- **Procedimiento Nº: E/08454/2019**

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 investigación se inician por la recepción de un escrito de notificación de quiebra de seguridad remitido por DCL SUMINISTROS Y SERVICIOS DIGITALES, S.L. (en adelante DCL), con NIF : B74092800, en el que informan a la Agencia Española de Protección de Datos (en adelante AEPD) de que, con fecha 3 de septiembre de 2019, han detectado un ataque *Ransomware* que encriptó toda la información ubicada en un servidor, incluidas las bases de datos y copias de seguridad.

El mismo día 3 de septiembre presentaron denuncia ante la Dirección General de la Policía en el que se pone de manifiesto que los autores del ciberataque dejaron una dirección web de contacto (***EMAIL.1) al objeto de abonar una cantidad en *bitcoin* para su desencriptación y en caso contrario todos los ficheros serían borrados.

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 de quiebra, teniendo conocimiento de los siguientes extremos:

ANTECEDENTES

Fecha de notificación de quiebra: 5 y ampliación el 11 de septiembre de 2019.

ENTIDADES INVESTIGADAS

DCL SUMINISTROS Y SERVICIOS DIGITALES, S.L. con NIF: B74092800 y con domicilio en AVENIDA DE LA ARGENTINA, NUM 132, PTA. 011 - 33213 GIJÓN (ASTURIAS).

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1. Con fecha 26 de septiembre de 2019 se requiere información a DCL y de la respuesta recibida se desprende:

Respecto de la empresa

- DCL tiene como clientes a 25 federaciones deportivas y pone a disposición de cada uno de ellos, el acceso a la página web y al sistema de gestión on-line.

Respecto de la cronología de los hechos. Medidas de minimización de la de la incidencia

- En fecha 3 de septiembre, a las 9:00 horas, DCL recibió un correo de un cliente (federación deportiva) informando de la imposibilidad de acceder a su página web. Al verificar la información indicada por el cliente, DCL detecta que han sido atacados por un virus tipo *ransomware* que ha encriptado todo el contenido del servidor por lo que proceden a apagarlo después de descargar algunos archivos como muestra.

Esa misma mañana reciben más llamadas de clientes informando de la imposibilidad de acceso. DCL les va informando que han sufrido un ataque y están evaluando las consecuencias.

- Al comprobar que no disponían de medios de desencriptación, DCL contacta con los ciberatacantes y empresas del sector especializas con objeto de intentar recuperar la información, así mismo proceden a la denuncia ante la Policía Nacional en Gijón. Y esa misma tarde proceden a informar a todos los clientes de la situación.
- El día 4 de septiembre contactan con la Oficina de Seguridad del Internauta los cuales, después de evaluar los ficheros de muestra, les indican la imposibilidad de la desencriptación.

Este mismo día, DCL contrata un nuevo servidor al considerar que tanto el servidor como la dirección IP utilizada estaban comprometidos. Y por la tarde remiten un correo electrónico a todos sus clientes informando de la evolución del incidente.

- El 5 de septiembre presentan notificación de brecha en la AEPD y ponen en marcha el nuevo servidor con la versión de la aplicación más reciente y la última copia de la base de datos.

Esa misma tarde, contactan con los ciberatacantes, quienes les facilitan una herramienta para desencriptar los archivos. Dicha herramienta genera un código que tenían que remitirles para que les facilitaran el código final de desencriptación de los ficheros, el cual fue enviado el 6 de septiembre.

Inmediatamente se procedió a la desencriptación de los ficheros y trasvasados al nuevo servidor. También se realizó una copia.

Posteriormente dieron de baja al antiguo servidor borrando todos los datos que contenían.

DCL ha aportado copia de los correos intercambiados con los ciberatacantes el día 3 de septiembre de 2019.

Respecto de las causas que hicieron posible la incidencia

- El virus *ransomware* con el que fueron atacados (PHOBOS) utiliza un cifrado para hacer que todos los archivos sean inaccesibles. El

ransomware modifica los nombres de archivo durante el cifrado, agregando la identificación de la víctima, la dirección de correo electrónico de los delincuentes y una extensión de archivo específica a los nombres de archivo originales.

- DCL considera que fueron atacados aleatoriamente por un *robot* que accedía a través de fuerza bruta por el escritorio remoto. El servidor tenía instalado una sesión de Windows con una cuenta activa de administrador a través de la cual accedieron y una vez accedido depositaron el virus que encriptó los archivos dejando el contacto con el ciber secuestrador.

DCL manifiesta que el escritorio remoto utilizado por el administrador de la empresa (*Escritorio remoto de Microsoft*) no tenía restricciones de dirección IP por lo que no rechazo la dirección IP desde la que se produjo el ataque.

Respecto de los datos afectados. Notificación e indexación

- La incidencia ha afectado a los datos de los 25 clientes. Los datos afectados corresponden a los datos de afiliación de los deportistas, técnicos y árbitros junto con la actividad propia de las federaciones que eran sus clientes: tramitación de licencias, partidos, pagos, cobros, resultados, etc..
- DCL manifiesta que aunque no se puede descartar que se haya extraído algún dato del servidor, el tipo de ataque sufrido y el tiempo de acceso del usuario administrador que fue mínimo permite considerar que la intención de los atacantes era la encriptación y pedir un rescate.
- DCL ha aportado copia de los correos electrónicos remitidos a los clientes en fechas 3, 4 5 y 6 de septiembre informando sobre el ataque recibido y las medidas adoptadas hasta la resolución final.

Respecto de las medidas de seguridad implantadas con anterioridad al incidente

DCL considera que, según los análisis realizados, las medidas de seguridad implantadas eran suficientes ya que tienen evidencias de ataques que no llegaron a materializarse. Entre otras, tenían implantadas las siguientes medidas de seguridad:

- Conexiones seguras *https*
- Copias de seguridad diarias.
- Sistemas de disco clonados
- Seguridad del sistema operativo y del software de gestión de la base de datos.
- DCL ha aportado copia del registro de actividades de tratamiento *Gestión de Actividades Deportivas.*

Respecto de las medias implementadas con posterioridad a la incidencia

DCL ha implantado nuevas medidas con dos objetivos: evitar accesos por fuerza bruta y evitar la pérdida de copia 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 una quiebra de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como una posible brecha de disponibilidad, como consecuencia del encriptado de la información residente en el sistema de información de DCL

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

Asimismo, la entidad DCL disponía de protocolos de actuación para afrontar un incidente como el ahora analizado, lo que ha permitido de forma diligente la identificación, 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 e implementar nuevas medias razonables y oportunas 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 por las distintas figuras implicadas como son el responsable del tratamiento y el Delegado de Protección de Datos.

No constan reclamaciones ante esta Agencia de los afectados.

En consecuencia, consta que la entidad DCL disponía de forma previa de medidas técnicas y organizativas razonables, en concreto prevención a ataques mediante el uso de sistemas de *fuerza bruta,* en función del nivel de riesgo para evitar este tipo de incidencia. No obstante, se recomienda la realización de un informe final sobre el incidente notificado. 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 ahora analizada.

III

Por lo tanto, se ha acreditado que la actuación de DCL 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 DCL SUMINISTROS Y SERVICIOS DIGITALES S.L., con NIF : B74092800 y con domicilio en AVENIDA DE LA ARGENTINA, NUM 132, PTA. 011 - 33213 GIJÓN (ASTURIAS).

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