Organización de Aviación Civil Internacional

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

NOTA DE ESTUDIO

DECIMOTERCERA CONFERENCIA DE NAVEGACIÓN AÉREA

Montreal, Canadá, 9 al 19 de octubre de 2018

COMITÉ A

Cuestión 5 del orden del día: Cuestiones emergentes
5.4: Ciberresiliencia

FORTALECIMIENTO DE CONCEPTOS DE CIBERSEGURIDAD EN LA AVIACIÓN

(Nota presentada por Austria en nombre de la Unión Europea y sus Estados miembros[1], los demás Estados miembros de la Conferencia Europea de Aviación Civil[2]; y por EUROCONTROL)

RESUMEN

En esta nota se presentarán brevemente las razones por las que las organizaciones deberían gestionar sus propios riesgos, productos y servicios de ciberseguridad a través de un Sistema de Gestión de la Seguridad de la Información (ISMS) que tenga en cuenta los riesgos relativos a las interacciones de la organización con las otras organizaciones o sistemas que ellas operan.

La nota se centra también en la confiabilidad, los motivos por lo que esta es necesaria y las ventajas que aporta a las organizaciones el uso de un ISMS. Además, en la nota también se abordarán los motivos por los que un nivel equivalente de performance de ciberseguridad, independientemente del tiempo y la ubicación, de los sistemas conectados es un requisito previo esencial y la manera en que eso se puede lograr en las operaciones tierra/tierra o aire/tierra.

Asimismo, la nota introduce una perspectiva común de carácter crítico para la aviación y las ventajas del intercambio de información.

Medidas propuestas a la Conferencia:
Se invita a la Conferencia a convenir en las recomendaciones contenidas en el párrafo 3.

[1] Alemania, Austria, Bélgica, Bulgaria, Chipre, Croacia, Dinamarca, Eslovaquia, Eslovenia, España, Estonia, Finlandia, Francia, Grecia, Hungría, Irlanda, Italia, Letonia, Lituania, Luxemburgo, Malta, Países Bajos, Polonia, Portugal, Reino Unido, República Checa, Rumania y Suecia.

[2] Albania, Armenia, Azerbaiyán, Bosnia y Herzegovina, Georgia, Islandia, ex República Yugoslava de Macedonia, Mónaco, Montenegro, Noruega, República de Moldova, San Marino, Serbia, Suiza, Turquía y Ucrania.

1. INTRODUCCIÓN

1.1 La disponibilidad de información precisa y el correcto funcionamiento de los sistemas críticos para la seguridad operacional son requisitos previos para la seguridad de la aviación civil a medida que el sector experimenta una mayor digitalización. El sistema de aviación está sumamente integrado y la información recorre el mundo. Por lo tanto, se debe adoptar un enfoque integral de extremo a extremo para las iniciativas de ciberseguridad del sector de la aviación.

1.2 En esta nota se destacan las ventajas de la introducción de Sistemas de Gestión de la Seguridad de la Información (ISMS) en el sector de la aviación. Esos sistemas de gestión, de preferencia armonizados o integrados con los sistemas existentes de gestión de riesgos de la aviación, ayudan tanto a cada organización como al sector en general a estar más preparados y responder mejor a las amenazas a la seguridad de la información.

1.3 Un enfoque común del sistema de gestión permite coordinar medidas en todo el sector, teniendo en cuenta que la información se intercambia, que los mismos sistemas son comunes a numerosos actores del sector y que los riesgos se comparten.

1.4 Además de un enfoque de ISMS, en esta nota también se desarrolla la noción de confianza. En el sector de la aviación, la confianza en cada asociado es fundamental. Un sistema sólido de instrucción, certificación, vigilancia y doble control asegura que, para cada vuelo, todos los asociados tengan confianza en que los demás harán correctamente y a conciencia su parte en la cadena de aviación.

2. ANÁLISIS

2.1 **Cómo aprovechar un ISMS** – Los conceptos existentes de ISMS están limitados intrínsecamente a las organizaciones de manera individual. Sin embargo, la aviación civil es un sistema de sistemas tan estrechamente entrelazados y que comprende productos, personas y procesos interconectados, incluso conexiones con sistemas militares[3], que una perspectiva a nivel de cada organización no resulta suficiente. Así, la aviación civil tendrá que incorporar el ISMS con la noción de la gestión transorganizacional de la ciberseguridad.

2.2 Un enfoque de ISMS coordinado a nivel mundial es, por lo tanto, un factor clave para el sector de la aviación civil. Ese marco mundial facilitaría la implantación coherente de una serie de conceptos de apoyo, como una infraestructura de comunicación segura e interoperable a nivel mundial, y un marco de confianza u otros conceptos que permitan la creación de un sistema futuro basado en el intercambio confiable de información. Como ese futuro no se construirá en un momento, será necesario facilitar la evolución de cada organización, Estado o región. La existencia de un ISMS en todas las organizaciones será un requisito previo para que esos conceptos se hagan realidad. La implantación del ISMS debería alinearse con los sistemas de gestión existentes para la gestión de riesgos de seguridad operacional (por ejemplo, el Anexo 19 — *Gestión de la seguridad operacional*) y seguridad de la aviación, las disposiciones de la OACI y las normas de la industria, así como con mecanismos eficaces de vigilancia.

