SEGURILATAM

REVISTA DE SEGURIDAD INTEGRAL Nº 5 SEGUNDO CUATRIMESTRE 2017

ESPECIAL SEGURIDAD AEROPORTUARIA

EVENTOS: SEGURILATAM, PROTAGONISTA

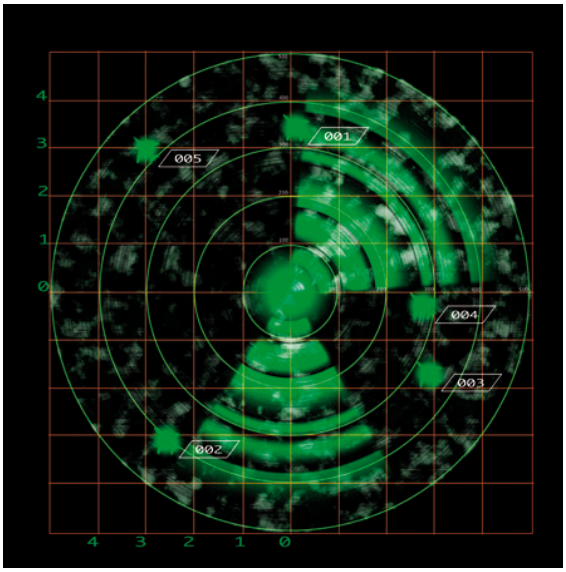
Breve análisis de la vulnerabilidad de los sistemas informáticos aéreos

José Alejandro Calle Cuervo
Líder del Equipo Consultor en Seguridad Aeronáutica de COLADCA*

Los incidentes generados por ataques de fuerza bruta a los sistemas de operación aérea y aeroportuaria han sido de bajo nivel, además de limitados. Y los avances tecnológicos en el diseño de las aeronaves y sus sistemas de navegación se han revelado fundamentales para reducir las probabilidades de materialización de riesgos que produzcan un accidente, bien sea por error humano, bien por manipulación externa de su sistema de operación.

Hoy por hoy, la alta dependencia de las computadoras abre la posibilidad de que estos sistemas de información sufran una irrupción por parte de *hackers* y/o piratas informáticos con fines terroristas o simplemente para causar congestión en las terminales aéreas y generar malestar en los viajeros. Por lo anterior, las empresas de la comunidad aérea deben generar estrategias con el fin de anticipar estos eventos. Al respecto, una herramienta útil es la correcta gestión del riesgo en sus departamentos de Seguridad.

Recordemos que la aviación es un conjunto que, a su vez, se divide en dos elementos diferenciales: tierra y aire. Por un lado, los sistemas de información en tierra, el control del tráfico aéreo y la seguridad aeroportuaria nos garantizan que las operaciones en tierra sean seguras. Y por otro, los sistemas de navegación y operación en vuelo permiten que una aeronave cumpla un plan de desplazamiento desde un origen hasta un destino, de acuerdo a una ruta y puntos de control establecidos, sin ningún contratiempo. Por ello, la tecnología ha sido fundamental en la seguridad aérea; en este sentido, podemos afirmar que se contabilizan menos de dos fallecidos por cada 100 millones de pasajeros.



Pero, aunque sea así, no hemos magnificado el problema. La integración de los sistemas de información facilita que los ciberataques tengan mayor probabilidad de éxito. La decisión humana cada vez es más reducida en los procedimientos aéreos, especialmente cuando se vuela en modo automático (*fly-by-wire*). Obsérvese que el 57 por ciento de los accidentes aéreos ocurre durante la fase de aterrizaje, mientras el 24 por ciento sucede en las etapas de despegue y ascenso, donde el factor humano es preponderante en el procedimiento, y el 9 por ciento tiene lugar en el periodo de crucero –normalmente, en *fly-by-wire*–. Ahí se encuentra el riesgo real de un ciberataque, justo en la interfaz electrónica de los equipos de aviación.

Fragilidad

Hasta ahora, los ataques documentados dan cuenta de intrusiones en los sistemas de registro de pasajeros. Un ejemplo es el protagonizado por la aerolínea polaca LOT en el aeropuerto de Varsovia en 2015. Entonces, 1.400 viajeros sufrieron demoras en sus desplazamientos a diferentes destinos de Europa y se cancelaron 10 vuelos internacionales.

