conf/14-WP/136
30/6/24
Révision n° 1
30/7/24

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

MISE EN COMMUN D'INFORMATIONS VIA LA PLATEFORME D'ÉCHANGE D'INFORMATIONS SUR LES LOGICIELS MALVEILLANTS (MISP) ET CONTRIBUTION DE LA PLATEFORME AU RENFORCEMENT DE LA CYBERSÉCURITÉ ET DE LA RÉSILIENCE DES SYSTÈMES D'INFORMATION

(Note présentée par le Brésil et appuyée par 20 États membres[1] de la Commission latino-américaine de l'aviation civile [CLAC])

RÉVISION N° 1

RÉSUMÉ ANALYTIQUE

La présente note traite des efforts déployés par le Brésil en matière de cybersécurité de l'aviation pour assurer l'échange d'informations au moyen de la Plateforme d'échange d'informations sur les logiciels malveillants (MISP), donnant ainsi suite aux propositions du Groupe d'experts de la cybersécurité (CYSECP). Il y est fait remarquer que cette solution n'entraîne pas de dépenses additionnelles de cybersécurité et qu'elle favorise la collaboration entre États, organisations et entreprises du secteur pour renforcer la sécurité du cyberespace.

Suite à donner : La Conférence est invitée à :
a) noter que jusqu'à présent l'utilisation de la MISP par le Service de contrôle de l'espace aérien du Brésil (DECEA) en tant que plateforme pour l'échange d'informations sur la cybersécurité a été positive ;
b) encourager les États membres à adopter la MISP en tant que plateforme d'échange d'informations et de renseignements sur la cybersécurité ;
c) porter le sujet de la présente note à la connaissance du Groupe d'experts de la cybersécurité (CYSECP) et créer un groupe de travail chargé d'aborder la normalisation de l'échange d'informations en matière de cybersécurité et l'utilisation éventuelle de la MISP par les États membres.

[1] Argentine, Aruba (Royaume des Pays-Bas), Bélize, Chili, Colombie, Costa Rica, Cuba, Équateur, El Salvador, Guatemala, Honduras, Jamaïque, Mexique, Nicaragua, Panama, Paraguay, Pérou, Uruguay et Venezuela (République bolivarienne du).

1. INTRODUCTION

1.1 L'OACI améliore constamment ses normes et règlements pour faire face à l'environnement mondial de menaces, qui est en évolution permanente, conformément aux résolutions du Conseil de sécurité des Nations Unies qui soulignent l'obligation des États de protéger les services aériens sur leurs territoires. Les résolutions en question invitent instamment tous les États à collaborer avec l'OACI pour évaluer, améliorer et mettre en œuvre des normes de sûreté internationales. Le Plan d'action pour la cybersécurité (CyAP) a été formulé pour réaliser effectivement les objectifs énoncés dans les sept piliers de la stratégie de cybersécurité pour l'aviation et créer un environnement robuste de sécurité de l'information.

1.2 Les principales fonctions du DECEA comprennent la supervision du contrôle de l'espace aérien, la protection des vols, les services de recherche et de sauvetage, ainsi que la gestion des télécommunications de l'aviation civile au Brésil. De plus, le DECEA fournit un soutien logistique et assure la maintenance de systèmes de cybersécurité qui sont essentiels pour l'exécution de ces fonctions.

2. ANALYSE

2.1 Échange d'informations en matière de cybersécurité

2.1.1 Les menaces mondiales sont un sujet de préoccupation croissante. Pour assurer des opérations aériennes sûres et sans interruptions, les systèmes de navigation aérienne et de surveillance doivent être protégés lors des échanges d'information à l'échelle mondiale. Il est essentiel de recenser et de surveiller ces systèmes pour éviter que des vulnérabilités ne soient exploitées, provoquant des pannes et des interruptions de service. De plus, l'arrivée de nouveaux systèmes dans le contexte de l'hyper-connectivité de la navigation aérienne sera un enjeu majeur d'ici 2030. À cet égard, il est essentiel de déceler les menaces à temps pour que les dispositifs de cybersécurité puissent protéger plus efficacement les systèmes qui fournissent les services aériens.

2.1.2 Ainsi, l'échange d'informations sur les menaces contre la cybersécurité est en tous points conforme à la Politique nationale du Brésil sur la cybersécurité (PNCiber), promulguée par le décret n° 11 856 du 26 décembre 2023, dont l'un des objectifs vise à :

> --Art. 3, al. XI – « mettre en œuvre des stratégies de collaboration pour développer la coopération internationale en matière de cybersécurité ».

2.1.3 Dans le contexte de l'OACI, l'échange d'informations relatives à la cybersécurité est énoncé dans le Plan d'action pour la cybersécurité (CyAP, 2e édition, janvier 2022). L'échange d'informations est spécifiquement décrit au paragraphe 3.1.1 comme un des piliers de la stratégie du Plan d'action pour la cybersécurité.

