Procedimiento Nº: E/05722/2019
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 20 de mayo de 2019, la entidad ***MULTICANAL IBERICA, S.L.U.,*** con NIF ***B81367773,*** notificó a esta AEPD una violación de la seguridad de los datos personales de sus clientes que están siendo tratados desde el sitio web www.canalcocina.com y de los que es responsable. Respecto de la tipología de los datos cuya seguridad ha sido vulnerada figuran el nombre de usuario, contraseña de acceso al sitio web, nombre real del usuario, dirección de correo electrónico, y operador de Televisión. En su caso, figuran también otros datos personales que algunos clientes aportan de forma voluntaria, como son la fotografía de perfil, dirección, fecha de nacimiento y género.

La entidad manifiesta que el motivo de la vulneración de la seguridad en el tratamiento de los datos personales de sus clientes se debió a un ataque utilizando la técnica *sql injection* para obtener las credenciales de acceso al sitio web www.canalcocina.com mediante el cual consiguieron acceso al servidor.

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

ENTIDADES INVESTIGADAS

Durante las actuaciones se han realizado investigaciones a las siguientes entidades:

MULTICANAL IBERICA, S.L.U. con NIF B81367773 con domicilio en C/ Saturno 1 - 28224 Pozuelo de Alarcón (Madrid)

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

- Multicanal Iberia, S.L.U.) pertenece a un grupo internacional de titularidad americana (AMC Networks, Inc.). En la subsanación del incidente, además de un proveedor externo experto en seguridad (Securízame), estuvo involucrado un equipo internacional con personal en Estados Unidos y Reino Unido.

Respecto del informe de la incidencia.

- Aportan copia del informe interno sobre el incidente del que se desprende los puntos que vienen a continuación.

Respecto de la cronología de los hechos

- En la mañana del miércoles 10 de abril de 2019 se detecta una actividad anómala en la web www.canalcocina.es : el equipó de Marketing advierte una publicidad (pop-up) ajena.

- Se comprueban los logs y se sospecha que ha habido una intrusión, si bien únicamente a nivel de CMS (Sistema de Gestión de Contenidos). Se informa según el protocolo habitual, pero no hay indicios de que la intrusión haya afectado a la *máquina* ni, por tanto, a la base de datos de usuarios registrados denominada "Comunidad Canal Cocina". Por ello, en este momento, únicamente se documenta en el Registro de Incidencias (Entrada 1/2019).

- Al día siguiente (jueves 11 de abril), se decide contratar a un proveedor externo para proteger la web (Securízame).

- El viernes 12 de abril. Securízame Inicia su actividad. Simultáneamente, el equipo de seguridad de la información de la matriz del grupo en Estados Unidos recibe un correo electrónico sospechoso, en ruso, que informa de la intrusión. El equipo de Estados Unidos lo comunica al Director de IT de España (en su mañana, esto es, por la tarde en España). Como resultado de esta comunicación, junto con los primeros resultados de la actividad de Securízame, se llega a la certeza de la ocurrencia, así como de su alcance que, contrariamente a lo inicialmente supuesto, también alcanza a *la máquina.* (Entrada 1/2019 B). La web se cierra la tarde del viernes 12 de abril.

- Durante el fin de semana (el 13 v 14 de abril), el equipo español, inglés y americano trabajan conjuntamente en la subsanación de la incidencia de seguridad.

- En el plazo de tres días desde que se tiene certeza sobre el alcance del incidente, se notifica sobre la brecha de seguridad a la Agencia Española de Protección de Datos (el 15 de abril). El 29 de abril se comunica el incidente a los interesados.

- En las mismas fechas del incidente se había puesto en marcha un proceso de negocio en relación con la web: dado que el modelo participativo requería una moderación editorial continuada muy exigente, ya desde el año anterior se procuraba la migración de los usuarios de la Comunidad Canal Cocina a otro modelo de tratamiento de mera suscripción, con el mismo y compatible fin de fidelización (denominado "Club"), sin registro de usuario ni posibilidad de insertar contenidos en la web. En estas fechas todavía subsistían los dos modelos en paralelo, por lo que se decide aprovechar el incidente para implementar el cambio, de modo que la web, en su nueva configuración, se implementara ya debidamente securizada y protegida.

Respecto de las causas que han hecho posible la incidencia

- El intruso se hace con la cuenta del administrador para perpetrar un ataque denominado *sql Injection* que explota una vulnerabilidad en la tecnología de la web (MYSQL, PHP, Debian Linux) y un fallo del sistema de seguridad *CloudFare*, servicio que debiera haber detectado y repelido la intrusión, pero que no funcionó contra este ataque.

