Procedimiento Nº: E/05727/2019
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: Las actuaciones de inspección se inician por la recepción de un escrito de notificación de quiebra de seguridad remitido por la UNIÓN Temporal de Empresas (UTE) formada por ***HIBERUS TECNOLOGIA DE LA INFORMACIÓN, S.L.*** y ***SICOMORO SERVICIOS INTEGRALES, S.L.*** (en adelante UTE) en el que informan a la Agencia Española de Protección de Datos (en adelante AEPD) de que, con fecha 17 de mayo de 2019, han recibido un correo electrónico de un periodista del diario EL CONFIDENCIAL indicando que un tercero les ha comunicado un fallo de seguridad en el sitio web que gestiona la venta de entradas del "***PATRONATO DE LA ALHAMBRA DE GRANADA Y GENERALIFE"*** (en adelante el Patronato). En el escrito de notificación la UTE considera que la posible fecha de inicio de la brecha de seguridad es el 18 de febrero de 2019.

El 22 de mayo de 2019 se reciben en la AEPD escritos de reclamación de la Asociación de Consumidores y Usuarios en Acción **FACUA** y de ***A.A.A.*** en el que informan del fallo de seguridad en la web de la Alhambra de Granada que ha dejado expuestos los datos de los visitantes durante dos años. ***A.A.A.*** manifiesta que sus datos se encuentran entre los expuesto por el incidente de seguridad.

Con fecha 24 de mayo de 2019 se reciben en la AEPD sendos escritos de reclamación de las compañías ***GLOBAL 3D VIRTUAL STORIES, S.L.*** y ***CITY TOUR ALHAMBRA VIAJES, S.L.*** en los que se pone de manifiesto que con motivo de un fallo de seguridad en el sitio web que gestiona la venta de entradas a la Alhambra de Granada han sido expuestos los datos de sus compañías, entre ellos, datos bancarios y credenciales de acceso a la web de gestión de entradas. Ambas entidades manifiestan que mantienen una relación mercantil con la UTE y el Patronato de la Alhambra motivo por el cual disponen de clave de acceso a la web objeto del incidente de seguridad.

Con fecha 4 de junio de 2019 se recibe en la AEPD un escrito de reclamación de ***B.B.B.*** en relación con el incidente en la venta de entradas donde indica que tal y como se ha publicado en el diario EL CONFIDENCIAL (el ******FECHA.1***, se publica una noticia en la dirección ******URL.1***, sobre la brecha de seguridad) han quedado expuestos al público los datos los visitantes, entre los que se encuentran sus datos personales.

SEGUNDO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos objeto de la reclamación, teniendo conocimiento de los siguientes extremos:

ANTECEDENTES

Fecha de notificación de quiebra: 23 de mayo de 2019

ENTIDADES INVESTIGADAS

UTE HIBERUS TECNOLOGIAS DE LA INFORMACIÓN, S.L. Y SICOMORO SERVICIOS INTEGRALES, S.L. (UTE) con ***NIF U99493280*** y con domicilio en c/ ***BARI 25, 1-2, 50197 ZARAGOZA.***

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1 Con fecha 24 de junio de 2019 se requiere información a la UTE y de la respuesta recibida con 9 de julio de 2019 se desprende:

Respecto de la UTE y la Plataforma de venta de entradas

- La UTE ha aportado copia del contrato suscrito con el Patronato de la Alhambra de Granada, de fecha 31 de mayo de 2017, para el Servicio de Gestión Integral de la Reserva y Venta de Entradas del Patronato de la Alhambra y Generalife y copia del contrato de encargado del tratamiento de fecha 7 de mayo de 2018, por el que se habilita a la UTE a tratar los datos personales necesarios para la prestación del servicio de Gestión de Reserva y Venta de entradas cuyo responsable es el Patronato de la Alhambra y el Generalife.
- En el documento de encargado del tratamiento se especifica que los datos personales serán: nombre y apellidos, documento de identidad, nacionalidad, edad, sexo, email, dirección postal, ciudad, país, teléfono. Se incluye grado de disfuncionalidad en caso de que sea superior al 33%.

