El uso de redes sociales por profesionales de la aviación, riesgos y amenazas

Pablo López. *Centro Nacional de Inteligencia-Centro Criptológico Nacional*

Un uso no siempre responsable de las redes sociales por parte de algunos profesionales de la aviación, la revelación de información sensible, la ingeniería social, el robo de identidad, el perjuicio reputacional para el piloto o su aerolínea o la distribución de malware son solo alguno de los peligros que se ciernen por parte de unos usuarios que, no nos olvidemos, están dentro de un sector considerado estratégico en nuestro país.

Una sociedad moderna está integrada por una serie de infraestructuras críticas que permiten el desarrollo de sectores como el del agua, energía, financiero, salud, TIC o transporte y que, por tanto, posibilitan el correcto funcionamiento de la misma.

El sector aéreo en cuanto a transporte está catalogado como sector estratégico en España y, además, es uno de los servicios esenciales que vertebran nuestro país y que posibilita el mantenimiento de las funciones sociales básicas, como la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas.

Los numerosos servicios en los que se basa o que facilita, en sectores tan relevantes como seguridad y defensa, meteorología, energía, telecomunicaciones, economía, transporte, marítimo, aviación, ingeniería, desarrollo urbano, ocio, turismo, etc., hacen de este un bien de valor incalculable.

La tecnología aérea como infraestructura crítica española

Para que el sector aeroespacial pueda funcionar correctamente, cuenta con un gran componente tecnológico de avanzados sistemas de información y telecomunicaciones que se distribuyen globalmente y dan servicio a un complejo entramado de centros de seguimiento y control, radares, comunicaciones digitales de voz y datos, aeronaves, así como instalaciones aeroportuarias.

> Es de vital importancia que los pilotos y los profesionales de la aviación adopten una serie de medidas y buenas prácticas, de modo que no pongan en riesgo su seguridad y la de los pasajeros, su carrera profesional o la imagen de la aerolínea.

Todo este conglomerado de tecnologías, redes y equipos supone una de las infraestructuras críticas más indispensables de nuestro país, pues sobre él descansa el funcionamiento del transporte aéreo y, por tanto, de la sociedad moderna española en su conjunto.

Sin embargo, el cada vez mayor uso de la tecnología aeroespacial, así como el altísimo nivel de interconectividad entre los diversos sistemas y equipos que la conforman, implica una importante vulnerabilidad ante un desafío cuyo auge es cada vez mayor: las ciberamenazas, los ciberataques y el cibercrimen.

España es uno de los países más interconectados del mundo. Un vistazo a las noticias diarias nos informa de la enorme cantidad y peligrosidad de las amenazas cibernéticas a las que nos enfrentamos. La generalización del uso de los medios electrónicos en el normal desenvolvimiento de la sociedad ha incrementado la superficie de exposición a ciberincidentes y ataques y, en consecuencia, los beneficios potenciales derivados.

De hecho, en el noveno informe de riesgos publicado por la aseguradora Allianz, vemos que los ciberincidentes son, por primera vez, el principal peligro al que están expuestas las empresas, tanto a nivel global como en España. Además, este documento incluye un anexo en el que se diferencian los principales riesgos en función del sector, siendo las amenazas del ciberespacio el más dañino para la aviación. Y ello es confirmado por los propios profesionales que operan para el transporte aéreo.

Los ciberatacantes pueden aprovecharse de la enorme superficie de exposición de este sector para llevar a cabo diversas acciones malintencionadas con un enorme potencial disruptivo, como la modificación no autorizada de la información contenida en las bases de datos de los clientes, la filtración de información sensible, la alteración del mercado del tráfico aéreo o los ataques contra los sistemas de las aeronaves, los sistemas de control de tierra, las ayudas a la navegación o los sistemas de coordinación de tráfico aéreo nacional.

