Organización de Aviación Civil Internacional
Comisión Latinoamericana de Aviación Civil
Grupo Regional sobre Seguridad de la Aviación y Facilitación NAM/CAR/SAM OACI/CLAC (AVSEC/FAL/RG)

NOTA DE ESTUDIO

AVSEC/FAL/RG/5 — NE/ 23
28/05/15

QUINTA REUNIÓN DEL GRUPO REGIONAL SOBRE SEGURIDAD DE LA AVIACIÓN Y FACILITACIÓN (AVSEC/FAL/RG/5)

Oficina Regional SAM de la OACI, Lima, Perú, del 3 al 5 de junio de 2015

Cuestión 9 del Orden del Día: **Otros asuntos**

CIBERSEGURIDAD: ENFRENTANDO LOS DESAFÍOS DE UN PERFIL TERRORISTA SIEMPRE CAMBIANTE

(Presentada por Jamaica)

RESUMEN EJECUTIVO

Esta nota de estudio presenta información sobre los recientes ciberataques perpetrados contra entidades no relacionadas con la aviación a nivel mundial y la experiencia de Jamaica sobre esta nueva amenaza, y llama a tomar atención para que no se presuma que la industria de la aviación es inmune a este respecto.

Acción:	La acción sugerida se presenta en la Sección 5.
Objetivos Estratégicos:	• Seguridad de la aviación y facilitación
Referencias:	• "*Tendencias de Ciberseguridad en América Latina y el Caribe*", Informe de la Organización de los Estados Americanos 2014 • "*Uniendo a la aviación* ", Comunicado de Prensa de la OACI 2014 • "*Estrategia para la Ciberseguridad Nacional*", Gobierno de Jamaica 2015 • "*Amenazas Emergentes de Ciberseguridad en los Desafíos y Mitigaciones de la Aviación*", Revista de la Gestión de la Aviación 2014

1. Introducción

1.1 La cambiante naturaleza de la amenaza a la aviación civil se ha tornado cada vez más evidente en tanto el mundo se sumerge profundamente en la era tecnológica. La gran sofisticación con la que se realizan ataques calculados en nuestra industria, justifica un nuevo paradigma en el modo en el que abordamos estos nuevos desafíos. Una preocupación creciente para las regiones de Norteamérica, Caribe, Centroamérica y Sudamérica (NAM/CAR y SAM) es la amenaza del ciber-terrorismo y otros crímenes relacionados, y nuestra capacidad para prevenir y responder adecuadamente a incidentes críticos de esta naturaleza. Entidades que buscan hacer daño al transporte aéreo se encuentran, aparentemente, más dispuestas a atacar a la industria en la arena cibernética, cuyo impacto en el mundo real es tan potencialmente devastador como un ataque físico.

1.2 Aunque muchos de los ataques cibernéticos recientes han sido perpetrados contra entidades no relacionadas con la aviación, no se debería asumir que la industria de la aviación es inmune en este respecto. En 2013, el sistema de control de pasaportes en la terminal de salidas del Aeropuerto Internacional de Estambul y en el Aeropuerto Sabiha Gokcen en Turquía fueron víctimas de ataques cibernéticos que derivaron en una variedad de problemas en esos aeropuertos. Asimismo, en 2014, Japan Airlines reportó que el ataque de un virus en la terminal de computadoras dentro de su red resultó en la filtración de información relacionada con aproximadamente 750,000 pasajeros frecuentes.

1.3 Los desafíos a la ciberseguridad han sido reconocidos por la OACI, siendo propuesto como un documento de trabajo en la Conferencia de Alto Nivel de la OACI de 2012 para mayor discusión en la 12° Conferencia de Aeronavegación de la OACI. Esto resultó en la conformación de un grupo de tarea sobre ciberseguridad para evaluar el alcance del problema. En su 25° encuentro, el Panel AVSEC de la OACI deliberó sobre algunos asuntos relacionados con la ciberseguridad.

1.4 La necesidad de que todos los Estados miembros y agencias internacionales trabajen en conjunto fue enfatizada en diciembre de 2014. La OACI, junto con cuatro organizaciones internacionales, llegó a un acuerdo para alinear sus respectivas acciones en asuntos de amenazas cibernéticas. El objetivo común del acuerdo suscrito por las cinco mayores organizaciones internacionales de aviación, como fuera expuesto por el Secretario General de la OACI fue *"trabajar más eficientemente y en conjunto para establecer y promover una robusta cultura de la ciberseguridad y una estrategia para el beneficio de todos los actores en nuestra industria"*. El acuerdo convoca a los signatarios *"…a ser más proactivos a la hora de compartir información crítica como la identificación de la amenaza, la evaluación de los riesgos y las buenas prácticas en ciberseguridad"*, y alienta una *"…coordinación más sustancial a nivel de los Estados entre sus gobiernos y los intereses de la industria en todas las estrategias, políticas y planes para la ciberseguridad."*

1.5 Los principios fundamentales del acuerdo precedente han sido encarnados en las acciones requeridas en este documento de trabajo. Estas acciones son vistas como necesarias por los Estados dentro de esta región para superar sus desafíos peculiares en términos de costo y experiencia, a fin de enfrentar esta amenaza de ciberseguridad.

