Organización de Aviación Civil Internacional

NOTA DE ESTUDIO

AN-Conf/14-WP/136
30/6/24
Revisión núm. 1
30/7/24

DECIMOCUARTA CONFERENCIA DE NAVEGACIÓN AÉREA

Montreal, Canadá, 26 de agosto - 6 de septiembre de 2024

Cuestión 4: Hiperconectividad del sistema de navegación aérea
4.2: Ciberseguridad y resiliencia de los sistemas de información

INTERCAMBIO DE INFORMACIÓN MEDIANTE LA PLATAFORMA DE INTERCAMBIO DE INFORMACIÓN SOBRE PROGRAMAS MALICIOSOS (MISP) Y CONTRIBUCIÓN DE LA PLATAFORMA A LA MEJORA DE LA CIBERSEGURIDAD Y LA RESILIENCIA DE LOS SISTEMAS DE INFORMACIÓN

[Nota presentada por el Brasil con el respaldo de 20 Estados miembros[1] de la Comisión Latinoamericana de Aviación Civil (CLAC)]

REVISIÓN NÚM. 1

RESUMEN

En esta nota de estudio se destacan las iniciativas sobre ciberseguridad de la aviación del Brasil relativas al intercambio de información sobre ciberseguridad mediante la Plataforma de Intercambio de Información sobre Programas Maliciosos (MISP), en consonancia con las propuestas del Grupo Experto en Ciberseguridad (CYSECP) de la OACI. Se hace hincapié en que esta solución no requiere gastos adicionales de ciberseguridad y fomenta la colaboración entre Estados, organizaciones e industria para mejorar la ciberseguridad operacional.

Medidas propuestas a la Conferencia: Se invita a la Conferencia a:

a) tomar nota de que el uso de la MISP por el Departamento de Control del Espacio Aéreo (DECEA) del Brasil como plataforma de intercambio de información sobre ciberseguridad ha sido positivo hasta la fecha;
b) animar a los Estados miembros a que adopten la MISP como plataforma de intercambio de información sobre ciberseguridad; y
c) transmitir el asunto de la presente nota al Grupo Experto en Ciberseguridad (CYSECP) y crear un grupo de trabajo que se ocupe de la normalización del intercambio de información sobre ciberseguridad y el posible uso de la plataforma MISP por los Estados miembros.

1. INTRODUCCIÓN

1.1 La OACI mejora continuamente sus normas y reglamentos para hacer frente al panorama mundial de amenazas, que se encuentra en constante cambio, en consonancia con las resoluciones del Consejo de Seguridad de las Naciones Unidas que hacen hincapié en la obligación de los Estados de salvaguardar

[1] Argentina, Aruba (Reino de los Países Bajos), Belice, Chile, Colombia, Costa Rica, Cuba, Ecuador, El Salvador, Guatemala, Honduras, Jamaica, México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana, Uruguay y Venezuela (República Bolivariana de).

los servicios aéreos dentro de su jurisdicción. En esas resoluciones se insta a todos los Estados a que colaboren con la OACI para evaluar, perfeccionar y aplicar normas internacionales de seguridad de la aviación. El Plan de Acción de Ciberseguridad (CyAP) se ha formulado para alcanzar de manera eficaz los objetivos descritos en los siete pilares de la Estrategia de Ciberseguridad de la Aviación y establecer un entorno sólido de ciberseguridad.

1.2 Las funciones principales del DECEA abarcan la supervisión del control del espacio aéreo, la protección de los vuelos, los servicios de búsqueda y salvamento, así como la gestión de las telecomunicaciones de la aviación civil brasileña. Además, el DECEA ofrece apoyo logístico y mantiene sistemas de ciberseguridad que son fundamentales para la ejecución de estas tareas.

2. ANÁLISIS

2.1 Intercambio de información sobre ciberseguridad

2.1.1 Las amenazas mundiales generan cada vez más preocupación. Para velar por la seguridad y continuidad de las operaciones de vuelo, los sistemas de navegación aérea y de vigilancia deben estar protegidos en los intercambios mundiales de información. Resulta fundamental determinar cuáles son estos sistemas y supervisarlos para evitar que se exploten las vulnerabilidades, con las consiguientes fallas o interrupciones del servicio. Además, la aparición de nuevos sistemas en el ámbito de la hiperconectividad de la navegación aérea constituirá un problema importante de aquí a 2030. En este contexto, resulta esencial detectar oportunamente las amenazas para que los activos de ciberseguridad puedan proteger con mayor eficacia los sistemas que prestan servicios de aviación.

2.1.2 Así, la práctica de intercambio de información sobre amenazas de ciberseguridad está en perfecta consonancia con la Política Nacional de Ciberseguridad del Brasil (PNCiber), establecida por el Decreto núm. 11.856, de fecha 26 de diciembre de 2023, que establece entre sus objetivos:

— art. 3, inc. XI – "implementación de estrategias de colaboración para desarrollar la cooperación internacional en ciberseguridad".