Las consecuencias de una posible alteración en cualquiera de estos casos serían, sin duda alguna, catastróficas y con serias implicaciones en el normal desenvolvimiento económico y

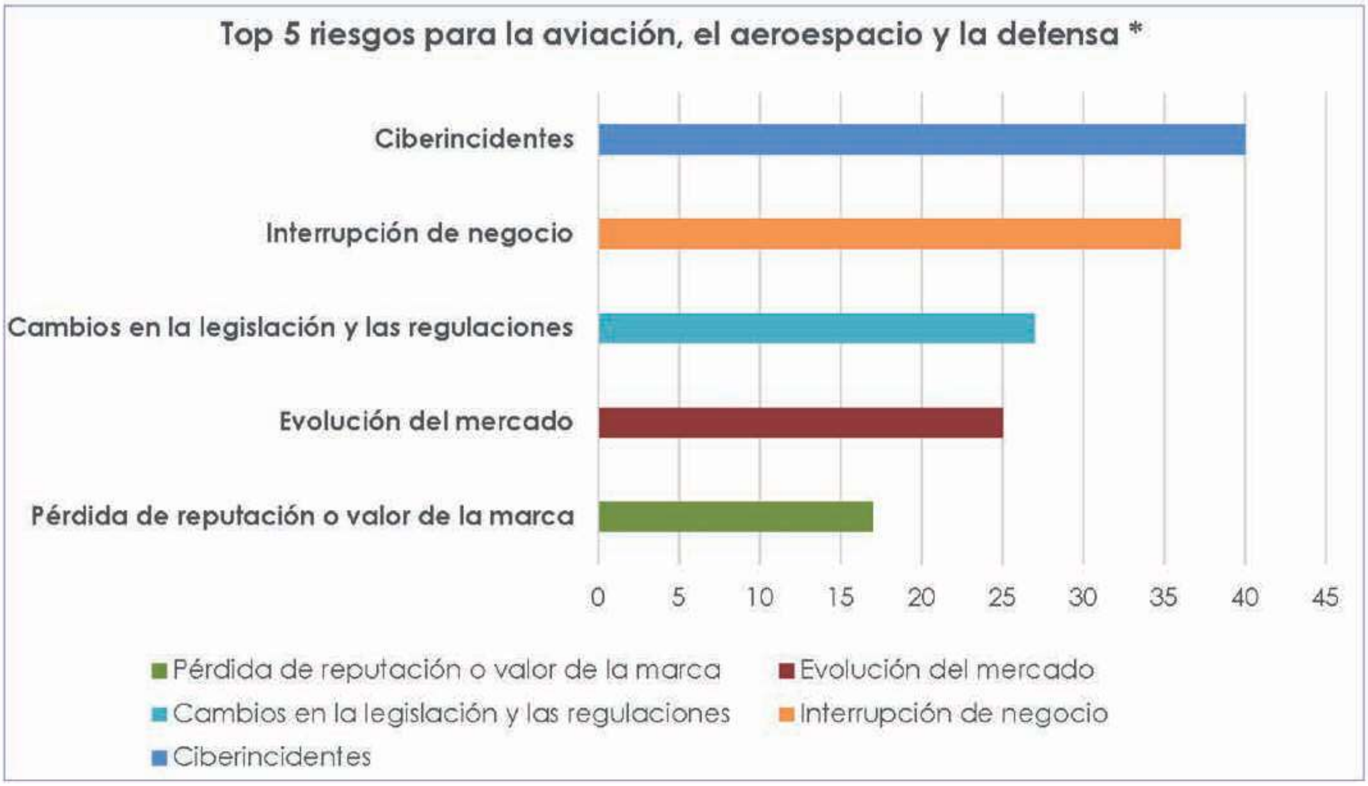

Fig. 1 Las figuras representan el porcentaje de ocasiones en las que los riesgos fueron mencionados por los profesionales del sector encuestados. Fuente: Allianz Risk Barometer Results Appendix 2020

social del país. Por tanto, la protección de toda la infraestructura tecnológica es una prioridad para todos.

La información, un activo de alto valor que hay que proteger

Dentro de todas las tecnologías que cumplen funciones esenciales en el sector aéreo hay un activo especialmente delicado, objetivo de los ciberatacantes, que es necesario salvaguardar: la información.

El ciberespacio ya se ha establecido como un territorio propio en el que individuos, colectivos, empresas e instituciones llevan a cabo actividades y "hacen vida": interactúan, se comunican, realizan acciones comerciales, educativas, sociales o laborales. Estos intercambios sociales crecen exponencialmente, pues así lo permite el vertiginoso avance de las TIC.

