- **Procedimiento Nº: E/01562/2020**

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 como consecuencia de la recepción de un escrito de notificación de brecha de seguridad de los datos personales remitido por SHARING MUVING, S.L. (en adelante, MUVING), entidad cuyo objeto social es el <Alquiler de motos eléctricas por minutos a través de una app> y sitio web <***URL.1** >, en el que informan a la Agencia Española de Protección de Datos de que han detectado de una brecha de seguridad de datos personales como consecuencia de la recepción de notificaciones de sus clientes acerca de un correo electrónico recibido desde MUVING solicitándoles actualizar sus datos bancarios.

El 3 de febrero a las 12.00h CET (hora estándar de Europa Central, UTC+1), MUVING identificó que se estaban utilizando dos cuentas de correo electrónico de trabajadores del Departamento de Atención al Cliente para “inyectar” minutos gratis en la App de MUVING a determinados clientes.

Posteriormente, el sábado 8 de febrero de 2020 a las 16.40h CET, MUVING detectó, que el 8 de febrero de 2020 a las 14.27h CET se envió desde la cuenta de correo electrónico <***EMAIL.1**> un email fraudulento a 25.000 clientes solicitándoles una actualización de sus datos de pago.

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 notificación, teniendo conocimiento de los siguientes extremos:

ANTECEDENTES

Fecha de notificación de la brecha de seguridad de datos personales: 11/02/2020.

ENTIDADES INVESTIGADAS

SHARING MUVING SL, con NIF B72327000 y con domicilio en c/ Fuentebravía, Edificio Hindustan, 7, piso 1, puerta 1, 11500 Puerto de Santa María, Cádiz.

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

MUVING aporta junto a la notificación de la brecha de seguridad de datos personales un informe del que se desprende lo siguiente:

1. Respecto de la cronología de los hechos

El 3 de febrero a las 12.00 CET, MUVING identificó que se estaban utilizando dos cuentas de correo electrónico de trabajadores del departamento de atención al cliente para inyectar minutos de consumo gratis en la App de MUVING a determinados clientes. En el mismo momento en que se tuvo conocimiento de los hechos, MUVING comenzó a investigar la situación y descubrió un fallo de seguridad en sus sistemas por el cual se permitía inyectar código malicioso, lo que hacía que se pudiesen robar las cookies de acceso a los sistemas de MUVING de determinados trabajadores de MUVING.

El jueves 5 de febrero de 2020 a las 16.45 CET, MUVING corrigió el fallo de seguridad protegiendo el *backend* para evitar nuevas inserciones de código en cualquiera de los campos de las APIs públicas.

Posteriormente, el sábado 8 de febrero de 2020 a las 16.40 CET, MUVING detectó que se había enviado desde la cuenta de correo <******EMAIL.1***> un email fraudulento a 25.000 clientes de la base de datos de MUVING, solicitándoles una actualización de los datos de su tarjeta de crédito. El correo electrónico tenía el siguiente contenido: *"Hola [NOMBRE DEL CLIENTE]: Necesitamos que vuelvas a introducir tu información de pago para seguir disfrutando de MUVING. ACTUALIZAR INFORMACIÓN".*

Al pulsar el botón "ACTUALIZAR INFORMACIÓN" se redirigía al usuario al dominio <******DOMINIO.1***>, en el que se solicitan datos de su tarjeta, en concreto: número de tarjeta, fecha de caducidad y código CVV.

El día 8 de febrero de 2020 a las 16:55, y tras analizar que los mails proceden de la cuenta en Postmarkapp, se decide revocar la *API Key* y generar una nueva, ya que debido a la vulnerabilidad detectada el 3 de febrero de 2020, pudo obtener este dato antes de que corrigiese el incidente de seguridad el 5 de febrero.

2. Respecto al número y tipología de los datos afectados

El ataque se realizó contra la base de datos de MUVING tomando el control de la aplicación de mensajería. Los datos afectados son de tipo básico: nombre, apellidos y correo electrónico.

En los casos en los que los afectados (clientes de MUVING) facilitaran sus datos bancarios directamente en el portal fraudulento (<******DOMINIO.1***>), sus datos bancarios quedaron expuestos al atacante.