2.3 **Concepto de confiabilidad** – En la aviación civil, se ha creado un sólido marco de fiabilidad durante décadas. La confiabilidad es ahora un concepto formal por el cual una organización –o un sistema que esta opera– puede depender de las propiedades de ciberseguridad de otra organización –o de un sistema que esa organización opera–[4]. Como la confianza nunca es absoluta, el concepto propone

[3] Véase AN-Conf/13-WP/39

[4] En la nota de información (AN-Conf/13-WP/160) se explicarán los conceptos y principios del ISMS, los conceptos de confiabilidad y condiciones operativas de ciberseguridad y las ventajas de intercambiar información.

niveles múltiples de confiabilidad, que dependerán de las repercusiones (seguridad operacional o continuidad del servicio, por ejemplo, la afluencia rápida de tránsito en una región) que tendrá en la parte dependiente.

2.4 Por ejemplo, en la certificación de aeronaves, la mayor parte de la confianza respecto de la aeronavegabilidad se deriva de la garantía de que se han llevado a cabo las acciones apropiadas y que estas han dado resultados aceptables. Esas acciones se han diseñado para hacer frente a la gravedad de las repercusiones de los riesgos de seguridad operacional. A niveles más altos de gravedad de las repercusiones, se requerirán mayores niveles de análisis durante el proceso de desarrollo. Para las propiedades de ciberseguridad se propone un concepto similar, diseñado para reflejar la efectividad de la protección contra amenazas cibernéticas. Básicamente, la confianza en la ausencia de errores y vulnerabilidades de desarrollo y en que las organizaciones protejan adecuadamente a la aviación civil es lo que allanará el camino para los vuelos seguros en el futuro. Se debería integrar el concepto de confiabilidad en el ISMS, que a su vez debería alinearse o integrarse con los sistemas de gestión existentes.

2.5 **Condiciones operativas de ciberseguridad** – Para aprovechar al máximo el concepto de confiabilidad, también se debe abordar la dinámica de la evolución de cada organización y de los sistemas que estas operan, en relación con la infraestructura segura e interoperable a nivel mundial. Las condiciones operativas de ciberseguridad especificadas previamente son una forma de afrontar el desafío. Por cada conexión entre homólogos, será esencial que los niveles de confiabilidad sean compatibles entre sí, por lo que es preciso definir pares afines. Se permitirá la conexión entre pares con determinados de niveles de confiabilidad, ya que estos cumplirán los objetivos de ciberseguridad con niveles de riesgo aceptables. Es posible que con otras combinaciones no se alcancen los objetivos. De este modo, se crearán incentivos para llegar a acuerdos entre homólogos sobre las condiciones para niveles de confiabilidad compatibles, aunque divergentes, lo que, en última instancia, dará lugar a enfoques equilibrados. Se deben distinguir dos niveles de migración de conexiones entre homólogos: el nivel entre las organizaciones que conectan sus sistemas y el nivel entre los vehículos aéreos o espaciales y los sistemas terrestres, que hacen una transición entre conexiones a un ritmo acelerado. Aquí, el factor discriminador clave es la velocidad a la que evoluciona su condición de ciberseguridad.

2.6 Evolución lenta: Por un lado, los sistemas terrestres en general –y la gestión del tránsito aéreo (ATM) y los servicios de navegación aérea (ANS) en particular– evolucionan a un ritmo comparativamente lento. Los cambios de condiciones de funcionamiento están determinados en gran medida por los cambios en su propia situación respecto de la ciberseguridad o bien por la de los sistemas a los que están conectados. Esto permite adaptar, en estrecha coordinación, las propiedades de ciberseguridad de modo que todas las partes conectadas cumplan los requisitos generales de ciberseguridad. El concepto de condiciones operativas aborda la combinación adecuada de niveles de confiabilidad entre las organizaciones que se conectan.

2.7 Evolución rápida: Por otro lado, las aeronaves migran de un lugar a otro a una velocidad acelerada en comparación y se conectan de forma dinámica con una gran cantidad de homólogos en un breve período. En términos generales, los sistemas de las aeronaves o de los ATM/ANS no estarán en un estado de ciberseguridad coincidente en un día en particular. Para mantenerlos operacionales, se requerirá la migración de ambas partes. Para la ciberseguridad, la adaptación del concepto de condición operativa podría dar una respuesta. Por ejemplo, en el concepto existente de condiciones operativas, los requisitos de separación horizontal aplicables dentro de un espacio aéreo requieren un cierto equipamiento de sistemas de tierra y de a bordo para cumplirlos. Por lo tanto, el concepto de condiciones operativas podría servir como proyecto para la ciberseguridad, respondiendo a los requisitos con respecto a las propiedades de ciberseguridad introducidas por niveles de confiabilidad. Los niveles de confiabilidad correctamente combinados entre los sistemas de los ATM/ANS y de las aeronaves permitirían un uso seguro del espacio aéreo.