Entre los diferentes sistemas y equipos que se integran dentro del conjunto de la tecnología aeroespacial hay un enorme y constante flujo de datos. Por ejemplo, que un vuelo se pueda llevar a cabo con éxito depende, en gran medida, de la información que el avión intercambia con los centros de control de tráfico aéreo.

En este sentido, es necesario tener muy en cuenta que la tecnología presente en la aviación es tan atacable como el resto. De hecho, profesionales de la ciberseguridad ya han demostrado que se pueden interferir los datos entre un avión y la torre de control, donde hay gran cantidad de sistemas a través de los cuales conseguir que el tránsito de aeronaves en los aeropuertos y espacios aéreos sea lo más seguro, ordenado y rápido posible.

Por otro lado, los vuelos comerciales comparten una gran cantidad de información con aplicaciones de seguimiento de vuelos. Esta, en algunas de estas apps, no está cifrada, por lo que también podría ser interceptada, dando lugar a posibles ataques como la creación de datos falsos en los sistemas informáticos, crear un tráfico erróneo o interferir en el GPS.

La información que maneja el sector, especialmente la que se maneja en el cockpit se puede convertir en un blanco de interés preferente para los ciberdelincuentes. Su protección implica, de un lado, una mayor atención y una gestión adecuada de las obligaciones que trae consigo la seguridad de las aeronaves y que tendrá prioridad sobre cualquier otro tipo de consideración.

Riesgos de las redes sociales

Mucha de la información que hoy en día circula por el ciberespacio viene a través de las redes sociales, donde se conforman las identidades digitales de las personas y donde principalmente tiene lugar la "vida en el ciberespacio" de cada individuo.

Lo que es más importante, asociado a esas referencias hay un volumen significativo de contenidos en texto, imagen, audio o vídeo, donde una persona muestra su comportamiento, sus afinidades, sus intereses y, en definitiva, una traza más o menos detallada de su vida personal, social y, a menudo, laboral.

1 https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html

Fig.2 Buenas prácticas en el uso de las redes sociales

Las identidades virtuales asociadas a pilotos y controladores aéreos son claves. En algunos casos, se trata de cuentas que tiene una finalidad didáctica para explicar aspectos del vuelo; pero generalmente son perfiles que buscan ser referentes en el sector aéreo, pero no siempre teniendo en cuenta los riesgos que supone para el transporte aéreo publicar determinados datos o imágenes e incluso para su relación laboral/profesional con su compañía aérea.

Obviamente, los pilotos dentro de su ejercicio profesional comparten información durante su actividad y desde las aeronaves de la compañía para la que operan, el reto es evitar incurrir en malas prácticas profesionales con los potenciales riesgos asociados.

En general, los actores que emplean las redes sociales como puerta de entrada para realizar ciberataques y comprometer la seguridad de los usuarios aprovechan tres tipos de vulnerabilidades implícitas a la propia "arquitectura social" de las redes:

1) **Sobreexposición de información personal.** La sobreabundancia de información personal, que los usuarios difunden a través de sus perfiles en redes sociales, constituye una atractiva materia prima para que los cibercriminales utilicen esa información con propósitos dañinos.

2)**Autopistas de información.** La propia fluidez y apertura inherente a la comunicación convierte a las redes sociales en auténticas autopistas de información por las que circulan comunicaciones socialmente inocuas y legítimas, así como contenidos vinculados a diversos tipos de código dañino.

3) **Utilización masiva.** Con un índice de penetración del 60% de la población mundial, las redes sociales son el vehículo perfecto para acceder a un gran número de personas, potenciales víctimas de un ciberataque a través de distintas herramientas:

• Ingeniería social: consiste en el diseño de mecanismos o esquemas de engaño, destinados a hacer que los usuarios lleven a cabo determinados comportamientos que les van a perjudicar.

• Robo de identidad: para ello, aprovechan la información personal difundida por los usuarios en redes sociales.

• Perjuicio reputacional: en el ámbito personal, social o laboral, derivado de contenidos en redes sociales que pueden perjudicar las relaciones de una persona en esos ámbitos.