2.2 Plateforme d'échange d'informations sur les logiciels malveillants

2.2.1 La Plateforme d'échange d'informations sur les logiciels malveillants (MISP) est un outil de cybersécurité essentiel pour l'échange de renseignements sur les menaces. Son adoption s'est généralisée en raison des nombreux avantages qu'elle offre aux organisations et aux professionnels de la cybersécurité. Voici certains de ses principaux avantages :

a) la plateforme MISP facilite la collaboration entre les organisations, permettant un échange d'informations sûr au sujet des menaces. C'est un élément clé dans un

environnement où les cybermenaces sont en constante évolution. La capacité d'échanger des indicateurs de compromission et des informations sur les menaces en temps réel permet de mettre en place un dispositif de défense plus robuste et plus efficace.

b) en centralisant et en diffusant l'information sur les menaces, la MISP offre aux organisations un accès en temps réel au renseignement sur les menaces. Cela permet de détecter rapidement les incidents et d'y réagir, améliorant ainsi la position générale de sécurité.

c) la MISP est très personnalisable et extensible, de sorte que les organisations peuvent l'adapter à leurs besoins spécifiques. On peut notamment y ajouter des attributs sur mesure, créer des modèles particuliers de menaces et intégrer la plateforme à d'autres outils de sûreté.

d) grâce à la plateforme, les utilisateurs sont connectés à des communautés de cybersécurité dans le monde et peuvent échanger des informations avec d'autres professionnels et organisations. La base de connaissances disponibles est ainsi élargie, ce qui renforce les moyens de défense contre des menaces à grande échelle et permet de comprendre les tactiques, les techniques et les procédures (TTP) employées par les adversaires.

e) la MISP est dotée de contrôles d'accès et de mécanismes de protection des renseignements personnels avancés pour faire en sorte que les organisations puissent échanger des renseignements de manière sélective et en toute sécurité. Cet aspect est fondamental pour protéger des données sensibles et se conformer à la réglementation sur la protection de la vie privée.

2.2.2 En résumé, la MISP est un outil fondamental pour gérer les cybermenaces, offrant une plateforme efficace d'échange d'informations en matière de cybersécurité. L'adoption de la plateforme renforce les défenses des organisations et la cybersécurité aux niveaux national, régional et mondial.

2.3 Utilisation de la plateforme MISP par le DECEA

2.3.1 Le DECEA a commencé à implanter la plateforme MISP en 2021 et se sert depuis de cet outil dont il a peaufiné l'utilisation. Ce perfectionnement permanent de son utilisation met en relief l'engagement du DECEA à rester au fait des défis en matière de cybersécurité, qui évoluent sans cesse.

2.3.2 L'adoption de la plateforme permet au DECEA de collaborer de manière effective avec d'autres parties prenantes brésiliennes, dont le Centre de traitement des incidents sur le réseau, de l'Armée de l'air (CTIR.FAB), la Compagnie brésilienne des pétroles (Petrobras), l'Agence nationale des télécommunications (ANATEL) et la Fédération brésilienne des banques (FEBRABAN), pour l'échange de renseignements critiques sur les menaces. Cette collaboration renforce les dispositifs de défense du DECEA, tout en contribuant à la sécurité générale du Système de contrôle de l'espace aérien brésilien (SISCEAB).

2.3.3 Les indicateurs de menaces et les alertes transmis par d'autres organismes au moyen de la MISP sont traités et forment la base pour l'élaboration des listes d'activités bloquées ou des règles relatives aux pare-feux. Ces indicateurs offrent un éclairage crucial sur des menaces potentielles à la sécurité, ce qui

permet aux organisations de protéger activement leurs réseaux et systèmes contre des activités malveillantes, de devancer les menaces émergentes et de renforcer leur position de cybersécurité.

2.3.4 Les règles associées à une menace sont déterminées par son niveau de risque dans le temps. Ce niveau de risque de chaque menace est continuellement actualisé en se fondant sur des indicateurs reçus au moyen de la MISP. Par l'ajustement dynamique du niveau de risque associé à chaque menace, les organisations s'assurent que leurs règles relatives aux pare-feux demeurent efficaces et réactives, pour un environnement plus sûr. Cette approche permet de mettre en place des stratégies d'atténuation des menaces plus adaptables de façon à renforcer la résilience générale de la cybersécurité.

2.3.5 À titre d'exemple, la figure 1 indique les dix types de menaces pour lesquelles le DECEA a reçu le plus d'alertes de la MISP au cours de la dernière année : le cheval de Troie Zeus, l'hameçonnage par URL, le logiciel malveillant Emotet IOC actualisé, le cheval de Troie Citadel et des sites d'hameçonnage.

