Procedimiento Nº: E/07039/2019
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 VIAJES PARA TI, S.L.U. (en adelante VIAJES PARA TI) en el que informan a la Agencia Española de Protección de Datos que el día 18 de junio a las 8:30 han detectado un ataque mediante herramientas de *inyección de sql*, en el que el atacante pudo acceder a cierto contenido de su base de datos de clientes. El responsable de tratamiento actuó rápidamente para bloquear el acceso no autorizado.

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: 21 de junio de 2019.

ENTIDADES INVESTIGADAS

VIAJES PARA TI, S.L.U. con NIF B55666952 con domicilio en AVDA. BELLISENS, NUM 42, PISO 1, PTA. 129 - 43204 TARRAGONA (TARRAGONA)

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

Con fecha 31 de julio de 2019 se requiere información a VIAJES PARA TI, y de la respuesta recibida con fecha 8 de agosto de 2019 se desprende:

Respecto de las causas que han hecho posible la incidencia

- El atacante aprovechó una vulnerabilidad existente en el código del programa (PHP) de acceso a la base de datos para intentar ejecutar sentencias SQL a la base de datos. Esta vulnerabilidad consistía en un parámetro que se pasaba en la consulta a la base de datos sin ser tratado previamente, con lo que permitía a un atacante enviar instrucciones SQL dentro del código.
- Han comprobado que el ataque no ha logrado modificar el contenido de los datos en los sistemas de información, siendo que la integridad de los datos se ha preservado en todo momento.
- Se desconoce el alcance exacto de la violación de seguridad de datos personales (en adelante brecha de seguridad), que ha debido ser mínima por cuanto se activaron los mecanismos de seguridad de forma rápida y efectiva. Asimismo,

aseguran que en ningún caso se ha accedido a datos de carácter sensible o especialmente protegidos.

Respecto de las acciones tomadas con el objeto de minimizar los efectos adversos del ataque

- El 18 de junio a las 8:30, momento en el que se detectó el ataque, la primera acción realizada fue la de bloquear las peticiones al servidor por parte de la IP que estaba realizando el ataque. Con esta acción, se cortó de raíz cualquier tipo de ataque procedente de la IP detectada como elemento malicioso.
- La segunda acción tomada fue el mismo día a las 11:00 h y consistió en solucionar la vulnerabilidad del fichero a través de la cual realizaron el ataque, tratando los datos recibidos por parámetro antes de ser enviados a la consulta SQL de la base de datos. Con esta acción, se procede a la resolución de la brecha de seguridad existente, vetando la posibilidad de nuevos ataques bajo la misma modalidad.
- Aportan copia de las actas de reunión del equipo de la organización de fechas 18/06/2019 y 25/06/2019, en las que constan documentadas que el equipo de la organización toma las medidas adecuadas para solventar la incidencia, así como minimizar las posibles consecuencias del ataque.

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

- Realización de una auditoría de seguridad interna, donde se han analizado diferentes tipos de ataque, entre ellos SQL inyectión.
- Instalación y configuración del módulo modSecurity con las reglas que previenen los diferentes tipos de ataques que actualmente se producen.
- Formación de seguridad al equipo técnico de la empresa, realizada durante los días 24 a 28 de junio de 2019.

Respecto de si tienen conocimiento de la utilización por terceros de los datos personales obtenidos a través de la brecha

- No tienen la certeza de que el atacante haya podido acceder a datos de carácter personal de los clientes. En cualquier caso, una vez revisados los sistemas de Información, se determina que no ha existido modificación y/o supresión alguna respecto de los datos existentes.
- No tienen conocimiento de ningún tipo de uso de datos por parte de un tercero. Nadie se ha puesto en contacto con la entidad al respecto ni tampoco han aparecido los datos en ningún tipo de indexación por buscadores.
- Los datos a los que se ha podido tener acceso, no constituyen en ningún caso datos sensibles o de especial protección.

Respecto de la seguridad de los tratamientos con anterioridad a la incidencia de seguridad

- Aportan copia de los Registros de Actividad que se han podido ver afectados.
- Aportan copia del Análisis de Riesgo y Ciclo de Vida de Datos realizado sobre las actividades de tratamiento que pudieron verse comprometidas por el ciberataque.

- VIAJES PARA TI tiene establecido un "Protocolo de actuación ante brechas o incidentes de seguridad" que se ha cumplido en la presente situación. Aportan copia del protocolo mencionado.

Respecto a la política de seguridad adoptada para los tratamientos de datos en los que se ha producido el ciberataque

- Actualmente, todas las actividades de tratamiento, en especial aquellas afectadas por el ciberataque, disponen de las adecuadas medidas 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, consta que se produjo una quiebra de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como brecha confidencialidad por el acceso indebido, a través de un ataque externo mediante el método de *inyección sql*, a la base de datos de VIAJES PARA TI.

No obstante, también consta que VIAJES PARA TI, a través del servicio de Informática, disponía de medidas técnicas y organizativas para afrontar un incidente como el ahora analizado, lo que ha permitido la detección, identificación, análisis y clasificación de la brecha de seguridad de datos personales así como la diligente reacción ante la misma al objeto de notificar y minimizar el impacto e implementar las medias razonables oportunas para evitar que se repita en el futuro a través de la puesta en marcha de un plan de actuación previamente definido por las figuras implicadas del responsable del tratamiento.

También debe valorase la adopción de medidas técnicas y de gestión, como es la contratación de una auditoria a todos los sistemas de información similares, y reconfiguración del fichero de acceso a la base de datos al objeto de comprobar y en su caso mejorar la calidad de las aplicaciones de gestión de datos personales.

El informe final tras el seguimiento y cierre sobre la brecha y su impacto es una valiosa fuente de información con la que debe alimentarse el análisis y la gestión de riesgos

futuros. El uso de esta información servirá para prevenir la reiteración del impacto de una brecha.

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 ***VIAJES PARA TI, S.L.U.*** con NIF ***B55666952*** y con domicilio en ***AVDA. BELLISENS, NUM 42, PISO 1, PTA. 129 - 43204 TARRAGONA (TARRAGONA)***

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