Organización de Aviación Civil Internacional

A40-WP/295
TE/119
1/8/19

NOTA DE ESTUDIO

ASAMBLEA — 40º PERÍODO DE SESIONES

COMISIÓN TÉCNICA

Cuestión 30: Otros asuntos que habrá de considerar la Comisión Técnica

APLICACIÓN DE CONTROLES DE CIBERSEGURIDAD DE LOS ESTADOS A LA AVIACIÓN

(Nota presentada por Nueva Zelandia)

RESUMEN

En la presente nota se analiza la elaboración de los marcos de ciberseguridad de la aviación de la OACI en el contexto de los controles vigentes de ciberseguridad no específicos del sector que utilizan los Estados. Se propone que la OACI centre sus esfuerzos en elaborar principios sólidos y acordados a partir de los cuales los Estados puedan hacer frente a los problemas de ciberseguridad.

Decisión de la Asamblea: Se invita a la Asamblea a:

a) tomar nota de que la implementación de normas de ciberseguridad de la aviación armonizadas a nivel mundial y demasiado prescriptivas puede entrar en conflicto con los marcos nacionales de ciberseguridad de los Estados y limitar la capacidad de estos para cumplir los SARPS de la OACI,
b) alentar a la OACI a que se centre en la elaboración de orientaciones basadas en principios sobre ciberseguridad del sector de la aviación para ayudar a los Estados a integrar la aviación en los marcos nacionales, teniendo en cuenta las normas establecidas en materia de seguridad de la información, como la serie ISO 27000; y
c) alentar a la OACI a que aporte orientaciones sobre el propósito y la aplicación del marco de confianza.

Objetivos estratégicos:	Esta nota de estudio se relaciona con los Objetivos estratégicos: Seguridad de la aviación y facilitación y Seguridad operacional
Repercusiones financieras:	Ninguna
Referencias:	AN-Conf/13-WP/270: Noción de sistema-de-sistemas en la ciberseguridad en aviación (28/09/2018)

1. INTRODUCCIÓN

1.1 Con los avances continuos de la tecnología y los niveles crecientes de complejidad de los sistemas de aviación, la seguridad operacional y de la aviación del sistema de aviación mundial depende cada vez más de controles efectivos de ciberseguridad.

1.2 La necesidad de controles efectivos de ciberseguridad es común en una amplia gama de sectores diferentes y no es, en absoluto, exclusiva de la aviación. Sin una ciberseguridad efectiva, las organizaciones tendrán dificultades para ofrecer productos y servicios digitales y conservar, a su vez, la confianza de sus clientes y partes interesadas.

1.3 Los Estados desempeñan la función de garantizar que organizaciones y sectores de importancia nacional alcancen niveles de ciberseguridad elevados y consistentes. El enfoque que se adopte variará de un Estado a otro en respuesta a las diversas amenazas, capacidades e intereses en materia de seguridad nacional.

1.4 Aunque el tipo de controles de seguridad establecidos por cada organización se ajusta, en general, a sus necesidades y capacidades y a las del sector en el que opera, los intereses de seguridad nacional imponen requisitos generales. El interés nacional de un Estado siempre tendrá prioridad por sobre el de un sector u organización.

1.5 La aviación mundial depende en gran medida de la seguridad en la transmisión digital de información entre los miembros de la comunidad de la aviación, incluso entre los Estados. En el documento AN-Conf/13-WP/270, presentado en la Decimotercera Conferencia de navegación aérea, se planteó un enfoque de "Sistema-de-sistemas" para la ciberseguridad. Este enfoque reconoce que el sistema general de aviación se compone de una serie de subsistemas operados por una variedad de partes interesadas y que esos subsistemas se deben considerar de manera integral para que el ambiente operativo sea seguro.

1.6 Se ha elaborado el Marco de confianza de la OACI para permitir que se entablen vínculos confiables de comunicación entre las partes interesadas. El Marco consta de los siguientes principios:

1.6.1 La interoperabilidad entre todas las partes interesadas se garantiza mediante un marco de confianza y una arquitectura comunes para servicios de mensajería eficientes y sin discontinuidades a nivel mundial.

1.6.2 La resiliencia de las comunicaciones se maximiza mediante conceptos de diseño que limitan la superficie de amenaza. Esto incluye la compartimentación de la red y las aplicaciones, así como la creación de diversas capas de protección en la infraestructura y la limitación de la cantidad de sistemas que participan.

1.6.3 Identificación, autenticación, autorización, integridad y confidencialidad sólidas.

1.7 Aunque el concepto del marco de confianza es importante, no están del todo claros su propósito y posible aplicación. Para seguir elaborando el marco será necesario examinar minuciosamente los intereses de seguridad nacional de los Estados de modo de garantizar que la función de dicho marco esté definida con claridad.

