Procedimiento Nº: E/06392/2019
940-0419

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 15 de abril de 2019 la entidad ***COMPAÑIA OPERADORA DE CORTO Y MEDIO RADIO IBERIA EXPRESS S.A.,*** con NIF ***A86312691*** (en adelante, IBERIA EXPRESS) notifica a esta Agencia española de Protección de Datos (en adelante AEPD) una violación de seguridad de datos personales como consecuencia que la entidad DEEPAIR SOLUTIONS (en adelante DEEPAIR), proveedor externo de servicio de análisis de datos de IBERIA EXPRESS, recibió -en fecha 10 de abril de 2019- un correo electrónico enviado por un *experto* en seguridad en el que se informaba de que una base de datos de IBERIA EXPRESS, se encontraba accesible desde Internet.

SEGUNDO: Con fecha 24 de junio de 2019, la Directora de la Agencia Española de Protección de Datos (en adelante AEPD) instó a la Subdirección General de Inspección de Datos a que procediera a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos objeto de la notificación, teniendo conocimiento de los siguientes extremos:

ANTECEDENTES

Las actuaciones de inspección se inician por la recepción de un escrito de notificación de quiebra de seguridad remitido por IBERIA EXPRESS en el que informan, a la Agencia Española de Protección de Datos que, con fecha 10 de abril de 2019, la entidad DEEPAIR, proveedor externo de servicio de análisis de datos de IBERIA EXPRESS, recibió un correo electrónico enviado por un *experto* en seguridad en el que se informaba de que una base de datos de IBERIA EXPRESS, se encontraba accesible desde Internet.

El 2 de abril de 2019, la base de datos de IBERIA EXPRESS se había modificado para facilitar su accesibilidad por Internet y una vez confirmada la información del correo electrónico recibido se reconfiguró la web para impedir su acceso por Internet.

La base de datos contenía información de unas 117.397 reservas desde el 30 de enero al 10 de abril de 2019 que correspondían a 181.256 pasajeros con datos de nombre y apellidos, dirección de correo electrónico, origen y destino del vuelo, fecha del vuelo, el número de vuelo y algunos otros detalles de reserva.

Con fecha 30 de mayo de 2019, IBERIA EXPRESS remite a la Agencia información adicional sobre la brecha notificada que incluye un informe que pone de manifiesto los siguientes aspectos:

- El día 10 de abril de 2019, DEEPAIR recibió un correo electrónico enviado por un *experto* en seguridad en el que se informaba de que una base de datos se encontraba accesible desde Internet. La base de datos correspondía a pasajeros de Iberia Express, compañía para la que DEEPAIR se encontraba prestando distintos servicios de análisis de datos en calidad de encargado del tratamiento.
- La base de datos fue creada y gestionada por DEEPAIR, en un servidor AZURE de Microsoft propiedad de IBERIA EXPRESS, y por la empresa BIRCHMAN CONSULTING, S.L. (en adelante BIRCHMAN) encargada del mantenimiento de la infraestructura en *cloud* y seguridad (encargada de los diferentes servidores de la plataforma AZURE).
- El día 2 de abril de 2019, BIRCHMAN, a petición de DEEPAIR, abrió un puerto que tuvo el efecto involuntario de permitir el acceso a la Base de Datos desde Internet. El puerto permaneció abierto desde el día 2 de abril de 2019 hasta el 10 de abril de 2019, fecha en la que DEEPAIR recibió el correo electrónico y solicitó a BIRCHMAN la clausura de puerto. En esa misma fecha DEEPAIR informó a Iberia Express del Incidente.
- IBERIA EXPRESS contrató a una tercera empresa especializada la realización de un informe sobre los hechos acaecidos que concluyó con los siguientes aspectos:

    a. La Base de Datos estuvo accesible a través de Internet entre el 2 y 10 de abril de 2019 (ambos incluidos) y desde 44 direcciones de IP se hicieron un total de 110 conexiones a la base de datos.

    b. Las 44 direcciones IP están asociados con delitos de baja complejidad cometidos a través de Internet (por ejemplo, *malware* básicos, *phishing*), y una variedad de servidores alquilados y hosts desconocidos, cuyos propósitos son desconocidos.

    c. De las 44 direcciones IP detectadas, dos estuvieron mucho tiempo conectadas, una de ellas correspondía al *Experto*, que estuvo conectado durante varias horas. La otra desconocida y registrada en China y permaneció conectada durante más de 16 minutos. Cuando el *Experto* estaba conectado, el análisis de la utilización de la red del servidor mostró un aumento en el tráfico. Sin embargo, cuando la dirección IP china se conectó, el tráfico de red no fue notablemente más alto que el nivel diario habitual.

    d. IBERIA EXPRESS manifiesta que es razonable concluir que sólo el *Experto* fue capaz de descargar una gran cantidad de datos. No existen evidencias que permitan discernir exactamente qué datos fueron extraídos.

    e. La Base de Datos contenía información relativa a un total de 117.397 reservas, que incluyen datos personales de 181.256 pasajeros. Los datos de carácter personal se corresponden con información asociada a un proceso de compra/reserva: PNR, nombre, dirección mail, teléfono, fecha de nacimiento, residencia, documento de identidad, origen y destino, necesidades especiales… y datos de pago protegidos que no permiten utilizar.