El correo electrónico malicioso fue enviado a 25.000 clientes de MUVING, de los cuales 9000 abrieron el correo electrónico y unos 1000 cliquearon en el enlace que los redirigía a la web fraudulenta en la que debían actualizar los datos de su tarjeta bancaria.

3. Medidas tomadas para solucionarla brecha y minimizar el impacto sobre los afectados

MUVING, según manifiestan, ha iniciado de manera inmediata una revisión exhaustiva de la seguridad de sus sistemas, ha identificado el origen de la brecha y solucionado aquella vulnerabilidad de seguridad.

Asimismo, se han tomado medidas para evitar que esto vuelva a ocurrir, protegiendo el *backend* para evitar nuevas inserciones de código malicioso en cualquiera de los campos de las APIs públicas.

Además, MUVING está examinando todos los demás aspectos en los que podrían mejorar la seguridad de su plataforma y está reforzando la forma de autenticación de usuarios de la plataforma para detectar previamente cualquier intento de ataque, así como poder neutralizarlo de forma inmediata. Respecto a este incidente concreto, han identificado la vulnerabilidad e implementado medidas para evitar en el futuro este tipo de ataques.

Al mismo tiempo, se va a realizar una auditoría de seguridad externa para un mejor análisis de la situación actual de los sistemas y corregir aquellos posibles fallos de seguridad que se encuentren.

Se han realizado comunicaciones informativas en aras de advertir a los interesados del incidente y establecer recomendaciones para mitigar los posibles perjuicios sufridos. El 8 de febrero de 2020 se envió una comunicación a todos clientes registrados (250.000 personas) y el 13 de febrero de 2020 una comunicación especial a los usuarios que se han interesado por el incidente (aproximadamente unos 230 clientes).

4. Respecto al uso de datos por terceros

MUVING no dispone de evidencias que acrediten la utilización por terceros de datos personales obtenidos a través del ataque. Sí ha tenido constancia, a través de las comunicaciones de algunos de sus clientes, de que se les envió un correo electrónico a través de una cuenta de correo electrónico que simulaba ser de MUVING, solicitándoles sus datos bancarios. Al respecto, puede concluirse que los atacantes pudieron tener acceso a información que los propios clientes de MUVING le proporcionaron, como consecuencia de los datos solicitados a los mismos haciéndose pasar por MUVING.

5. Respecto de las medidas de seguridad implantadas con anterioridad la brecha

- Aportan copia del registro de tratamientos y análisis de riesgos relativo a los tratamientos afectados por el ciberataque.
- Aportan copia de la evaluación de impacto de privacidad del tratamiento “gestión de clientes”.
- Aportan copia del procedimiento de notificación y gestión de brechas de seguridad.
- Aportan Política de seguridad de MUVING para los tratamientos de datos relativos a clientes.

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 una brecha 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 a la base de datos del sistema de información de MUVING.

De las actuaciones de investigación se desprende que MUVING disponía de razonables medidas técnicas y organizativas preventivas a fin de evitar este tipo de incidencias y acordes con el nivel de riesgo.

Asimismo, MUVING disponía de protocolos de actuación para afrontar un incidente como el ahora analizado, lo que ha permitido de forma diligente la identificación y corrección de la brecha, análisis y clasificación del supuesto incidente de seguridad de datos personales así como la diligente reacción ante la misma al objeto de notificar, minimizar el impacto, comunicar a los afectados e implementar nuevas medidas razonables y proporcionales para evitar que se repita la supuesta incidencia en el futuro a través de la puesta en marcha y ejecución efectiva de un plan de actuación.

En consecuencia, MUVING disponía de forma previa de medidas técnicas y organizativas razonables y proporcionales en función del nivel de riesgo para evitar este tipo de incidencia.

No constan reclamaciones ante esta AEPD por parte de los clientes afectados.

No obstante, se recomienda la realización de un informe final sobre la brecha de seguridad notificada. 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, en el caso concreto consta que la actuación de MUVING, como entidad responsable del tratamiento, ha sido razonable y proporcional 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 SHARING MUVING, S.L., con NIF B72327000 y con domicilio en c/ Fuentebravía, Edificio Hindustan, 7, piso 1, puerta 1, 11500 Puerto de Santa María, Cádiz.

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