- **Procedimiento Nº: E/08830/2019**

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 inspección se inician por orden de la directora de la Agencia Española de Protección de Datos (en adelante AEPD) de fecha 20/09/2019, tras la recepción de 21 escritos de notificación de quiebra de seguridad de datos personales (y otros cinco recibidos en días posteriores) remitidos por empresas clientes de ACENS TECHNOLOGIES, S.L.U. (en adelante ACENS), con NIF B84948736**,** en el que informan a la AEPD de que han recibido comunicación de ACENS de que se ha producido un ataque de tipo Ransomware sobre sus servidores, dando lugar a la indisponibilidad de estos y los datos que albergan.

ACENS actúa en calidad de encargada del tratamiento de sus clientes como proveedor de servicios *cloud.*

La incidencia fue detectada por ACENS el ******FECHA.1***, y afectó a servidores Windows de ACENS. El incidente está relacionado con el Ramsonware RYUK que provocó el cifrado de ficheros en los servidores afectados.

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: septiembre de 2019

ENTIDADES INVESTIGADAS

ACENS TECHNOLOGIES, S.L.U. con NIF B84948736 con domicilio en C/ San Rafael, 14 - 28108 ALCOBENDAS (MADRID).

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1. Con fecha 4 de octubre de 2019 se requiere información a ACENS y de la respuesta recibida con fecha 15 de octubre de 2019 se desprende:

Respecto de la cronología de los hechos

El incidente se detectó y evolucionó en dos días diferentes:

- 1º Fase:

1.- Con fecha ******FECHA.1*** a las 3:00 horas el malware comenzó su propagación siendo detectado por los sistemas de ACENS. Se contuvo en primera instancia desconectando varios sistemas de gestión interna y bloqueando el acceso a los servidores de control del malware. En este momento no se tenía constancia del número exacto de servidores afectados. Sobre las 9:30h am se lanza un primer aviso a los clientes afectados informándoles sobre la indisponibilidad de los servicios por motivo del ataque de un ransomware, no teniendo más datos en aquellos momentos. Se inician las tareas de recuperación.

Desde las 15:00 hasta las 17:00 se produjo un nuevo intento de expansión del virus que tuvo como consecuencia la infección y perdida del servidor controlador de domino y varias máquinas adicionales.

2.- Con fecha 4 de septiembre se informó al organismo INCIBE sobre la naturaleza del incidente para colaborar activamente en la detección, contención y resolución del incidente.

3.- Durante el día 5 de septiembre continuaron los trabajos de restauración y comunicación con información relevante a los clientes en materia afecta al RGPD en caso de actuar en calidad de responsables de datos que los servidores albergan.

4.- Durante los días 6,7 y 8 de septiembre se avanza en la restauración de los equipos.

- 2º Fase:

1.- Con fecha 9 de septiembre a las 10:00h, después de implementar medidas de monitorización y alerta sobre todas las máquinas del entorno se detectó de nuevo la infección, que fue reactivada durante la noche del día 7 de septiembre, en un número de 50 nuevos servidores. La cifra total en esta fecha era 781 de un total de 1343 servidores de los citados entornos, menos de un 0,5% de los clientes totales de ACENS.

2.- Durante el día 10 de septiembre se realizan tareas de monitorización y observación de la infraestructura.

3.- Con fecha 11 de septiembre se interpone una denuncia ante la Policía Nacional.

4.- Durante los días 12, 13 y 14 se revisan las maquinas afectadas en busca de rastros del ataque, continuando las labores de restauración hasta el día 14, donde se dieron por finalizadas.

Desde la detección del ataque el equipo técnico de ACENS aplicó las medidas necesarias para la contención, así como la desinfección y restauración del entorno. El área de ciberseguridad analizó la infección y malware para detener la propagación y bloquear en la medida de lo posible el ataque. Posteriormente, las labores se centraron en la restauración y recuperación de todos los entornos, finalizando estas tareas con fecha 14 de septiembre de 2019.