IBERIA EXPRESS ha aportado copia de los contratos suscritos con BIRCHMAN y DEEPAIR así como información sobre la infraestructura en *cloud* del canal web de la compañía.

ENTIDADES INVESTIGADAS

COMPAÑIA OPERADORA DE CORTO Y MEDIO RADIO IBERIA EXPRESS S.A. con NIF A86312691 con domicilio en C/ ALCAÑIZ 23 - 28042 MADRID (MADRID).

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

Con fechas 5 de julio y 1 de agosto de 2019 se requiere información a IBERICA EXPRESS y de la respuesta recibida en fecha 16 de agosto se desprende:

Respecto de la empresa

- IBERIA EXPRESS tiene suscrito un Acuerdo Marco para la prestación de servicios tecnológicos con BIRCHMAN sobre implantación de mejoras y desarrollos en tecnología informática, de fecha 1 de enero de 2016.

Entre los servicios contratados consta la *Gestión de Comunicaciones y redes* y en su punto número 4 se establece las reglas de gestión de los puertos de comunicación y el procedimiento para la apertura de puertos.

En este procedimiento se indica que se deben de cumplir, entre otras condiciones, la realización de un análisis de riesgo sobre este servicio verificando, entre otras, las vulnerabilidades, las credenciales de acceso, la seguridad que impidan a un tercero interceptar los datos en tránsito. Asimismo, se deben acotar las direcciones IP de acceso a los puertos (evitar el acceso a cualquier dirección IP).

Asimismo, se debe obtener autorización expresa del responsable de seguridad tras la presentación del análisis de riesgo y el impacto de la apertura del puerto.

IBERIA EXPRESS ha aportado copia del procedimiento mencionado y del contrato suscrito con BIRCHMAN.

- IBERIA EXPRESS tiene suscrito un contrato de prestación de servicios con DEEPAIR para envío de comunicaciones comerciales de productos y servicios a miembros del *Club Express* informando de las promociones de la compañía y otros servicios incluidos el análisis y creación de perfiles de usuario para mejor determinar los productos y servicios de interés.

IBERIA EXPRESS ha aportado copia del contrato mencionados.

Respecto de la cronología de los hechos. Medidas de minimización de la incidencia

IBERIA EXPRESS ha aportado copia del Informe sobre la incidencia realizado por la empresa MANDIANT. En dicho informe figura:

- El día 10 de abril de 2019, DEEPAIR recibió un correo electrónico de un investigador de seguridad indicando que una base de datos era accesible desde Internet. En el correo se incluía la captura de pantalla con datos que mostraban PNR (datos relacionados con una reserva de avión) y direcciones de correo electrónico asociadas.

A las 12:38 horas de ese día, DEEPAIR remitió un correo a BIRCHMAN solicitando el cierre de los puertos del servidor en el que se alojaba la base de datos impidiendo su acceso desde internet. A las 12:43 BIRCHMAN confirmó el cierre de los puertos.

- En un análisis en profundidad se comprobó que el acceso estuvo disponible desde el día 2 al 10 de abril de 2019 y 44 direcciones IP realizaron un total de 110 conexiones a la base de datos.

Dos direcciones IP destacaron por el tiempo de conexión. Una de ellas corresponde al investigador de seguridad de la empresa Security Discovery y otra dirección a una IP ubicada en China. El tráfico aumentó con la conexión del investigador por lo que concluyen que pudo descargar datos de la base de datos, aunque no se puede identificar exactamente qué información.

Asimismo, concluyen que no hay indicios suficientes que indiquen que cualquier usuario no autorizado descargara un gran volumen de datos ya que hubiera aumentado notablemente el tráfico.

Respecto de las causas que hicieron posible la incidencia

- DEEPAIR, en su calidad de gestor de la base de datos, solicitó a BRICHMAN la apertura de un puerto que tuvo el efecto involuntario de permitir el acceso a la base de datos desde Internet. Esta empresa verificó que el solicitante era un proveedor autorizado de IBERIA EXPRESS.

A este respecto, IBERIA EXPRESS manifiesta que:

  - Tanto la apertura como el cierre de los puertos se llevó a cabo por BIRCHMAN sin pedir autorización a IBERIA EXPRESS.
  - DEEPAIR no estableció controles de acceso a la base de datos y el trabajo debería haberse desarrollado en los propios sistemas de DEEPAIR, en un entorno cerrado.

IBERIA EXPRESS ha aportado copia del correo de DEEPAIR solicitando el cierre del puerto, de los correos intercambiados con el experto de seguridad y de los intercambiados con las empresas DEEPAIR y BIRCHAMN en relación con la incidencia.

Respecto de los datos afectados. Notificación.

