- **Procedimiento Nº: E/01150/2020**

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 los datos personales remitido por ORANGE ESPAÑA VIRTUAL, S.L. (en adelante Simyo) en el que informan a la Agencia Española de Protección de Datos que un usuario notificó al Centro de Coordinación de Orange -CERT- una posible vulnerabilidad en un servicio informativo sobre las ventas de Simyo montado sobre un servidor ******SERVIDOR.1*** que se encontraba abierto, lo que permitía el acceso a datos sin necesidad de autenticarse. Simyo tuvo conocimiento de estos hechos el 8 de enero de 2020.

La brecha ha podido afectar a datos básicos, de contacto y económicos financieros de unos 130.000 clientes y en caso de portabilidad de líneas telefónicas, datos de nacionalidad y de identificación de usuario.

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 la brecha de seguridad de datos personales: 10 de enero de 2020.

ENTIDADES INVESTIGADAS

ORANGE ESPAÑA VIRTUAL, S.L., con NIF B85057974 y domicilio en Paseo del Club Deportivo Nº 1, Parque empresarial LA FINCA, Edificio 8, Pozuelo de Alarcón, 28223 Madrid.

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1.- Con fecha 17 de febrero de 2020 se solicitó información a Simyo, y de la respuesta recibida se desprende lo siguiente:

Respecto de los contratos

- Simyo tiene suscrito un contrato marco de prestación de servicios con la compañía Paradigma Digital, S.L. (en adelante Paradigma) para, entre otras actividades, suministro, gestión y mantenimiento de aplicaciones y sistemas informáticos en el entorno de telecomunicaciones. En el contrato figura que, entre las categorías de datos tratados por esta compañía, se encuentran los datos de Clientes, Potenciales Clientes y Contactos del Usuario. (Documento 3. Copia del contrato mencionado de fecha 1 de enero de 2019).

Respecto del sistema ******SERVIDOR.1***

- Las peticiones de usuario llegan a los sistemas de información cifradas y algunas de ellas se almacenan en una base de datos para su posterior análisis mediante *dahborads (herramienta de gestión que monitoriza, analiza y muestra de manera visual los indicadores de rendimiento de marketing on line).* Asimismo, parte de la información que vuelve también se almacena para su posterior análisis.

  Por otro lado, existe una herramienta donde se encuentran configurados una serie de *dashboards* para monitorización de la infraestructura y consulta de métricas de negocio (datos de ventas, errores en las transacciones de usuario, analítica de respuestas, etc.). El acceso a esta herramienta se encuentra protegido con autenticación del propio software y se accede vía web HTTPS (TLS).

- Uno de *dashboards* permite el acceso a un único grafico de la herramienta ******SERVIDOR.1*** (herramienta que permite realizar consultas y descargar datos almacenados para análisis) que muestra el progreso de las ventas diarias. Para poder consultar ese gráfico, es necesario introducir un usuario y una contraseña.

Respecto de la cronología de los hechos

- El día 8 de enero de 2020, el CERT de Simyo recibió una notificación indicando que se encontraban disponibles en Internet, sin necesidad de autenticarse, los registros de algunos de los sistemas de Simyo, especialmente los relativos a los procesos de venta.

  Este mismo día el equipo de seguridad de Simyo notifica, vía correo electrónico, a Paradigma la incidencia y se indica la existencia de una vulnerabilidad por la cual era posible extraer datos de carácter personal sin autenticarse. Por lo que se procede a la parada del servicio afectado y al análisis de los registros de las aplicaciones.

- El día 9 de enero de 2020, después de las investigaciones, se descarta que la incidencia haya sido provocada por una vulnerabilidad en ******SERVIDOR.1***. Se comprueban las direcciones IP y las peticiones de acceso. Se inicia el estudio de los registros de accesos (logs).

  A las 19:00 horas, Simyo informa a Paradigma que un particular ha accedido a los datos y se obtienen los informes que potencialmente han sido descargados que indican el número de tarjetas de crédito descargadas almacenadas en forma de resumen criptográfico.

- El día 10 de enero se investigan las direcciones IP de los accesos a la plataforma y se procede a la notificación a la Agencia Española de Protección de Datos. Se comienza a investigar el motivo por el cual se ha producido una pérdida de autenticación en el acceso a ******SERVIDOR.1***.