2.8 **Intercambio de información sobre aspectos cibernéticos** – Otro aspecto que debe tenerse en cuenta como parte de un ISMS es el intercambio de información. Un marco mundial de ISMS

también podría contribuir a crear un mecanismo más coherente de intercambio de información sobre riesgos de ciberseguridad. El mundo de la tecnología de la información (TI) ha creado el concepto de centro de seguridad cibernética, que "maneja" información sobre incidentes de ciberseguridad y, entre otras cosas, recopila y mantiene bases de datos de incidentes, amenazas y vulnerabilidades y proporciona análisis y orientación sobre prácticas satisfactorias para contrarrestar un incidente real para sus grupos de intereses comunes. Esas tareas están asociadas con el intercambio de información.

2.9 A nivel internacional, los Equipos de intervención de urgencia en cuestiones de seguridad informática (CERT) y los Equipos de respuesta a incidentes de seguridad informática (CSIRT) han creado una comunidad, llamada Foro de Equipos de Seguridad y Respuesta a Incidentes (FIRST). Este foro podría servir a la comunidad aeronáutica como plan de trabajo para un enfoque concertado para el intercambio de información a nivel mundial con el objetivo no solo de reaccionar ante los incidentes, sino también de evitar que prosperen ataques futuros. Respecto del descubrimiento de nuevas vulnerabilidades, la información recopilada por los CSIRT permitirá anticipar, en cierta modo, los riesgos emergentes y así tomar medidas preventivas para limitar los efectos perjudiciales para la aviación civil. En suma, este objetivo procura concientizar sobre las amenazas y vulnerabilidades cibernéticas de los sistemas de aviación. Cuando los CSIRT de la aviación se hayan coordinado entre sí y con sus respectivos miembros, será posible adoptar medidas de mitigación y defensa armonizadas internacionalmente contra las amenazas cibernéticas.

2.10 Existen amenazas a la ciberseguridad fuera de la aviación civil, por ejemplo, en otros sectores del transporte, pero también en sectores que no guardan relación con el transporte (por ejemplo, sistema bancario, industria nuclear). Esos sectores suelen compartir tecnologías y aplicaciones y, por lo tanto, amenazas y vulnerabilidades. Por ello, resulta fundamental compartir políticas, información de inteligencia y mejores prácticas con las organizaciones de esos sectores. Un enfoque de la ciberseguridad en la aviación civil debería aprovechar otros enfoques y experiencias intersectoriales nacionales o regionales. Además, la comunicación estrecha con las entidades gubernamentales dedicadas a la ciberseguridad de otros sectores aumentará los beneficios para las Autoridades de Aviación Civil de los Estados.

3. CONCLUSIÓN

3.1 Se invita a la Conferencia a convenir en las siguientes recomendaciones:

Que la Conferencia:

a) inste a la OACI a respaldar a los Estados para que estos exijan a las organizaciones la gestión de los riesgos de ciberseguridad de sus operaciones, productos y servicios, incluidas las interfaces con sus homólogos, mediante un Sistema de Gestión de la Seguridad de la Información (SGSI), sobre la base de las normas de la industria y, de preferencia, armonizados o integrados con los sistemas de gestión existentes;

b) solicite a la OACI que aliente a los Estados a adoptar las medidas apropiadas para implantar una infraestructura interoperable a nivel mundial que sea resistente a los ciberataques. Esa infraestructura deberá cumplir los requisitos de interoperabilidad y ciberseguridad para reforzar los objetivos integrales y de alto nivel con respecto a la seguridad operacional y la afluencia rápida del tránsito;

c) inste a la OACI a que elabore, con un enfoque multidisciplinario, disposiciones para la confianza interorganizacional, como parte de un marco de confianza más amplio, y promueva su implantación;

d) solicite a la OACI que aliente a los Estados a adoptar medidas para que los explotadores de la aviación establezcan y faciliten el intercambio de información operacional relacionada con la ciberseguridad a través de canales debidamente designados, como una red mundial de "organizaciones de confianza";

e) inste a la OACI a que facilite la elaboración de disposiciones sobre confiabilidad y condiciones operativas de ciberseguridad para permitir el funcionamiento seguro de la infraestructura interoperable a nivel mundial;

f) solicite a la OACI que aliente a los Estados a que amplíen los canales de notificación, o creen nuevos, para comunicar hechos relacionados con la ciberseguridad, a fin de afrontar mejor los nuevos riesgos para la seguridad operacional y de la aviación y garantizar la rápida afluencia de tránsito; y

g) solicite a la OACI que inste a los Estados a promover la colaboración intersectorial gubernamental y no gubernamental en materia de ciberseguridad entre los ámbitos de la aviación y otros ámbitos.

— FIN —