- La Base de Datos contenía información relativa a un total de 117.397 reservas, que incluyen datos personales de 181.256 pasajeros. Los datos de carácter personal se corresponden con información asociada a un proceso de compra: PNR, nombre, dirección mail, teléfono, fecha de nacimiento, residencia, documento de identidad, origen y destino, necesidades especiales… y datos de pago protegidos que no permiten utilizar.
- IBERIA EXPRESS entiende que la naturaleza de los datos accedidos no puede causar daños que afecten gravemente a la privacidad y derechos de sus titulares ya que los datos sobre tarjetas de crédito completos no eran

accesibles y se ha hecho un seguimiento sobre las reservas para detectar cualquier operación sospechosa de utilización del resto de los datos.

- IBERIA EXPRESS manifiesta que no considera probable que los datos descargados por el experto se utilicen para finalidades ilegítimas ya que él mismo contactó con la entidad para ofertar consultoría sobre ciberseguridad.

Respecto de las acciones tomadas para la resolución final de la incidencia

- IBERIA EXPRESS contrató una auditoria de seguridad a la empresa All4Sec, S.L. que propuso una serie de recomendaciones que serán implantadas por DEEPAIR con el fin de garantizar en mayor medidas las alertas sobre accesos.

Respecto de las medidas de seguridad implantadas con anterioridad al incidente

- IBERIA EXPRESS ha aportado los siguientes documentos:
  - Copia del Registro de actividad correspondiente al tratamiento objeto del incidente.
  - Evaluación de Impacto sobre el tratamiento mencionado llevada a cabo el 28 de marzo de 2018 donde se especifican las medidas de seguridad para el acceso por terceros.
  - Procedimiento para las brechas de seguridad.
  - Auditorias de Seguridad.
  - Política General de Protección de Datos. Donde constan anexos respecto de: "*Gestión de tratamientos de datos personales*", y "*Directrices para el envío de comunicaciones comerciales".*

Respecto de las medias implementadas con posterioridad a la incidencia

- Formación y concienciación en materia de seguridad de la información del personal interno de la entidad y de los proveedores externos contratados.
- Revisión de pruebas de cumplimiento de prácticas de seguridad
- Auditorias de seguridad

FUNDAMENTOS DE DERECHO

I

De acuerdo con los poderes de investigación y correctivos que el artículo 58 del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) otorga a cada autoridad de control, y según lo dispuesto en el artículo 47 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y

garantía de los derechos digitales (en lo sucesivo LOPDGDD), es competente para resolver estas actuaciones de investigación la Directora de la Agencia Española de Protección de Datos.

II

El RGPD define, de un modo amplio, las "violaciones de seguridad de los datos personales" (en adelante quiebra de seguridad) como "todas aquellas violaciones de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos."

En el presente caso, se produjo una quiebra de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como una posible brecha de confidencialidad como consecuencia del acceso indebido por terceros ajenos al sistema de información de Iberia Express.

De las actuaciones de investigación se desprende que Iberia Express, en calidad de responsable del tratamiento, disponía de medidas técnicas y organizativas preventivas a fin de evitar este tipo de incidencias pero, sin embargo, de forma excepcional se produjo la incidencia ahora analizada.

Asimismo, Iberia Express disponía de protocolos de actuación para afrontar el incidente, lo que ha permitido la identificación, análisis y clasificación de la brecha de seguridad de datos personales así como la diligente reacción ante la misma al objeto de notificar, comunicar, minimizar el impacto e implementar nuevas medias razonables y oportunas para evitar que se repita la incidencia en el futuro a través de la puesta en marcha y ejecución efectiva de un plan de actuación por las distintas figuras implicadas como son el responsable del tratamiento y las agencias colaboradoras en calidad de encargadas, así como el Delegado de Protección de Datos.

No constan reclamaciones ante esta Agencia de los afectados.

En consecuencia, se debe concluir que Iberia Express disponía de medidas técnicas y organizativas razonables para evitar este tipo de incidencia y que al resultar insuficientes han sido actualizadas de forma diligente mediante formación y concienciación en materia de seguridad a los empleados y personal externo, revisión de pruebas de cumplimiento de prácticas de seguridad e implantación de auditorías de seguridad. Además, Iberia Express dispone de un Informe final sobre la trazabilidad del suceso y su análisis valorativo, en particular, en cuanto al impacto sobre los. Este Informe es una valiosa fuente de información con la que debe alimentarse el análisis y la gestión de riesgos y servirá para prevenir la reiteración de una brecha de similares características como la analizada causada previsiblemente por un error puntual.

III

Por lo tanto, se ha acreditado que la actuación de Iberia Express como entidad responsable del tratamiento ha sido acorde con la normativa sobre protección de datos personales analizada en los párrafos anteriores.

Por lo tanto, de acuerdo con lo señalado, por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución a ***COMPAÑIA OPERADORA DE CORTO Y MEDIO RADIO IBERIA EXPRESS S.A.,*** con NIF ***A86312691*** y con domicilio en ***C/ ALCAÑIZ 23 - 28042 MADRID (MADRID).***

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de conformidad con lo establecido en los arts. 112 y 123 de la citada Ley 39/2015, de 1 de octubre, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

Mar España Martí
Directora de la Agencia Española de Protección de Datos