  En el caso de menores se recaban, además, los datos de nombre y apellidos y documento de identidad de los padres o tutores. También se recogen los datos de contacto o de representantes de agentes, en su caso.
- La UTE ha aportado copia del manual de venta online de entradas a la Alhambra.

Respecto de la cronología de los hechos y las medidas realizadas para minimizar el impacto de la incidencia.

- El 17 de mayo de 2019 a las 13:23 la UTE recibe un correo electrónico enviado por un periodista de EL CONFIDENCIAL y en ese mismo momento se crea un equipo técnico de trabajo y se comienza una investigación interna. Asimismo, se contesta el mail recibido.

  La UTE ha aportado copia del mail recibido donde se informa de que una fuente anónima ha alertado de un fallo de seguridad en la web de compra

de entradas de la Alhambra al tener una versión desactualizada del software y presenta una vulnerabilidad del tipo *SQL injection.*

- Sobre las 15:30 horas del 17 de mayo día, el equipo técnico de la UTE comprueba la existencia de una vulnerabilidad que permite un ataque de *inyección SQL,* por lo que se podría haber accedido al contenido de las bases de datos de la venta de entradas online.
- Inmediatamente se aplica un *parche de seguridad* para impedir un nuevo ataque mediante la vulnerabilidad detectada. Cerrando la brecha en el plazo de dos horas aunque el ataque podría haberse efectuado entre los días 18 y 22 de febrero de 2019.
- A partir de este momento y todo ello el mismo día 17 de mayo se implantan las siguientes medidas.
  - Se suspenden todas las credenciales de acceso y se modifican las credenciales de usuarios privilegiados.
  - Se procede a realizar una copia del sistema para el análisis posterior con herramientas forenses
  - Se modifica el código de interfaz de programación y el código web para evitar el mismo incidente.
  - Se realizan pruebas de inyección de SQL contra el código modificado, se testea el servidor y una vez comprobado se implanta en producción.
  - Se anota el registro del incidente de seguridad en los procedimientos de la UTE. A este respecto la UTE ha aportado el Registro de la incidencia con dos anotaciones en fechas 17 y 22 de mayo en el que se incluyen las soluciones aportadas y las comunicaciones realizadas al Patronato.
  - Se comunica el incidente y su resolución al Patronato.
- El 18 de mayo se procede a la revisión y actualización del resto de sitios webs y se comprueba que no presentan la vulnerabilidad detectada.
- El 19 de mayo se remite un correo electrónico al diario EL CONFIDENCIAL informando de la resolución de la incidencia.
- El ******FECHA.1*** el diario EL CONFIDENCIAL publica la noticia de la brecha en la dirección ******URL.1***

  A este respecto, desde la Inspección de Datos, con fecha ******FECHA.2***, se ha accedido a la dirección ******URL.2*** verificando que figura información sobre una brecha de seguridad en la venta de entradas de la Alhambra por una vulnerabilidad que permitía una *inyección de SQL* dejando expuestos más cuatro millones y medio de datos personales de visitantes y de cerca de mil datos de agencias de viajes. En la publicación figura una fotografía en la que se muestran parcialmente datos de contraseña, direcciones de correo y cuentas bancarias de agencias de viajes.
- Ese mismo día ******FECHA.1*** el Comité de Protección de Datos y el equipo técnico acuerdan la realización de un análisis forense del ataque y una auditoria de seguridad. También se convoca reunión con el Patronato a fin de transmitirle la información disponible hasta ese momento.

A través del canal de Twitter de HIBERUS se publica una nota informativa en relación con el incidente de la web de entradas de La Alhambra en la que se indica que ha habido un ataque informático profesional y organizado ya corregido y que se va a proceder a notificar a los Cuerpos y Fuerzas de Seguridad del Estado y a la AEPD.