• Publicidad dañina o engañosa: difundida y suministrada a través de redes sociales, en numerosas ocasiones con propósitos de fraude o de difusión de código dañino.

• Criminalidad en el mundo físico: se vale de información obtenida en redes sociales para realizar conductas delictivas en el ámbito físico.

• Distribución de malware: Los grupos cibercriminales utilizan las redes sociales sencillamente como canales de distribución de todo tipo de código dañino.

> La información que maneja el sector, especialmente la que se maneja en el cockpit se puede convertir en un blanco de interés preferente para los ciberdelincuentes

Riesgos para la aviación

Lógicamente, entre los usuarios de redes sociales se encuentran los profesionales de la aviación. Y, si bien es cierto que hay muchos de ellos que hacen un uso ejemplar de las mismas para posicionarse como referentes, compartir información de utilidad para los futuros trabajadores o mostrar una visión diferente del mundo a través de sus fotografías y vídeos, recientemente se ha podido notar un uso no siempre responsable dentro del sector.

A pesar de la especial protección que requiere la información relativa al transporte aéreo, se observa cómo ciertos datos que deberían ser confidenciales por su potencial riesgo, se comparten a través de estas redes, uno de los canales con mayor visibilidad en la actualidad.

Concretamente, a través de redes sociales como Twitter o Instagram, dos de las más usadas por los usuarios en todo el mundo, se publican imágenes del plan de vuelo, las trayectorias geográficas o la documentación operacional que manejan para planificarlo.

También los profesionales del sector comparten, en algunas ocasiones, datos técnicos de la aeronave, de la ruta que van a seguir o del combustible que han cargado. Todo ello, en numerosas ocasiones, sin ser conscientes de ello. ¿Se paran a observar bien el fondo de las imágenes subidas a la red? ¿Caen en la cuenta de que ampliando dichas imágenes se puede sacar información confidencial de la aerolínea o de sus sistemas? ¿Tienen en cuenta que el etiquetado geográfico de contenidos o geoloca-

lización puede permitir a un atacante realizar un control de itinerarios -mapa de tiempos y lugares- con fines maliciosos?
Como ya se ha comentado, compartir ciertos datos de la aeronave o el vuelo podría permitir un acceso a los equipos informáticos por parte de una persona con intenciones dañinas.

A través de la ingeniería social, revisando los perfiles de redes sociales y usando un poco de ingeniería social[2] un cibercriminal puede conseguir información que podría poner en riesgo la seguridad de la aeronave.
Muchas compañías aéreas son cada vez más conscientes del

enorme riesgo que supone hacer un uso inapropiado de las redes sociales y compartir información sensible, más aún en un sector que ha de estar extremadamente protegido como es la aviación. Es primordial tener en cuenta que los contenidos que se publican en redes sociales no tienen ninguna protección, ni siquiera cuando estas son en conversaciones "privadas".

Los profesionales del vuelo, los pilotos, deben recordar que solo hace falta darle al botón de "publicar" para que un contenido se convierta en permanente. Aunque un usuario crea que los contenidos que publica solo van a llegar a un público determinado, nunca podrá estar seguro de dónde podrán acabar, ni en manos de quién. Tampoco sabrá tan siquiera a qué contenido podrían tener acceso terceras personas a través de sus perfiles.

Todos recordarán el caso reciente de dos pilotos de una aerolínea que, tras jugar con una aplicación de Snapchat durante un vuelo y subir el vídeo a las redes sociales, fueron sancionados por su empresa.[3]

Al igual que todo piloto designado comandante de aeronave deberá mantenerse en buenas condiciones psicofísicas, también deberá velar por un empleo adecuado de toda información sensible relacionada con el desarrollo del vuelo como los planes de vuelo, identificación de aeronaves, códigos, trayectorias geográficas, etc. evitando que el acceso o la alteración de la misma pudiera afectar a la seguridad del vuelo o a la realización de sus cometidos.

El comandante de aeronave se preocupará, en su caso, de que los miembros de su tripulación sigan los procedimientos adecuadas que no pongan en riesgo innecesario la aeronave y desarrollo del vuelo siendo permanente ejemplo ante sus subordinados, destacando por su competencia, liderazgo y profesionalidad.