También ese mismo año, según la Agencia Europea de Seguridad Aérea (EASA, por sus siglas en inglés), los sistemas aéreos fueron *hackeados* mil veces al mes de media. Y *Sputnik* publicó que un experto en informática logró acce-

> La gestión del espacio y el tráfico aéreos a nivel mundial es una cuestión que se debe armonizar con los sistemas de información aeronáutica para crear una arquitectura global de redes

der al sistema de mando de una aeronave, haciéndola volar de lado al manipular uno de sus motores.

Estos ejemplos evidencian la fragilidad a la que están expuestas las seguridades aéreas y aeroportuarias. Y la oferta de comodidades a los pasajeros también tiene su nivel de riesgo: estaciones de trabajo y entretenimiento a bordo con conectividad IP pueden afectar a la electrónica del avión y facilitar que se acaben franqueando y vulnerando los *firewalls* que protegen el sistema.

Identificar y anticiparse

Es importante identificar los elementos más críticos del sistema de aviación, aquellos que puedan ser aprovechados por ciberdelincuentes y ciberterroristas para realizar ataques. Me refiero a las aeronaves, los sistemas de navegación, vigilancia e información, los enlaces de datos, los aeropuertos, etc.

Si bien hoy en día se producen menos accidentes que en el siglo pasado, no es menos cierto que existen nuevos tipos de riesgos generados por los peligros y las amenazas actuales. Hablamos de la atención a la cadena de suministros, la interrupción de la actividad, la violación de datos, el terrorismo, el cibercrimen… Estos desafíos obligan a las autoridades aeronáuticas a fortalecer las normas y los métodos en materia de seguridad. Y también a que las líneas aéreas, los gestores de aeropuertos, los fabricantes, los servicios de seguridad, los proveedores y todos aquellos que intervienen en la actividad aeronáutica tomen medidas que contribuyan a minimizar los riesgos y anticiparse a hechos futuros.

Nuevas medidas

Ante este panorama, algunas empresas y organizaciones han apostado por la innovación. Un ejemplo es el fabricante europeo Airbus, que ha desarrollado el denominado Keelback NET. Este sistema lleva a cabo una vigilancia continua de las redes, investiga el *malware* y genera alarmas inmediatas en casos de intrusión. Y la compañía también cuenta con productos cuyo objetivo es proteger las redes de clientes, las estaciones de trabajo y los datos empresariales.

Por su parte, EASA ha creado unos espacios de intercambio de información proactivo y colaboración voluntaria con estrategias de desarrollo de sitios web públicos, servicios de inteligencia de código abierto para sus miembros y una plataforma para que estos últimos compartan información sectorial de ciberseguridad.

La gestión del espacio y el tráfico aéreos a nivel mundial es una cuestión que se debe armonizar con los sistemas de información aeronáutica para crear una arquitectura global de redes. De esta manera, las regiones de información en vuelo se coordinarán correctamente y se tornarán anticipativas. Para completar el monitoreo y conocer en tiempo real lo que sucede con las aeronaves que surcan los cielos, el sistema mundial de socorro y seguridad aeronáuticos (GADDS, por sus siglas en inglés) permitirá conocer la ubicación de una aeronave cada 15 minutos a partir de 2018 y cada minuto desde 2021.

Y el año pasado, durante la 39ª asamblea de la Organización de la Aviación Civil Internacional (OACI), se acordó firmar un plan de acción para reforzar la ciberseguridad en la aviación civil y conformar un grupo de expertos que preste asistencia y asesoramiento para la dirección y coordinación en materia de ciberseguridad, ciberintegridad y ciberresiliencia.

Alerta temprana

La probabilidad de que los sistemas informáticos aéreos se vean perjudicados es posible, ya que las aeronaves son susceptibles de ser infectadas con *malware* o afectadas con fugas de información. Con el levantamiento del mapa o el listado de riesgos futuros determinaremos los puntos críticos de tolerancia y tendremos la facilidad de elaborar un sistema de alerta temprana que nos permita contar con indicadores para diseñar y evaluar escenarios exploratorios y críticos de los peligros citados. Con ello se generarán estrategias que nos faciliten contrarrestar las amenazas de los ciberterroristas, los *hackers* y las bandas organizadas. Pero conviene advertir que estas acciones son responsabilidad de toda la comunidad aérea.

**Con sede en Bogotá (Colombia), COLADCA es la Comunidad Latinoamericana de Consultores y Asesores en Gestión de Riesgos y Seguridad.* ■