- El día 14 de enero se descubre la causa de la pérdida y se finaliza el análisis sobre los accesos a ******SERVIDOR.1*** y los datos descargados

Respecto de las causas que hicieron posible la brecha

- Simyo manifiesta que la causa de la incidencia fue debido a la automatización de la renovación de certificados en servicios web de Simyo, con la finalidad de asegurar que el servicio tuviese los certificados vigentes y actualizados, así como el resto de los parámetros de configuración del servidor.

  A este respecto, Paradigma manifiesta que la causa de la incidencia fue la pérdida de autenticación que permitió el acceso sin contraseña a la herramienta ******SERVIDOR.1***, y con ello la posibilidad de realizar consultas contra una base de datos donde se encontraban una serie de datos de usuarios de Simyo.

- Paradigma manifiesta que la incidencia se debió a un error humano, ocurrido al implantar un proceso automático para mantener actualizado el certificado digital utilizado para cifrar las comunicaciones del servicio (anteriormente la renovación era manual y debía hacerse cada tres meses), que eliminó la autenticación requerida para acceder a los registros.

- Simyo manifiesta que la plataforma web que recoge las transacciones de la web de Simyo estuvo accesible sin mecanismos de autenticación previa desde el 16 de diciembre de 2019, hasta el 8 de enero de 2020.

  En relación con la información disponible en la plataforma, Simyo manifiesta que esta plataforma no refleja registros de clientes sino transacciones realizadas desde la plataforma web que posteriormente son sincronizadas con la plataforma de gestión de clientes. Por ello, son registros individualizados y con información parcial de un cliente. También manifiestan que la información de cuentas bancarias se transmite empleando algoritmos *hash* (mecanismo técnico de cifrado no reversible)

- Paradigma manifiesta que según su investigación la mayor parte de datos descargados fue en el periodo comprendido entre el 6 y el 8 de enero de 2020 y prácticamente toda la información fue descargada por el usuario que notificó la incidencia desde tres direcciones IP.

  Tienen constancia de la descarga de información relativa a unos 130.000 clientes de Simyo. La IP de esta descarga corresponde con el usuario que hizo la notificación de la incidencia a Simyo, el cual aporto alguno de los archivos descargados.

Medidas de minimización del impacto de la brecha

- Se procedió al el apagado del sistema de forma inmediata y se incorporó un mecanismo de autenticación en el servidor web sobre el que se desplegaba la plataforma.

- Se procedió a la revisión de la arquitectura y a la realización de una auditoria técnica para evitar que se pueda provocar un suceso similar.

Respecto de los datos afectados.

- El número de afectados fue de aproximadamente 130.000 clientes (se han calculado a partir de la información sobre tarjetas de crédito que aparecen

en los registros). Aunque incluyen datos incorrectos, datos de personas jurídicas y autónomos además de datos de personas físicas.

- Los datos expuestos corresponden a: nombre y apellidos, número de tarjeta SIM, número de tarjeta SIM portada y operador de origen, número del contrato e *id* de usuario (solo en caso de portabilidad), números de móvil, y datos de la tarjeta de crédito (tipo, titular, fecha de caducidad y resumen criptográfico). Los datos de tarjetas de crédito son las utilizadas para el pago de los servicios.
- Paradigma manifiesta que en ningún momento estuvo expuesta la información completa de la base de datos sino los registros de las operaciones que se realizaron en distintos intervalos de tiempo.
- Paradigma manifiesta que los datos descargados están desestructurados obtenidos en bruto de distintas fuentes.
- Simyo manifiesta que el dominio ******DOMINIO.1*** no es intuitivo, lo que dificulta la posibilidad de ser explotado el fallo por terceros. De igual forma, el dominio no quedó indexado en los buscadores tradicionales, por lo que se minimizan de manera significativa las posibilidades de identificación.
- Simyo manifiesta que no ha comunicado a los clientes afectados, ya que, de manera inmediata, se tomaron medidas de protección, entre ellas el cierre de la plataforma, que mitigaron totalmente el posible impacto para los afectados y garantizaron que ya no había posibilidad de que el riesgo se materializase.
- Simyo ha aportado copia del correo electrónico remitido por la persona que notifico al CERT de Simyo la incidencia en la que consta textualmente *"confirmarles que he procedido al borrado de los archivos que fueron descargados por mi parte con fecha 06/01/2020 y que contenían un conjunto de registros de clientes de Simyo con la finalidad de poner en su conocimiento una vulnerabilidad detectada en el interfaz* ******SERVIDOR.1*** *que soporta el acceso a la web de usuarios. También les confirmo que no he realizado ninguna copia de estos ficheros…*"