A este respecto, desde la Inspección de Datos y con fecha ******FECHA.3***, se ha comprobado la existencia de la mencionada nota informativa en la dirección ******URL.3***

- Asimismo se remite informe preliminar al Patronato. Dicho informe ha sido aportado por la UTE y se informa de lo acaecido y de las medias inmediatas implantadas.
- El 23 de mayo de 2019 se presenta denuncia ante la Guardia Civil y ante la AEPD, remitiendo posteriormente copia de las mismas al Patronato e informando de que se ha resuelto realizar una auditoría de seguridad y un análisis forense de los hechos. El Patronato da su conformidad para el acceso a los datos personales necesarios al sistema.
- El 17 de junio de 2019 la UTE recibe informe pericial en el que se concluye que con anterioridad ha habido ataques infructuosos y la causa de acceso parece ser que alguna versión del sistema había dejado abierta una vulnerabilidad. Este informe se remite también al Patronato.

  La UTE ha aportado copia del informe pericial en el que se analizan los registros de accesos (logs). En el análisis de la actividad de la web se detalla:

  - Un primer intento por inyección de SQL resultó fallido.
  - Posteriormente se intentaron tres nuevo ataques, también fallidos.
  - Se detecta el intento de acceso a través de una IP ubicada en Singapur.
  - Se detectan diversos intentos de albergar programas maliciosos (Malwere)
  - De enero a abril de 2019 se realizó un ataque organizado directamente a las bases de datos para explotar una vulnerabilidad que han ido testando en ataques anteriores con medidas que lo ocultaban a los sistemas de seguridad implantados.
  - Los datos no consta que hayan sido alterados
  - Tras una actualización en el sistema se quedó abierta una vulnerabilidad que permite el ataque a través de *inyecciones SQL.*

  Con fecha ******FECHA.4*** se ha accedido a la dirección ******URL.4*** sin obtener resultado de la publicación mencionada. La dirección web devuelve el mensaje de "*No encontrado"*
- El 19 de junio de 2019 se procede a comunicar el incidente a las agencias de viajes (504) a través de correo electrónico.

  La UTE ha aportado copia del escrito de comunicación a las agencias en el que se informa, entre otros aspectos, del ataque sufrido ya ha sido

corregido y que la información de las tarjetas bancarias no ha resultado comprometido.

- El 3 de julio la UTE recibe dos nuevos informes periciales denominados "*Auditoría técnica Hiberus (dominio actual Alhambra*)", y *"Auditoría técnica Hiberus - (dominio atacado Alhambra)",* que analizan las vulnerabilidades existentes en el momento en el que se efectuó el ataque y en el momento actual tras la aplicación de las medidas implantadas. En dichos informes se concluye que la única vulnerabilidad existente en el momento del ataque corresponde a la ahora analizada y el resto no tenía problemas de filtración. Asimismo, se concluye que:
  - No existe posibilidad de acceso a datos y cualquier ataque realizado ha rechazado el acceso a datos.
  - Existen pequeños elementos a corregir pero eso no expone en la actualidad peligro alguno a acceso a los datos.
  - Se observa también una vulnerabilidad que permitiría poder deshabilitar temporalmente el funcionamiento de la web, no alterando en ningún momento ni poniendo en peligro las bases de datos.
- El 4 de julio se presenta el informe relativo a los incidentes de seguridad, incluyendo una valoración global, análisis y juicio crítico.

Respecto de los datos afectados

- La UTE manifiesta que el ataque permitió el acceso a las bases de datos pero se desconoce el volumen de datos afectados por la brecha. Solo se ha podido constatar que las consultas o instrucciones enviadas por medio de la *inyección de SQL* tuvieron un resultado positivo.
- En cuanto a la tipología de los datos de clientes corresponden a: nombre y apellidos, documento identificativo, dirección postal, dirección de correo electrónico, número de teléfono, edad, nacionalidad, sexo, ciudad de nacimiento, país, reservas efectuadas o entradas adquiridas y la mención a grado de disfuncionalidad igual o superior al 33%.

  En relación con este último dato, la UTE manifiesta que el sistema permitía marcar una opción a fin de poder adquirir entradas a un precio bonificado. La identificación y comprobación de la condición de disfuncionalidad y su grado se realizaba al momento de acceder al recinto de La Alhambra, por lo que en el sistema solo se recoge la declaración del comprador.
- Respecto de los datos de las Agencias de Viajes (personas jurídicas) correspondían a: razón social, CIF/NIF, dirección de correo electrónico, dirección postal, número de teléfono, cuenta corriente y contraseña de acceso con datos de 2017por lo que resulta obsoleta e inservible.
- Se están realizando búsquedas en Internet, en la *deep web* y en la *darknet* para detectar posibles exposiciones de los datos afectados. Hasta el momento del informe el resultado ha sido negativo.
- La UTE manifiesta que el comunicado en su web se realizó a efectos de minimizar la alarma social que causó el incidente publicado en El

Confidencial y dar explicaciones ante los medios de comunicación. No constituyó una comunicación a los afectados, sino meras declaraciones.