Respecto de la categoría de los datos afectados

El incidente de seguridad ha afectado a un total 731 equipos de 347 clientes diferentes, siendo bloqueados y encriptados de manera parcial o total los archivos de esos equipos.

Dado el número de afectados, la naturaleza del ataque y el tipo de servicios que ofrece ACENS, desconocen la tipología de todos y cada uno de los datos afectados.

ACENS como proveedor de servicios de hosting, housing y cloud, ofrece soluciones a empresas de toda índole para almacenar los datos, garantizando una serie de medidas de seguridad técnicas para proteger los mismos, con independencia de si son datos personales o de otro tipo. Es el cliente, en calidad de responsable de los datos que alberga en los diferentes servicios, quien debe determinar qué medidas deben aplicar según la naturaleza de los datos tratados.

ACENS, desconoce la naturaleza de dichos datos, no accediendo a los mismos y siguiendo las instrucciones del responsable según sus necesidades en calidad de encargado de tratamiento.

Respecto a la utilización de datos por terceros

ACENS no tiene ninguna evidencia de que los datos afectados, de tipo personal o no, por el ataque hayan sido difundidos, publicados o utilizados por terceros ajenos.

Los registros que figuran en sus bases de datos relativos a tráfico de datos de salida y entrada durante los días previos al ataque, durante y después no reflejan unas métricas que permitan deducir que se ha producido una extracción de datos por parte de los atacantes, siendo el flujo normal.

Respecto de las acciones tomadas para minimizar la incidencia

La duración total del incidente desde su detección hasta su resolución fue de 12 días, desde el martes ******FECHA.1*** hasta el martes ******FECHA.2***

Entre las medidas realizadas por ACENS para mitigar el impacto del ataque entre los clientes podemos enumerar las siguientes:

• Comunicaciones

Una vez detectado el ataque y tras las primeras horas para determinar el alcance del mismo e identificar a los clientes afectados, desde ACENS se fueron sucediendo varios tipos de comunicaciones:

- Comunicación inicial: Desde las 9:00 horas del ******FECHA.1*** se fueron realizando comunicaciones a los posibles clientes afectados por el ataque, informando sobre la indisponibilidad de los servicios contratados por motivos de seguridad y que aún se disponía de poca información.

- Actualización del estado: a las 12:00 de la mañana de ese mismo día se procedió a actualizar la información disponible indicando que ACENS estaba centrando sus esfuerzos en contener el ataque y restablecer los servicios siempre que fuera seguro para los clientes y la infraestructura.

- Actualización para clientes no afectados por el ataque: a las 16:00 horas del 3 de septiembre se informó a los clientes no afectados por el ataque de que, tras los análisis pertinentes, su infraestructura no parecía afectada, instándoles a revisar sus medidas de seguridad para evitar posibles contagios.

- Comunicaciones con fecha 4 de septiembre: una vez se pudo discernir los diferentes tipos de clientes afectados, se procedió a realizar sobre las 16:30 comunicaciones con diferente contenido en función del alcance del ataque y los efectos sobre los clientes.

- Comunicación de restablecimiento de servicios: con fecha 5 de septiembre, se procedió a informar a las 13:00 horas a los clientes a los que se les había restablecido el servicio tras el ataque *ransomware*.

- Comunicación a clientes infectados con *backup filesystem empresa cloud*: a las 20:43 horas del 5 de septiembre se informó a los clientes con servicios con *backup filesystem empresa cloud* que debían realizar algunos ajustes en sus nuevos servicios para recrear los ajustes del servidor anterior y acceder a las copias de seguridad recuperadas.