<u>Respecto de las medidas de seguridad implantadas con anterioridad la brecha</u>

- Paradigma ha aportado listado de las medidas de seguridad implantadas, entre ellas:
    - o Acceso HTTPS cifrado a todos los servicios web expuestos, incluido ******SERVIDOR.1***).
    - o Cifrado para el tráfico de vuelta hacia Simyo.
    - o Protección de ciertos campos mediante resumen criptográfico.
    - o Sistemas de autenticación *login/password* en los interfaces web.
    - o Comunicaciones con terceros cifradas de cara al exterior.
    - o Cortafuegos.
    - o Existencia de sistema de *backup*, que permite restauración de los distintos componentes en caso de pérdida.

- Protección del tráfico de red
- Gestión de usuarios y roles

- Simyo ha aportado los siguientes documentos:
  - Política de Seguridad de la información del Grupo Orange España
  - Registro de Actividad de Simyo donde consta el tratamiento de "Gestión de Clientes".
  - Análisis de Riesgos y manifiestan que el tratamiento no entraña un alto riesgo para los derechos y libertades de las personas físicas por lo que no han realizado Evaluación de Impacto.
  - Procedimiento de notificación y gestión de incidencias y violaciones de seguridad elaborado por la Oficina del DPO. Estándar de gestión de incidentes de seguridad y Procedimiento de Comunicación de Incidentes de Seguridad elaborados por el Área de Seguridad Global del Grupo Orange.

Respecto de las medias implementadas con posterioridad la brecha

- Se han incluido nuevas medidas para aumentar la seguridad, entre ellas, Sistema de monitorización que incluye vigilancia de diversos activos incluidos el funcionamiento de la autenticación.
- Elaboración de un plan de acción con medidas técnicas y organizativas.

Simyo aporta documental acreditativa y suficiente de las medidas de seguridad anteriores y las implementadas con posterioridad la brecha 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

En el presente caso, consta que con anterioridad a la brecha de seguridad la investigada tenía implantadas medidas de seguridad razonables en función de los posibles riesgos estimados.

Consta también que disponía de registro de actividad y análisis de riesgos según se indica en los antecedentes y se han tomado las acciones posteriores oportunas tanto técnicas como organizativas para evitar la repetición del incidente.

En cuanto al impacto del incidente, cabe señalar que no consta tratamiento posterior de los datos de clientes a los que se ha accedido y se han destruido las descargas utilizadas para informar a la investigada del incidente. En cuanto a los datos relativos a medios de pago, consta que se encontraban encriptados, lo que hace inviable su identificación por terceros.

En consecuencia, acaecido el riesgo de error humano, en lo sucesivo deberá contemplarse riesgos similares y a tal efecto consta que la investigada ha implantado protocolos de monitorización a estos efectos.

La documentación generada de todo el proceso de detección, contención, respuesta y recolección y custodia de evidencias ante una brecha de seguridad de los datos personales es también importante de cara a comunicaciones a las posibles partes interesadas tanto de carácter interno o externo, y para la elaboración de un informe final que tras su análisis permita extraer conclusiones. Este informe final, elaborado 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 de hechos similares.

Por último, no consta hasta la fecha en esta AEPD reclamación por terceros en relación con el incidente analizado.

III

En el presente caso, la actuación de la investigada, como entidad responsable del tratamiento, ha sido diligente y proporcional 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 ORANGE ESPAÑA VIRTUAL, S.L., con NIF B85057974 y domicilio en Paseo del Club Deportivo Nº 1, Parque empresarial LA FINCA, Edificio 8, Pozuelo de Alarcón, 28223 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.

940-0419

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