2.3.6 Dans la figure 2, on peut voir le nombre d'activités malveillantes bloquées sur la base des indicateurs reçus dans la MISP au cours d'une semaine. On observe que la plateforme contribue à bloquer environ 40 millions d'activités malveillantes par année.

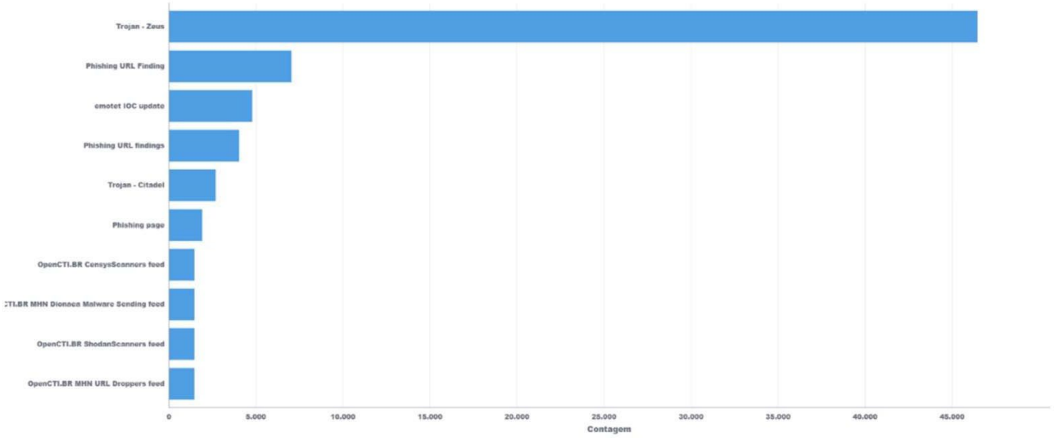

Figure 1 – Les dix principaux types de menaces reçus par le DECEA

Figure 2 – Activités malveillantes bloquées grâce aux indicateurs provenant de la MISP

2.3.7 Aujourd'hui, la MISP permet de recevoir une alerte ou de notifier une activité malveillante suspecte ou confirmée visant la sécurité des systèmes ou des réseaux informatiques, ce qui contribue à assurer la sécurité de l'information au SISCEAB.

3. CONCLUSION

3.1 L'utilisation par le DECEA de la plateforme MISP renforce de manière significative la cybersécurité de l'aviation au Brésil. Cette approche proactive répond aux normes internationales, comme celles du Plan d'action pour la cybersécurité (CyAP) de l'OACI. Le DECEA épaule également l'Agence nationale d'aviation civile du Brésil (ANAC) dans son utilisation de la MISP pour améliorer l'échange d'informations et de renseignements sur les cybermenaces dans l'aviation civile du Brésil, en tirant parti des capacités de la plateforme pour l'échange de renseignements en temps réel dans un environnement ouvert.

3.2 Le Brésil réaffirme son engagement à contribuer à assurer la sûreté de l'aviation internationale, en particulier dans le domaine de la cybersécurité. Son approche collaborative permet de renforcer aussi la sécurité de l'aviation dans le monde. Alors que l'hyperconnectivité accroît la surface d'exposition aux attaques des systèmes de navigation aérienne, il est déterminé à adopter les meilleures stratégies et technologies pour protéger son infrastructure critique de l'aviation contre l'évolution des cybermenaces.

3.3 Le Brésil entend encourager les membres de la région Caraïbes/Amérique du Sud (CAR/SAM) à utiliser la MISP parmi, examiner plus avant l'initiative d'échange d'informations et de renseignements sur les cybermenaces et y participer activement, de façon à promouvoir l'emploi de la MISP en tant que plateforme robuste de collaboration. L'objectif est d'augmenter la résilience des systèmes d'information de l'aviation régionale afin de parvenir, dans le futur, à une intégration à l'échelle mondiale, conformément aux recommandations de l'OACI.

3.4 Compte tenu de ce qui précède, la Conférence est invitée à approuver la recommandation suivante :

Recommandation 4.2/x – Cybersécurité et résilience des systèmes d'information

a) noter que l'utilisation par le Service de contrôle de l'espace aérien du Brésil (DECEA) de la Plateforme d'échange d'informations sur les logiciels malveillants (MISP) pour l'échange d'informations en matière de cybersécurité a été positive jusqu'à présent ;

b) encourager les États membres à adopter la MISP en tant que plateforme pour l'échange d'informations sur la cybersécurité ;

c) porter le sujet de la présente note à la connaissance du Groupe d'experts de la cybersécurité (CYSECP) et créer un groupe de travail chargé d'examiner la façon de normaliser l'échange d'informations sur la cybersécurité ainsi que l'emploi éventuel de la plateforme MISP par les États membres.

— FIN —