Organización de Aviación Civil Internacional

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

NOTA DE ESTUDIO

ASAMBLEA — 41º PERÍODO DE SESIONES

COMITÉ EJECUTIVO

Cuestión 14: Seguridad de la aviación — Política

LA SEGURIDAD DE LA AVIACIÓN A TRAVÉS DEL ENFOQUE DE CONFIANZA CERO

(Presentada por Sudáfrica)

RESUMEN

El sector de la aviación depende en ocasiones de largas cadenas de suministro que atraviesan distintos sectores, acrecentando las amenazas para la aviación. El uso de sistemas que funcionan a partir del protocolo de internet (IP) para una mayor eficiencia exige una actitud proactiva para dar protección a los sistemas actuales y los convencionales.

El Plan de Acción de Ciberseguridad de la OACI destaca la necesidad de concentrar los recursos y la acción en sistematizar la gestión de la ciberseguridad en la aviación en aras de un enfoque sistémico que permita a la aviación adaptarse a tiempo y resistir las nuevas amenazas.

Esta nota de estudio plantea el concepto de confianza cero, que los Estados y demás participantes de la aviación podrían adoptar como principio de mitigación. El concepto puede reforzar los medios actuales de protección de la ciberseguridad con protección de punta a punta. Se aparta de la seguridad perimetral tradicional, favoreciendo en su lugar el despliegue de recursos de seguridad en el límite o más cerca de las instalaciones de control de tránsito del usuario final y de los datos de ayuda para la navegación en sitios remotos (radar de alimentación).

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

a) reconocer el beneficio de aplicar enfoques ágiles de evaluación continua y adaptativa del riesgo y de la confianza (CARTA) para proteger las operaciones de la aviación;
b) solicitar a la OACI que a través del Grupo Experto en Ciberseguridad elabore orientación técnica para ayudar a los Estados en la incorporación del marco de confianza cero en los sistemas de gestión de la seguridad de la información; y
c) instar a los Estados a considerar la incorporación de los principios de confianza cero en sus sistemas de gestión de la seguridad de la información.

Objetivos estratégicos:	Esta nota de estudio se relaciona con el objetivo estratégico de *Seguridad de la aviación y facilitación*
Repercusiones financieras:	No tiene repercusiones presupuestarias adicionales, ya que se llevará a cabo con recursos del presupuesto de la OACI.
Referencias:	*Plan de Acción de Ciberseguridad* *Manual de seguridad de la aviación* de la OACI (Doc 8973)

1. INTRODUCCIÓN

1.1 En los últimos años, el sector de la aviación ha experimentado una transformación impulsada por la adopción de tecnología, derivando en un aumento de los riesgos informáticos que requiere atención. Se ha dado un salto gigantesco sin precedentes en el avance tecnológico que exige la adopción de enfoques y modelos de evaluación continua y adaptativa del riesgo y de la confianza (CARTA).

1.2 Anteriormente, el sector de la aviación era considerado en forma aislada. Pero la interdependencia y la convergencia de la tecnología de la información y la tecnología operacional en el ecosistema de la aviación ha hecho que ingresen otros participantes que no se rigen por los mecanismos normativos de la aviación. Como resultado, se han abierto más flancos a los ciberataques y se impone la necesidad de reexaminar algunos conceptos tradicionales.

1.3 En el pasado, la gestión y el mantenimiento de los equipos y programas informáticos de la aviación se podía realizar a través de una red privada virtual (VPN) de acceso remoto seguro y de confianza, lo que en la actualidad pone en peligro la seguridad de los sistemas.

1.4 Ciberamenazas tales como los programas de chantaje (“ransomware”), el robo de datos y los ataques de ciberestafa (“phishing”) se han vuelto frecuentes en la industria de la aviación, afectando todos los servicios informáticos (acceso a módulos de gestión interna, colaboración, correo electrónico) y operativos (sistemas de control y adquisición de datos, controlador programable) en las áreas de control de los aeropuertos y los centros de procesamiento de datos.

2. ANÁLISIS

2.1 Al ampliarse la cadena de suministro de la aviación, se abre una puerta de acceso para las ciberamenazas que pone más de manifiesto la necesidad de soluciones nuevas e innovadoras que les hagan frente. Esto se debe a que la aviación depende de múltiples partes interesadas que tienen diferentes sistemas, aplicaciones y tecnología que deben integrarse entre sí.