Respecto de la categoría de los datos afectados

- La base de datos de usuarios registrados de la web Comunidad Canal Cocina se componía de 137.725 individuos. No puede confirmarse que todos estos usuarios hayan sido afectados en la práctica. De hecho, a la luz de la escasa respuesta de los usuarios a la comunicación que remitimos para informarles del incidente de seguridad (sólo hubo 148 interacciones de usuarios), es esperable que el impacto real en cuanto a número de usuarios sea muy inferior.

- Tipología de datos afectados:

Los datos que los usuarios proveían eran:

• Con carácter necesario: Nombre de usuario, contraseña, correo electrónico, nombre real, y operador de TV.

• Con carácter voluntario: Fotografía de perfil (no necesariamente del usuario), dirección, fecha de nacimiento y género (masculino o femenino).

El nombre de usuario y la fotografía de perfil eran públicos en la web.

Respecto de las acciones tomadas para minimizar la incidencia

- Durante los días 13 y 14 de abril y en adelante, se tomaron esencialmente las siguientes medidas: (i) la remoción de la base de datos de la web, (ii) su indisponibilidad y bloqueo hasta su securización, así como (iii) la comunicación a los usuarios. La comunicación a los usuarios se realizó por email en fecha 29 de abril de 2019.

Como respuesta a la comunicación a los usuarios, se atendieron las siguientes solicitudes:

- Supresión de datos: 81
- Información adicional: 44
- Derecho de acceso: 8
- Rectificación: 1 (cambio de email)
- Portabilidad: 1 (un usuario, en relación con sus contenidos)
- Agradecimiento por la comunicación: 2

Respecto de la resolución final de la incidencia

- Durante los días 13 y 14 de abril y en adelante, se tomaron esencialmente las siguientes acciones: (i) la implementación de la web segura y bajo nueva configuración, sin requerir el registro; (ii) la implementación de medidas de verificación de los controles aplicados (scan); y (iii) se previó la supresión de los datos (previo su bloqueo) tras un periodo de 3 meses, por si se recibieran solicitudes adicionales de usuarios.

Respecto de la utilización por terceros de los datos personales obtenidos a través del ataque

- El análisis realizado no resultó plenamente concluyente sobre el hecho de si la base de datos se vio o no efectivamente comprometida (esto es, si, además de quedar potencialmente expuesta, los datos -o parte de ellos- fueron extraídos en la práctica). El breve lapso de tiempo de permanencia en el sistema, así como el escaso flujo de datos al exterior, parece sugerir que no fue el caso.

- No tienen constancia a la fecha de filtración pública ni han recibido ninguna reclamación en este sentido, ni por parte de autoridades ni por parte de los interesados.

Respecto de la seguridad:

- Aportan copia del del Registro de Actividad de los tratamientos donde se ha producido el ciberataque.

- Aportan matriz de análisis básico de riesgos que indica un nivel residual de riesgo bajo, por lo que no se precisa evaluación de impacto.

- Aportan copia del procedimiento establecido ante brechas de seguridad, tanto de la versión actual como de la anterior, que estaba en vigor a la fecha de incidente.

- Aportan copia de la Política de Seguridad de IT del grupo AMC Networks (actualmente en proceso de actualización) y la Política específica adoptada con ocasión de la entrada en vigor del Reglamento General de Protección de Datos.

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, la entidad investigada ha informado de las investigaciones internas realizadas y resultado de las mismas.

Hay que destacar del análisis realizado la detección del método de intrusión utilizado, *sql inyection*, 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 debió detectarlo y repelerlo, pero que no funcionó de forma adecuada.

Añadir también, que tras la comunicación a los usuarios (137.725 usuarios) de la incidencia de seguridad sólo han respondido 148, por lo que el impacto ha sido mínimo.

Tampoco consta que los datos personales de los usuarios hayan sido tratados por terceros sino que quedaron expuestos a dicho riesgo sin que se haya materializado al no tener constancia de su publicación ni haber recibido reclamación en este sentido ni por los usuarios afectados ni por parte de las autoridades públicas.

III

Por lo tanto, se ha acreditado que la actuación de la entidad investigada en calidad de responsable del tratamiento y entidad informante de la quiebra de seguridad ha subsanado la incidencia con la implantación de las medidas de seguridad adecuadas y reconfiguración del sistema de información al objeto de evitar en el futuro la repetición de situaciones similares resultando adecuadas las actuaciones con la normativa sobre protección de datos personales.

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 ***MULTICANAL IBERICA, S.L.U.*** *con* ***NIF B81367773*** *y domicilio en* ***C/ Saturno 1, 28224 Pozuelo de Alarcón (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