- **Procedimiento N.º: E/06707/2020**

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 brecha de seguridad de datos personales remitido por 2GETHER MONEY MANAGEMENT, SL (en adelante 2GETHER), en el que informan a la Agencia Española de Protección de Datos que, con fecha ******FECHA.1***, se detecta una brecha indicándose que "*se tiene constancia de que los atacantes, a través del equipo de un técnico de la empresa, han logrado acceder a bases de datos de la compañía, realizando consultas a tablas con datos personales de usuarios.*"

Declaran la afectación de datos identificativos y de contacto, credenciales de acceso, datos económicos o financieros y de localización.

En la notificación inicial indican un número aproximado de personas afectadas de 45.000, aumentándose en la notificación adicional a 111.182. Manifiestan que la brecha se ha comunicado a los afectados, aportando copia de la notificación (español e inglés).

Asimismo, aportan copia de la denuncia interpuesta ante la Guardia Civil, copia de las actas notariales haciendo constar los procesos de obtención de datos del servidor y de copias de los datos, una vez sufrido el ataque.

En fecha 7 de agosto de 2020, se reciben tres reclamaciones de tres afectados en las que declaran haber recibido ese mismo día, un correo electrónico de 2GETHER, notificando la brecha de seguridad sufrida, su impacto y las medidas adoptadas hasta ese momento. Aportan copia del correo recibido.

SEGUNDO: En fecha 11 de agosto de 2020, la Directora de la Agencia Española de Protección de Datos ordena a la Subdirección General de Inspección de Datos que valore la necesidad de realizar las oportunas investigaciones previas con el fin de determinar una posible vulneración de la normativa de protección de datos, teniendo conocimiento de los siguientes extremos:

Fecha de notificación de la brecha de seguridad de datos personales: ******FECHA.2*** (inicial) y ******FECHA.3*** (adicional).

ENTIDAD INVESTIGADA:

2GETHER MONEY MANAGEMENT, S.L.

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN:

Respecto de la empresa:

Según AXESOR la entidad investigada es una PYME con 11 empleados y un capital social de 859.177 euros.

Respecto de los datos afectados:

Los tipos de datos afectados declarados son:

- Datos básicos.
- DNI, NIE y/o pasaporte.
- Credenciales de acceso o identificación.
- Datos de contacto.
- Datos económicos o financieros.
- Datos de localización.

Existen un total de 111.182 personas afectadas, a las que la entidad declara haber informado aportando copia de la notificación (español e inglés) que coincide con la aportada por los tres reclamantes ante esta Agencia.

Con fecha 18/08/2020 se solicitó información a la entidad 2GETHER habiendo manifestado los representantes de la entidad lo siguiente:

Respecto de la cronología de los hechos y las Medidas de minimización del impacto de la brecha:

"Gracias a uno de los sistemas de monitorización, la Compañía pudo detectar, el viernes 31 de julio sobre las 17:00h, un descuadre en los balances de las cuentas. Inmediatamente se puso en conocimiento del Presidente Ejecutivo la situación, desplegando las acciones de información y comunicación necesarias, entre otras, alertar al Director de Tecnología.

Inmediatamente se iniciaron las labores de investigación para determinar las causas de la incidencia y, ante la sospecha de un acceso no autorizado, se procedió a actuar, tomando las medidas de protección necesarias. Durante las actuaciones posteriores, el Responsable de Sistemas junto con el Director de Tecnología, son expulsados de la VPN por lo que se confirma la hipótesis de estar sufriendo un ataque por varios flancos.

Se procedió a comprobar los registros de la base de datos con las credenciales del técnico de soporte y efectivamente se encontraron diferentes accesos y modificaciones en datos de usuario que el técnico confirmó no haber realizado. Se inhabilitaron, entonces, todas las credenciales de dicho empleado y se bloqueó el acceso a la APP de 2gether con severidad alta para todos aquellos usuarios a los que los atacantes habían modificado algún dato.

A las 18:00h, el Responsable de Sistemas, logra recuperar el control de la VPN y de este momento hasta las 19:00h, restringe el acceso habilitando sólo las direcciones IP de 2gether, revocando el acceso a cualquier otra IP y desactivando todos los inicios de sesión de los clientes de 2gether, y expulsando a todo el mundo de la APP, incluidos los atacantes.

A partir de este momento se inician los trabajos de evaluación de daños, al mismo tiempo que se solicita ayuda para la resolución del incidente al CERTSI (19:44h).

Alrededor de las 21:00h se conformó un Comité de Crisis compuesto por el Consejo Ejecutivo, el Director de Tecnología, el Responsable de Sistemas y el Director de Seguridad.