2.2 También es clave señalar que el funcionamiento de estas operaciones puede depender de recursos ubicados tanto dentro como fuera de las fronteras de un Estado, lo que expone aún más la cadena de valor del transporte aéreo a las ciberamenazas.

2.3 Los métodos tradicionales de seguridad perimetral de redes han demostrado ser ineficaces, como queda claro ante el aumento de los incidentes de ciberseguridad en la aviación. Una vez vulnerado el perímetro, ya no hay obstáculos para el movimiento lateral del agente de ataque.

2.4 Conceptos como el de confianza cero ofrecen la posibilidad de hacer frente a las amenazas avanzadas y de nueva generación que se presentan en la actualidad, permitiendo que con cada pedido de recursos se active el proceso de evaluación, validación y autorización de acceso siguiendo procesos de control razonados y eficaces.

2.5 El concepto de confianza cero tiene principios rectores que rigen la organización de las tareas, el diseño de los sistemas y las operaciones, y que pueden servir para reforzar la seguridad de las actividades críticas y sensibles para evitar intrusiones en los datos y limitar los movimientos laterales internos.

2.6 El concepto de confianza cero postula que no se puede confiar en nadie, ni dentro ni fuera de la organización. El objetivo es minimizar los frentes de ataque aplicando las siguientes ideas clave:

a) el perímetro no existe. Se elimina la presunción de que se debe confiar en las personas porque han entrado en la red de una empresa;

b) verificar a la persona usuaria antes de conceder el acceso y verificar la integridad de los dispositivos antes de conectarse a la red;

c) erradicar la presunción de que las personas usuarias harán las cosas bien. En su lugar, verificar la autorización de acceso en cada solicitud de servicio; y

d) en lugar de perseguir malhechores, colocar obstáculos para desacelerar el avance.

2.7 El concepto puede reforzar los medios actuales de protección de la ciberseguridad con protección de punta a punta. Se aparta de la seguridad perimetral tradicional, favoreciendo en su lugar el despliegue de recursos de seguridad en el límite o más cerca de las instalaciones de control de tránsito del usuario final y de los datos de ayuda para la navegación en sitios remotos (radar de alimentación).

2.8 El concepto de confianza cero recurre a diferentes tecnologías subyacentes que ofrecen protección en varios frentes:

a) microsegmentación: las primeras manifestaciones del concepto de confianza cero, que está diseñado primordialmente para proteger contra el movimiento lateral para minimizar los daños en caso de vulneración. El movimiento lateral para capturar información de activos clave del centro de procesamiento de datos es un componente central de diversos ataques. El objetivo del concepto de confianza cero es limitar la comunicación no autorizada entre procesos si no tienen ninguna razón operativa para hacerlo, minimizando el impacto de la vulneración. A diferencia de la típica protección norte-sur que ofrecen los cortafuegos, la microsegmentación contempla la seguridad este-oeste de los procesos;

b) en el concepto de confianza cero, el acceso a la red crea un límite lógico basado en el contexto para el acceso a las aplicaciones. El objetivo es minimizar el acceso y el abuso generado por conceder acceso a las aplicaciones porque se trata de personas usuarias y dispositivos conocidos. Se cuestiona la presunción de confiabilidad por la mera ubicación de una entidad (por ejemplo, por estar dentro de una red);

c) oculta todas las aplicaciones en la red y permite el acceso en función de atributos como la identidad de la persona usuaria, el dispositivo, la geolocalización y las garantías de seguridad. Esto significa que las personas usuarias tienen acceso a las aplicaciones que necesitan, pero no ven nada más en la red; y

d) el aislamiento de navegadores remotos se basa en el principio de que los usuarios finales representan los eslabones más débiles de cualquier organización y el acceso a Internet es uno de los mayores frentes de ingreso de los ataques. Por lo tanto, una de las formas más eficaces de minimizar la vulnerabilidad en el punto final/usuario final es aislar el acceso a la web para prevenir amenazas como los programas de chantaje, los programas malignos y las ciberestafas.

3. CONCLUSIÓN

3.1 Los principios de la confianza cero pueden servir para que la aviación civil se refuerce a sí misma adoptando un enfoque de "seguridad integrada". Garantizar la seguridad de los elementos y procesos críticos "desde el diseño" quiebra el paradigma de la seguridad reactiva en favor de la proactividad, y fomenta el desarrollo de un sistema de aviación civil que se refuerza a sí mismo, lo que le permite evolucionar y genera resiliencia de forma más automatizada, si se demuestra su eficacia.

— FIN —