2. Panorama general de la ciberseguridad en la Región NAR/CAR y SAM

2.1 En 2013 la Organización de los Estados Americanos (OEA), junto con otros colaboradores, investigó el estado de la ciberseguridad y otros desarrollos relacionados con el Cibercrimen en la Región NARCAR/SAM. La investigación evaluó lo que denominó como las principales tendencias en la región en términos de amenazas cibernéticas que enfrenta un amplio espectro de usuarios de la tecnología. Los resultados fueron instructivos ya que nos proporcionó una fotografía de las vulnerabilidades y desafíos que enfrenta la región en la salvaguarda de nuestra infraestructura, dependiente de manera crítica de la tecnología.

2.2 El informe de la OEA sobre las tendencias de seguridad cibernética en la región puso en relieve aumentos significativos en los delitos cibernéticos y los incidentes relacionados. Estos incidentes incluyen el phishing, fraude financiero perpetrado a través del uso de las redes sociales, la difamación y el acoso cibernético. El incremento de los delitos cibernéticos se ven agravados por el hecho de que la información y la tecnología de la comunicación, para incluir el uso de Internet, facilita otras actividades criminales no relacionadas a lo cibernético, tales como el tráfico de armas y drogas.

2.3 El informe también destaca un gran reto para los responsables de diseñar políticas en el ámbito de la recopilación de datos: comunicar cierta toma de decisiones relacionada con la seguridad cibernética ya que, por una variedad de razones, hay un grueso sub registro de los ciber-ataques por parte de las organizaciones.

2.4 Aunque el informe encontró que las proyecciones para las actividades gubernamentales que persiguen atender necesidades de ciberseguridad son positivas, también reconoció que se necesita trabajar más en este sentido y que otros actores, en particular los usuarios de sistemas de tecnología del sector privado, deben adquirir una mayor participación.

3. Estudio de Caso: Jamaica

3.1 En noviembre de 2014 más de 10 sitios web del gobierno de Jamaica fueron víctimas de un ataque cibernético cuando una debilidad en un sitio web que se encontraba alojado en una plataforma común fue penetrado por un grupo de atacantes cibernéticos. Se sabía que la plataforma de programación era vulnerable y un “parche” para corregirlo había sido generado; sin embargo, el servidor no se había actualizado en el momento del ataque.

3.2 La página web de la Autoridad de Aviación Civil de Jamaica fue uno de los sitios web gubernamentales que cayó víctima de una "negación de servicio" (DOS). Las investigaciones están actualmente en curso y buscan determinar a los perpetradores. El Gobierno de Jamaica, Comunicaciones, la Unidad Forense de Delitos Cibernéticos (UCFC), junto con los asistentes técnicos de la OEA están trabajando en conjunto. La asistencia de la Unión Internacional de Telecomunicaciones también ha proporcionado experiencia técnica en la implementación del Equipo de Respuesta a Incidentes Cibernéticos (CIRT).

3.3 El cibercrimen se está volviendo una tendencia en Jamaica. En 2012 se actualizó la legislación sobre la delincuencia cibernética, y en 2015 la *Estrategia Nacional de Seguridad Cibernética* fue publicada como punta de lanza encabezada por un grupo de trabajo conformado por varias agencias a nivel nacional.

3.4 La ciberseguridad es un tema nuevo para los grupos de interés de la seguridad de la aviación en Jamaica. En febrero de 2015, como parte de una iniciativa entre Jamaica y la OEA, con la asistencia técnica del Gobierno de Israel y de Gobierno de Estados Unidos, el tema fue presentado como parte de un curso de tres días sobre amenazas internas. La información tratada en las dos horas que duró la presentación, aportó la noción de que se necesita una mayor conciencia de la amenaza cibernética y del uso de las evaluaciones de riesgos a los fines de comenzar a dar la pelea contra la próxima generación de amenazas a la aviación civil.

4. Conclusión

4.1 Para que los Estados de la Región aborden adecuada y eficientemente los sofisticados desafíos planteados por las amenazas cibernéticas a sus sistemas de aviación, se recomienda adoptar las siguientes medidas con el objetivo común de lograr conformidad en el acuerdo de las cinco organizaciones internacionales, Consejo Internacional de Aeropuertos (ACI), la Organización de servicios de navegación aérea civil (CANSO), la Asociación Internacional de Transporte Aéreo (IATA) , Consejo Coordinador Internacional de Asociaciones de Industrias Aeroespaciales (ICCAIA) y la Organización de Aviación Civil Internacional (OACI).

5. Acciones sugeridas

5.1 Los Estados dentro de la región deben adoptar medidas adecuadas y efectivas para abordar los sofisticados retos de las amenazas cibernéticas a sus sistemas de aviación civil, y considerar la adopción de las siguientes acciones proactivas:

a) desarrollar cursos de formación de conciencia frente a la necesidad particular de generar conciencia en seguridad cibernética;
b) a través de la red AVSEC PoC, compartir información de seguridad cibernética en toda la región; e
c) inclusión de preocupaciones de los Estados sobre la ciberseguridad en el proceso de evaluación de riesgos en la seguridad de la aviación.

— FIN —