La organización del Comité de Crisis se realizó mediante un slack privado de la Compañía, un Drive compartido y una ubicación física desde la que gestionar la crisis. El sábado 1 de agosto se reunió en Madrid dicho Comité y se empezó a trabajar en tres frentes:

1. Se tomó la decisión de la contratación de los servicios profesionales de una empresa experta en gestión de crisis y de una firma de servicios forenses para analizar con detalle el ataque y disponer de la máxima información para esclarecer los hechos, interponer la denuncia y las notificaciones correspondientes y rápidamente poner medidas de contención.

2. Garantizar que los servidores de 2gether no habían estado, ni estaban comprometidos de cara a restablecer la operativa cuanto antes.

3. Analizar los daños para comunicar lo antes posible y con la mayor información posible el incidente a la comunidad de 2gether.

Posteriormente, los días 1 y 2 de agosto, el departamento técnico de 2gether estuvo trabajando en la recuperación de los sistemas y rehaciendo los saldos contables de la Compañía de cara a conocer con detalle el importe sustraído. De esta primera valoración se obtuvo, con bastante precisión, el importe sustraído de los balances de 2gether.

Adicionalmente, entre otros aspectos de gestión de la crisis, se iniciaron las acciones necesarias por parte del Comité de Dirección de la empresa para buscar capital con la finalidad de reforzar la Compañía y aumentar los niveles de seguridad.

Durante los días siguientes el equipo de sistemas y back-end trabajaron intensamente para reabrir la aplicación y restablecer todos los servicios con total seguridad y lo más pronto posible. En primer lugar, se procedió a regenerar todas las claves de la Compañía de usuarios, servicios y sistemas. Inicialmente, se procedió a abrir el acceso de la VPN, exclusivamente al responsable de sistemas y al CTO de 2gether. Además, se reforzaron todos los sistemas de prevención, defensa, monitorización y respuesta, tanto de servidores como de todas las estaciones de trabajo de todos los empleados. Para ello se instalaron el software de seguridad ******SOFTWARE.1*** *y realizamos una auditoría de todos los componentes de nuestro entorno para confirmar que no existían posibles puertas traseras o programas instalados no autorizados. Se reconfiguraron todos los sistemas de la plataforma, tanto los que estuvieron expuestos al ataque como los que no lo estuvieron. Se reconfiguraron todas las conexiones y configuraciones de los diferentes componentes, microservicios y bases de datos. Fue un trabajo arduo e intenso que demoró la apertura de la plataforma, siendo la seguridad la principal prioridad. El miércoles 5 de agosto a las 14:00h, una vez recopilada toda la información sobre el robo, acudimos al Grupo de Delitos Telemáticos de la UCO e interpusimos la denuncia correspondiente para iniciar la investigación. Posteriormente, sobre las 18:00h se abrió de nuevo la aplicación a todos los usuarios."*

La notificación de brecha a los afectados la realizan con más de 72 horas alegando en la notificación de brecha que "*fue necesario llevar a cabo una extracción de datos forense del equipo comprometido y de los registros del cloud y el correspondiente peritaje ante notario, lo que ralentizó el proceso debido a la falta de disponibilidad de los no-*

tarios. siendo un hecho relevante el que el incidente de seguridad haya sido perpetrado al inicio del finde semana en el que coinciden el fin de vacaciones de las personas que se han ido en julio y el inicio de las que se van en agosto.
Respecto de las causas que hicieron posible la brecha:

*"El *****FECHA.1**, los atacantes accedieron a través del equipo de uno de los técnicos informáticos de la organización a diversos recursos de la nube de Amazon. A través de dicho acceso se realizaron una serie de modificaciones en varias cuentas de clientes, se entiende que para poder realizar las transferencias posteriores.*

Los atacantes actuaron de forma hábil, haciendo uso del equipo del técnico como cobertura para que sus acciones pasarán desapercibidas y deshabilitando los controles de seguridad existentes (como por ejemplo el doble factor de autenticación desplegado para el acceso a la VPN). Este usuario contaba con permisos de sistemas para llevar a cabo las funciones asignadas dentro de la Compañía.

Como parte de su proceso de ataque, los atacantes tuvieron acceso a varias tablas de las bases de datos de la Organización que contienen datos de carácter personal, constituyendo estas acciones una brecha de seguridad según lo indicado por el RGPD.

El análisis forense del equipo ha permitido determinar que estaba comprometido por el malware, DarkGate, integrando un módulo de acceso remoto o RAT denominado Nanocore.

Con ambas piezas de malware los atacantes tenían el control completo del mismo, usándolo como proxy para realizar sus operaciones.

Dicho malware fue desplegado en el sistema a través de un script en Visual Basic Script, que se hizo pasar por un supuesto fichero de descarga de un Torrent y fue ejecutado por el propio técnico en enero de 2020. Los atacantes activaron este malware a lo largo de la segunda quincena de julio, provocando el incidente de seguridad.