2. ANÁLISIS

2.1 Los intereses nacionales de un Estado imponen restricciones en el carácter de los marcos de ciberseguridad que puede implementar cada sector y organización. Cuando existan normas y requisitos reglamentarios de un Estado para la seguridad de la información, estos prevalecerán por sobre las normas específicas de sectores y organizaciones.

2.2 Así, es probable que la capacidad de un Estado para cumplir los SARPS prescriptivos de la OACI sobre ciberseguridad de la aviación se vea limitada por sus propios marcos de seguridad nacional. Esta limitación variará considerablemente de un Estado a otro y según la medida en que los propios SARPS sean prescriptivos.

2.3 De manera similar, es poco probable que un enfoque muy prescriptivo y normalizado reglamente de modo efectivo un ámbito en el que la tecnología y el entorno de amenazas evolucionan con rapidez. Es posible que unos requisitos mundiales demasiado prescriptivos obstaculicen la capacidad de un Estado para responder al cambio y que no sean apropiados en la misma medida para diferentes tipos de operaciones.

2.4 A pesar de las diferentes necesidades de ciberseguridad de cada Estado y los problemas de imponer requisitos internacionales muy prescriptivos, se necesita un conjunto de principios coherentes y acordados para regir la transferencia segura de información entre las partes interesadas.

2.5 Para apoyar la aplicación de estos principios, la elaboración de los textos de orientación de la OACI debería centrarse en ayudar a los Estados a apoyar la ciberseguridad de la aviación como parte integral de los marcos nacionales. A tal efecto, es probable que un enfoque basado en la performance o en los principios resulte ser el más efectivo.

2.6 Al adoptar un enfoque basado en principios, cada Estado podría adaptar la orientación de la OACI de una manera que permita implementar un marco de confianza mundial armonizado con los requisitos nacionales. Las normas de seguridad de la información existentes basadas en principios, como la serie ISO 27000, sirven de base para dicha orientación. Idealmente, se tratarían cuatro esferas principales:

2.6.1 **Gobernanza:** promover la ciberseguridad a nivel de los funcionarios de categoría superior para proteger los activos digitales más importantes de una organización. Las juntas y los ejecutivos son responsables en última instancia de los resultados de todo incidente cibernético, incluidas las repercusiones en la confianza de las partes interesadas y los clientes.

2.6.2 **Inversión:** invertir en ciberseguridad para minimizar el riesgo y maximizar la rentabilidad. El acuerdo a nivel de la gobernanza sobre la avidez por el riesgo de la organización y la identificación de activos clave son los primeros pasos fundamentales para garantizar que la inversión esté dirigida y equilibrada de modo adecuado.

2.6.3 **Preparación:** preparar a la organización para detectar un incidente de ciberseguridad, responder a él y recuperarse. La cuestión es cuándo una organización experimentará un incidente de ciberseguridad y no si hay posibilidad de que este ocurra. La preparación para un incidente permite a las organizaciones reducir el riesgo general de ciberseguridad gracias a una recuperación rápida y efectiva.

2.6.4 **Cadena de suministro:** mantener la vigilancia y conciencia de los riesgos de ciberseguridad de la cadena de suministro de una organización. Esta esfera reviste particular importancia en el sector de la aviación, ya que suelen intervenir extensas cadenas de suministro en la provisión de equipos y servicios. Esto incluye el componente técnico del diseño de sistemas y el aspecto de factor humano del diseño de procesos.

2.7 Unas orientaciones bien formuladas basadas en la performance y en normas de seguridad de la información establecidas serían beneficiosas para las organizaciones del sector de la aviación y

promoverían un enfoque coherente que abarque los elementos esenciales de los controles efectivos de ciberseguridad.

2.8 La elaboración de dichas orientaciones también debería considerar los ámbitos que requieren ciertos controles mínimos y la manera en que estos deben abordarse teniendo en cuenta los marcos aplicados por los distintos Estados.

2.9 La elaboración del marco de confianza de la OACI brinda la oportunidad de establecer protocolos para el intercambio de información entre partes interesadas, pero es preciso aclarar mejor su propósito y aplicación.

2.10 Se debe considerar la elaboración del marco de confianza junto con los marcos de ciberseguridad implementados por las partes interesadas. Para que la seguridad del intercambio de datos sea elevada, también debe serlo la seguridad de la fuente de los datos, y eso depende de que los Estados y organizaciones adopten controles efectivos.

— FIN —