Por su parte, cada vez son más las aerolíneas que regulan el uso de las redes sociales por parte de los pilotos y demás profesionales de la aviación, incidiendo en la importancia de no tomar fotografías, ni grabar vídeos desde la cabina cuando el avión esté volando a una altura inferior a 3.000 metros, a menos que cuenten con permiso previo explícito y por escrito.

De hecho, algunas compañías especifican que tampoco está permitido que los pilotos publiquen fotografías ni vídeos en redes sociales cuando las imágenes muestren al piloto y/o a sus compañeros con uniforme, cuando se muestre cualquiera de las instalaciones o cuando esas imágenes se tomen mientras el piloto está de servicio.

2 La Ingeniería social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Es una técnica que pueden usar ciertas personas para obtener información, acceso o permisos en sistemas de información que les permitan realizar algún acto que perjudique o exponga la persona u organismo comprometido a riesgos o abusos. El principio que sustenta la ingeniería social es el que en cualquier sistema "los usuarios son el eslabón débil"

3 https://www.ondacero.es/noticias/mundo/sancion-a-dos-pilotos-de-easyjet-por-jugar-con-el-movil-durante-un-vuelo_201803265ab913acocf271a8efee22dd.html

Cómo prevenir los riesgos

Como ya hemos comentado, los riesgos mencionados son a menudo subestimados, o incluso desconocidos. Muchos profesionales de la aviación, confiados en que sus cuentas no alojan nada interesante para los cibercriminales, descuidan lo que comparten en estas.

En este sentido, es de vital importancia que los pilotos y los profesionales de la aviación adopten una serie de medidas y buenas prácticas, de modo que no pongan en riesgo su seguridad y la de los pasajeros, su carrera profesional o la imagen de la aerolínea.

Minimizar los riesgos en redes sociales no es muy distinto a reducirlos en el espacio físico: el comportamiento del usuario aumentará o disminuirá el ecosistema para que las amenazas operen maliciosamente.

Las buenas prácticas de comportamiento en redes sociales pueden contribuir a reducir o anular las intenciones maliciosas.

Dicho lo cual, desde el CCN-CERT recomendamos aplicar los siguientes consejos:

1. Prestar atención a cómo defines tu perfil en redes sociales es clave, ya que será la carta de presentación de tu identidad en el ciberespacio. Es importante que, si se vas a publicar información relativa a tu actividad profesional, especifiques la compañía para la que trabajas y dejes claro que todo lo que compartes es personal, es decir, que no se hace en nombre de la empresa.
2. Personaliza los permisos que concedes a las aplicaciones de redes sociales en los diferentes dispositivos en que están instaladas.
3. La información que compartes en redes sociales, por privadas que estas estén configuradas, permanecerá y podrá ser utilizada en un futuro. Por ello, es esencial meditar bien que lo que publicas no podrá llevar asociadas consecuencias negativas posteriormente, ya sea en el ámbito personal o en la relación laboral con la aerolínea.
4. No compartas información que pueda identificar los vuelos, trayectorias geográficas o datos confidenciales. Cuantos más contenidos de este tipo compartas, más probabilidades habrá de que un ciberatacante lleve a cabo una actividad ilícita.
5. Controla la geolocalización de perfiles y contenidos en redes sociales. Desactiva la geolocalización por defecto en el menú de configuración de los perfiles y haz un uso inteligente de la misma.
6. No acceder a ninguna red social ni tomar fotografías durante el despegue o aterrizaje del avión, así como cuando se esté volando por debajo de 3.000 metros de altura o bajo condiciones adversas.
7. Aplicar las políticas de privacidad y de redes sociales, si la hubiera, de la aerolínea para la que se opera.
8. Por último, y como base de todo lo anterior, adopta la consciencia de que la primera línea de defensa para la protección en el ciberespacio es uno mismo. De esta manera, la ayuda que instituciones y organizaciones de ciberseguridad presten será mucho más eficiente y uno mismo será de ayuda inapreciable para mantener unas redes sociales seguras. ■