*La Compañía estaba en proceso de adquirir un software de *****SOFTWARE.1** para su implantación y sustitución de las medidas de antivirus de las que se disponían en el momento del ataque. La adquisición de este software *****SOFTWARE.1**, tomó más tiempo del esperado por los problemas que sufrió la Compañía a nivel operativo, causadas por el Coronavirus.*

Uno de los problemas operativos que se produjeron, sumado al del teletrabajo y a las causas mencionadas anteriormente, fue la dificultad de encontrar un técnico con un perfil de sistemas adecuado y con los conocimientos de las arquitecturas de seguridad que utiliza la Compañía."

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

"La resolución final de la brecha se realiza cuando el equipo técnico de la Compañía, tras la contención inicial del incidente y su posterior análisis, identifica las acciones realizadas por los atacantes y establece las acciones necesarias para volver a levantar al sistema de una forma segura.

Dicho análisis se realiza desde el sábado, día 1 de agosto, al lunes 3 de agosto, incluido, y traza las acciones realizadas por los atacantes en los sistemas."

Los representantes de la entidad enumeran una serie de acciones tomadas que involucran, entre otras, el despliegue de nuevas máquinas y configuraciones, acciones

sobre la VPN, accesos y credenciales de diferentes servicios, nuevas API, extracción de evidencias por parte del perito informático en presencia del Notario, análisis forense de la imagen extraída del equipo comprometido y del impacto de la brecha, normalización usuarios afectados, bases de datos, instalación de herramientas de detección, etc.

Respecto de la posible utilización por terceros de los datos personales obtenidos a través de la brecha

*"2gether encargó a la consultora de riesgos globales, *****CONSULTORA.1**, la realización de un servicio de monitorización o de vigilancia digital de marca y posibles activos en la Deep y Dark Net (DDN).*

*Desde el *****FECHA.1** y los 10 días siguientes, se han utilizado métodos no intrusivos de consultas para realizar un análisis de la presencia digital de 2gether en algunas fuentes de información abiertas, pero principalmente en la Deepweb, Darknet, Tor, IRC, Zero net y Paste Sites.*

*De las investigaciones realizadas se desprende que la marca 2gether, a fecha de emisión del informe de *****CONSULTORA.1**, no tiene menciones o exposiciones de riesgo en la DDN, de lo que se deduce que no existe evidencia de que se hayan puesto a la venta o utilizados datos personales extraídos en la brecha de seguridad."*

Respecto de las medidas de seguridad implantadas con anterioridad la brecha:

Se ha requerido a la entidad para que aporte lo siguiente respecto de la seguridad de los tratamientos de datos personales con anterioridad a la brecha:

7-1. Copia del Registro de Actividad de los tratamientos donde se ha producido la brecha notificada.

7-2. Documentación acreditativa del Análisis de Riesgo que ha conllevado la implantación de las medidas de seguridad y copia de las Evaluaciones de Impacto, en su caso, de los tratamientos donde se ha producido la brecha notificada.

7-3. Detallar aquellas medidas técnicas y organizativas adoptadas para garantizar un nivel de seguridad adecuado a los riesgos detectados en los tratamientos afectados por la brecha.

7-4. Política de seguridad adoptada por la entidad para los tratamientos de datos en los que se ha producido la brecha notificada.

7-5. Información sobre si existe un procedimiento general escrito en la entidad ante la posible ocurrencia de brechas. Copia de este, en caso afirmativo.

7-6. Información sobre la realización de auditorías periódicas. Último informe de auditoría de seguridad de los sistemas de información objeto de la brecha de seguridad.

7-7. En su caso, códigos de conducta a los que están adheridos o certificaciones obtenidas en el marco de los arts. 40 y 42 del RGPD.

Los representantes de la entidad han aportado:

- Copia del Registro de Actividad de los tratamientos (RAT) donde se ha producido la brecha notificada.
- Copia del último análisis de riesgos (AR) realizado por la Compañía (finales de 2019). Declaran que dicho análisis se utilizó también para solicitar al Banco de España la autorización como Entidad de Dinero Electrónico (2gether EDE), sociedad que formará parte del grupo 2gether. Incluye AR asociado a los datos de carácter personal.

  Declaran que utilizan ISO 31000 como estándar internacional para el proceso de gestión del riesgo, y para el catálogo de amenazas el informe ENISA Threat Landscape Report 2018.
- Copia de las medidas técnicas y organizativas adoptadas.
- Copia de la Política de seguridad de la compañía.
- Copia del procedimiento interno a seguir en caso de brechas de seguridad.