2.1.3 En el contexto de la OACI, el intercambio de información sobre ciberseguridad se enuncia en su Plan de Acción de Ciberseguridad (CyAP), segunda edición, enero de 2022. El intercambio de información se describe específicamente en el inciso 3.1.1 como uno de los pilares de la Estrategia de Ciberseguridad de la Aviación del CyAP.

2.2 Plataforma de Intercambio de Información sobre Programas Maliciosos

2.2.1 La Plataforma de Intercambio de Información sobre Programas Maliciosos (MISP) es una herramienta de ciberseguridad esencial para compartir información sobre amenazas. El uso de la plataforma se ha extendido gracias a los numerosos beneficios que ofrece a las organizaciones y a las personas expertas en ciberseguridad. Entre las ventajas más importantes, cabe mencionar:

a) La MISP facilita la colaboración entre organizaciones, lo que permite compartir de forma segura la información sobre amenazas. Esto resulta imprescindible en un contexto en el que las ciberamenazas están en constante evolución. La capacidad de intercambiar indicadores de comprometimiento e información sobre amenazas en tiempo real permite una defensa más sólida y eficaz.

b) Dado que centraliza y comparte la información sobre las amenazas, la MISP permite a las organizaciones acceder a la información de inteligencia sobre las amenazas en tiempo real. Esto acelera la detección y la respuesta a incidentes, por lo que mejora la postura de seguridad general.

c) La MISP se puede personalizar y extender en gran medida, lo que permite que las organizaciones la adapten a sus necesidades concretas. Eso incluye la capacidad de agregar atributos a medida, crear modelos de amenazas específicos e integrar la plataforma a otras herramientas de seguridad.

d) La MISP conecta a los usuarios con las comunidades mundiales de ciberseguridad, de modo que habilita el intercambio de información con otras organizaciones y profesionales. Esto amplía la base de conocimientos disponible y fortalece la defensa contra amenazas a gran escala, ya que permite comprender las tácticas, técnicas y procedimientos de quienes organizan ataques cibernéticos.

e) La MISP incorpora funciones avanzadas de privacidad y control de acceso, para que las organizaciones intercambien información de forma selectiva y segura. Esto es fundamental para proteger los datos delicados y cumplir los reglamentos sobre privacidad.

2.2.2 En resumen, la MISP es esencial para gestionar las amenazas cibernéticas, ya que ofrece una plataforma eficaz para el intercambio de información sobre ciberseguridad. Al adoptarla, se mejora la defensa institucional y se fortalece la ciberseguridad a nivel nacional, regional y mundial.

2.3 Uso de la plataforma MISP por el DECEA

2.3.1 El DECEA comenzó a implementar la plataforma MISP en 2021 y, desde entonces, la emplea y perfecciona su uso. Ese perfeccionamiento continuo pone de manifiesto el compromiso del DECEA de mantenerse actualizado ante los problemas de ciberseguridad, que evolucionan constantemente.

2.3.2 La adopción de la MISP permite al DECEA intercambiar información de inteligencia sobre amenazas críticas de manera eficaz con otras partes interesadas brasileñas, como el Centro de Tratamiento de Incidentes de Seguridad en Redes de la Fuerza Aérea Brasileña (CTIR.FAB), la corporación de petróleo brasileña (Petrobras), la Agencia Nacional de Telecomunicaciones (ANATEL) y la Federación Brasileña de Bancos (FEBRABAN). Esta colaboración no solo refuerza los propios mecanismos de defensa del DECEA, sino que contribuye también a la postura mundial de seguridad del Sistema de Control del Espacio Aéreo de Brasil (SISCEAB).

2.3.3 Los indicadores de amenazas y las alertas recibidos de terceros a través de la MISP se procesan y sirven de base para componer listas de bloqueo o para definir reglas de cortafuegos. Estos indicadores aportan información crucial sobre posibles amenazas a la seguridad, lo que permite a las organizaciones proteger de forma proactiva sus redes y sistemas frente a actividades maliciosas, anticipándose a las amenazas emergentes, y reforzar su postura de ciberseguridad.

2.3.4 Las normas asociadas a una amenaza se determinan por su nivel de riesgo a lo largo del tiempo. Este nivel de riesgo para cada amenaza se actualiza continuamente en función de los indicadores recibidos a través de la MISP. El ajuste dinámico del nivel de riesgo para cada amenaza permite a las organizaciones asegurarse de que sus reglas de cortafuegos sigan siendo eficaces y reactivas para que los entornos sean más seguros. Este enfoque permite aplicar estrategias de mitigación de amenazas más adaptables y precisas, lo que mejora la resiliencia general de la ciberseguridad.