- Desde la Inspección de Datos y con fecha 26 de septiembre de 2019 se ha accedió a la web del Patronato de la Alhambra (www.alhambra.org) sin obtener constancia de un comunicado sobre el incidente de seguridad.

Respecto de las medidas de seguridad implantadas con anterioridad al incidente

- La UTE ha aportado Informe para acreditar el cumplimiento de las medidas establecidas respecto de la norma ISO 27001 y las correspondientes al Anexo II Esquema Nacional de Seguridad, todo ello de acuerdo con el contrato de encargo de tratamiento.

  HIBERUS y SICOMORO están certificadas conforme al estándar ISO 27001.

  HIBERUS ha aportado certificado de AENOR del sistema de gestión de seguridad de la información conforme con la norma ISO 27001 vigente hasta el 26/10/2019.

  SICOMORO aporto certificado de AENOR ISO/IEC 27001 vigente hasta el 27/11/2020.

- La UTE ha aportado los siguientes documentos:

  o Registro de Actividades de Tratamiento.

  o Activación Plan respuesta ante Brecha de Seguridad.

  o Manual del Sistema de Protección de Datos Hiberus.

  o Procedimiento de Seguridad HIBERUS.

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

En el presente caso, tras el requerimiento de información llevado a cabo por la inspección de esta AEPD, las entidades investigadas han informado en tiempo y forma sobre las actuaciones internas realizadas y resultado de las mismas al objeto de minimizar los efectos de la quiebra de seguridad y evitar en el futuro su repetición.

Hay que destacar del análisis realizado la detección del método de intrusión utilizado, *sql inyection*, que consta que ha sido organizado e insistente y con carácter profesional, lo que ha permitido configurar el sistema de información de forma adecuada para evitar su repetición. Se debe señalar, que la vulnerabilidad detectada ha sido consecuencia de un fallo en el propio sistema de seguridad implantado que, si

bien rechazó los ataques previos, finalmente una vulnerabilidad en el procedimiento de actualización se software ha permitido el acceso a datos por terceros.

Consta que la UTE encargada del sistema de gestión de entradas ha informado a través de su cuenta Twiter sobre la incidencia y resolución. No constan que los datos hayan sido alterados

Tampoco consta que los datos personales de los usuarios hayan sido tratados de forma maliciosa por terceros, sino que quedaron expuestos al público. Señalar también, respecto a los datos expuestos de las Agencias de Viajes correspondían al año 2017 por lo que las claves de acceso eran obsoletas.

En consecuencia, las entidades analizadas han actuado de forma diligente y con intensidad razonable - dado el tipo de ataque profesional, insistente y organizado - para minimizar el impacto de la incidencia de seguridad y han implantado las medidas correctoras para evitar su repetición en el futuro.

III

Por lo tanto, se ha acreditado que la actuación del reclamado 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:

- ***HIBERUS TECNOLOGIAS DE LA INFORMACIÓN, S.L. Y SICOMORO SERVICIOS INTEGRALES, S.L.*** (UTE) con ***NIF U99493280*** y con domicilio en ***calle BARI 25, 1-2, 50197 ZARAGOZA.***

- ***PATRONATO DE LA ALHAMBRA Y GENERALIFE,*** con ***NIF Q1818001H,*** y con domicilio en ***calle REAL DE LA ALHAMBRA S/N, 18009 GRANADA.***

- ***ASOCIACIÓN DE CONSUMIDORES Y USUARIOS EN ACCIÓN (FACUA), con NIF G91344986, calle Bécquer 25 B, Sevilla, 41002.***

- ***A.A.A., ***DIRECCIÓN.1***

- ***B.B.B., ***DIRECCIÓN.2***

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