No se observa en la documentación aportada normas internas de cumplimiento para los empleados con relación a la utilización de los sistemas informáticos de la entidad. No se aportan auditorias de protección de datos. Sí se aporta un informe de una auditoria especifica de seguridad (“*pen test”* cuyo objeto es la búsqueda de vulnerabilidades que pueden ser explotadas por un atacante). No se aportan códigos de conducta ni certificados.

Información respecto del motivo por el cual las medidas de seguridad implantadas no han impedido el incidente de seguridad:

“El principal motivo por el que las medidas de seguridad implementadas no han impedido el incidente de seguridad, se ha debido a que una vez el equipo del técnico había sido comprometido y los atacantes conocían sus contraseñas, todas las acciones de los atacantes se realizaron suplantando la identidad de éste e incluso utilizando su equipo como proxy.

El antivirus desplegado no contaba con medidas de detección y respuestas avanzadas como es un ******SOFTWARE.1****, por lo que no se pudo impedir la infección ni el posterior uso que se hizo del malware, que instaló contramedidas que incluso dificultaron la extracción de la memoria por parte del perito ante el notario.”*

Medidas técnicas y organizativas adoptadas para evitar, en lo posible, incidentes de seguridad como el sucedido:

“Como primera medida para evitar un nuevo incidente de seguridad, se ha desplegado un ******SOFTWARE.1*** *y contratado con la misma compañía, un servicio de análisis, además de haberse desplegado de nuevo la infraestructura, aunque ésta no se hubiese visto comprometida.*

Tras este incidente, la Compañía ha convocado al Director de Seguridad al Comité Ejecutivo de forma recurrente y le ha pedido que acelere la creación del framework de ciberseguridad, siendo estas las acciones acordadas tras la asistencia del Director de Seguridad a dicho comité:

- *Personas: se ha hecho hincapié en la importancia de las personas como primera medida de defensa y se ha pedido a todo el mundo que extremen las precauciones y se está buscando un curso de concienciación en ciberseguridad para toda la plantilla.*

- *Credenciales y accesos: se han regenerado todas las claves de la compañía de usuarios, servicios y sistemas (correo electrónico, VPN, aplicaciones, bases de datos, API a servicios externos, comunicación entre microservicios)*
- *Infraestructura:*

o *Tras el despliegue del *****SOFTWARE.1**, se van a configurar políticas en función de los colectivos que trabajan en la Compañía y su nivel de acceso a datos y activos y se va a formar al personal técnico que ha de monitorizar la herramienta.*

o *Se está analizando reducir la superficie de ataque eliminando el **XXXXXXXX** del parqué de equipos de la Compañía, quedando **XXXXXXXX, XXXXXXXX** y **XXXXXXXX.***

- *Aplicaciones: pese a no haber roto o vulnerado el sistema, se ha solicitado una **XXXXXXXX** a **XXXXXXXX** para mejorar las capacidades de desarrollo seguro de la Compañía."*

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 de confidencialidad, integridad y de disponibilidad, como consecuencia de un ataque a través del equipo de uno de los técnicos informáticos, lo que sirvió de cobertura para que sus acciones pasaran desapercibidas, y de esta manera, deshabilitar los controles de seguridad existentes, lo que derivó en el acceso a bases de datos de la compañía, realizando consultas a tablas con datos personales de los usuarios. Se han visto afectados datos básicos, D.N.I., N.I.E. y/o pasaporte, credenciales de acceso o identificación, datos de contacto, datos económico-financieros y de localización de 111.182 usuarios.

De las actuaciones de investigación se desprende que, con anterioridad a la brecha de seguridad, la entidad investigada disponía de medidas de seguridad razonables en función de los posibles riesgos estimados. Aporta copia del Registro de Actividad de los tratamientos donde se ha producido la brecha notificada, copia del último análisis de riesgos realizado, copia de las medidas técnicas y organizativas adoptadas, copia de la Política de Seguridad y del procedimiento interno a seguir en caso de brechas de seguridad.

Asimismo, contaba con protocolos de actuación para afrontar un incidente como el ahora analizado, lo que ha permitido de forma diligente la identificación, análisis y clasificación de la brecha de seguridad de datos personales así como la diligente reacción ante la misma al objeto de 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 el Delegado de Protección de Datos.

En consecuencia, se debe concluir que la entidad investigada disponía de medidas técnicas y organizativas razonables para evitar este tipo de incidencia y que al resultar insuficientes han sido actualizadas de forma diligente. Por último, se recomienda elaborar un Informe Final sobre la trazabilidad del suceso y su análisis valorativo, en particular, en cuanto al impacto final. 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.

III

A la vista de las actuaciones practicadas, se ha acreditado que la actuación de la entidad investigada 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 2GETHER MONEY MANAGEMENT, S.L.

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.

940-0419

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