2.3.5 A modo de ejemplo, la figura 1 señala los diez tipos de amenazas sobre las que el DECEA ha recibido más notificaciones a través de la MISP en el último año, a saber: el troyano Zeus, el phishing de URL, actualizaciones de IOC relacionadas con Emotet, el troyano Citadel y páginas de phishing.

2.3.6 La figura 2 presenta la cantidad diaria de actividades maliciosas bloqueadas por indicadores recibidos en la plataforma MISP durante una semana. De ese gráfico se desprende que la MISP contribuye al bloqueo de unos 40 000 000 de actividades maliciosas al año.

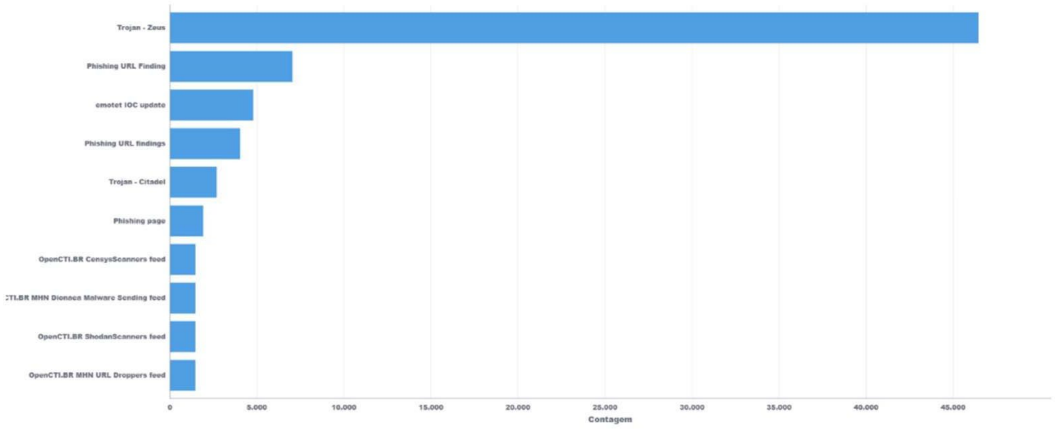

Figura 1 - Los diez tipos principales de amenazas recibidas por el DECEA

Figura 2 - Actividades maliciosas bloqueadas por los indicadores de la MISP

2.3.7 Actualmente, la MISP presta asistencia para la recepción y/o notificación de todo evento malicioso confirmado o presunto relacionado con la seguridad de los sistemas o redes informáticos, con el fin de contribuir a la seguridad de la información en el SISCEAB.

3. CONCLUSIÓN

3.1 En conclusión, el uso de la plataforma MISP por el DECEA fortalece considerablemente la ciberseguridad de la aviación en el Brasil. Este enfoque proactivo se ajusta a normas internacionales como el Plan de Acción de Ciberseguridad (CyAP) de la OACI. El DECEA también apoya a la Agencia Nacional de Aviación Civil (ANAC) del Brasil en el uso de la MISP para perfeccionar el intercambio de información sobre ciberamenazas en la aviación civil brasileña, aprovechando las capacidades de la MISP para el intercambio de datos de inteligencia en tiempo real y la adhesión a normas abiertas.

3.2 El Brasil reafirma su compromiso de contribuir a la seguridad de la aviación internacional, en especial en materia de ciberseguridad. Su enfoque colaborativo mejora la seguridad operacional de la aviación mundial. A medida que la hiperconectividad aumenta la superficie de los sistemas de navegación aérea que puede sufrir un ataque, el Brasil se vuelca en la adopción de las mejores estrategias y tecnologías para proteger sus infraestructuras críticas de aviación de las ciberamenazas en evolución.

3.3 El Brasil pretende incentivar el uso de la MISP entre los miembros de la Región Caribe y Sudamérica (CAR/SAM), para estudiar y participar de manera activa en la iniciativa de intercambio de información sobre ciberamenazas, promoviendo así el uso de la MISP como plataforma sólida de colaboración. Esto apunta a aumentar la ciberresiliencia de la aviación regional para que en el futuro exista una integración a nivel mundial, en consonancia con las recomendaciones de la OACI.

3.4 A la luz de lo anterior, se invita a la Conferencia a convenir en la siguiente recomendación:

Recomendación 4.2/x – Ciberseguridad y resiliencia de los sistemas de información

a) tomar nota de que el uso de la Plataforma de Intercambio de Información sobre Programas Maliciosos (MISP) por el Departamento de Control del Espacio Aéreo (DECEA) en el Brasil para el intercambio de información sobre ciberseguridad ha sido positivo hasta la fecha;

b) animar a los Estados miembros a que adopten la MISP como plataforma de intercambio de información sobre ciberseguridad; y

c) transmitir el asunto de la presente nota al Grupo Experto en Ciberseguridad (CYSECP) y crear un grupo de trabajo que se ocupe de normalizar el intercambio de información sobre ciberseguridad y el posible uso de la plataforma MISP por los Estados miembros.

— FIN —