- Comunicación Informativa sobre el RGPD: el 5 de septiembre a las 21:30, se procedió a informar a los clientes afectados sobre cómo actuar en caso de brechas de seguridad, facilitándoles la guía de la Agencia Española de Protección de Datos (AEPD): https://www.aepd.es/media/guias/guia-brechas-seguridad.pdf

- Comunicación informativa sobre el RGPD: desde ACENS se procedió a enviar de nuevo la anterior comunicación el 06/09/2019 a las 00:00 horas ya que por un error técnico algunos clientes recibieron comunicaciones anteriores repetidas generando confusión.

- Comunicaciones durante los días 6, 7 y 8 de septiembre 2019: durante estos tres días, ACENS fue notificando de manera constante y paulatina a los clientes a los que se les fue completando la recuperación del *backup.*

- Comunicación tras detectar los sistemas una réplica del ataque: el día 9 de septiembre 2019 se realizaron dos comunicaciones; en primer lugar, a las 15:34 horas se informó del bloqueo de los servicios, y en segunda instancia a las 20:30 horas para notificar del reinicio de estos junto a la instalación de medidas de seguridad como la instalación de tecnología antimalware y junto a recomendaciones de seguridad para que realizasen los clientes.

- Comunicaciones para informar a los clientes del reinicio en su servidor: el día 10 de septiembre 2019 se realizaron dos nuevas comunicaciones a las 20:00 horas indicando el reinicio del servidor para la recuperación de acceso RDP (Escritorio Remoto).

- Comunicación de restablecimiento de servidores: con fecha 11 de septiembre a las 16:10 horas se envió a los clientes la notificación de la recuperación del acceso RDP (Escritorio Remoto)

- Comunicación el 4 de septiembre al organismo INCIBE explicando la naturaleza del ataque durante las 24 primeras horas del incidente, compartiendo información técnica para contenerlo y solventarlo de la manera más rápida posible.

- Denuncia ante la Brigada Central de Investigación Tecnológica de la Unidad de Ciberdelincuencia de la Policía nacional con fecha 11 de septiembre.

Restauración del entorno

Desde la primera hora de martes ******FECHA.1*** (9:00 horas) se comenzaron los contactos con los clientes afectados para la restauración de los servicios. Las tareas consistieron en las siguientes acciones:

- Creación de nuevas máquinas virtuales según configuración de cliente

- Restauración de medios de back-up contratados o disponibles en ACENS

- Solución de problemas de conexión o credenciales puntuales de los clientes

- Apoyo en la configuración de los aplicativos de cliente donde fuera técnicamente posible.

Respecto de la resolución final de la incidencia

Con el objetivo de erradicar el ataque de los sistemas se aplicaron las siguientes medidas de seguridad por parte de ACENS a la vez se realizaban las labores de restauración:

- Reinstalación de los sistemas de gestión bajo demanda. Cambios frecuentes de usuarios/contraseña de administrador de estos sistemas
- Utilización de usuarios administradores locales
- Restricción de navegación
- Centralización y análisis de logs. Este sistema queda completamente implantado y operativo alrededor de las 9:00h am del día 4 de septiembre.
- Despliegue e instalación de software *antimalware* en todos los servidores de clientes de la *plataforma Empresa Cloud* y en algunos de la *plataforma Cloud*, así como en los sistemas de gestión.
- Bloqueo y monitorización de conexiones a los C2 (Servidores de Control o Comand and control) externos sospechosos

De manera complementaria a las medidas anteriormente descritas, ACENS contactó con los principales fabricantes de las plataformas para que ayudaran en el análisis, contención y resolución del incidente.

Asimismo, ACENS, contó con la asistencia de equipos de Ciberseguridad y Forense especialistas en respuesta ante incidentes de seguridad desde el inicio del incidente hasta su resolución. Estos equipos colaboraron activamente en el análisis de los datos telemétricos, artefactos recopilados, así como mecanismos de propagación del virus.

Respecto de seguridad de los tratamientos de datos con anterioridad a la incidencia de seguridad

Para realizar el registro de actividades de tratamiento de datos personales, utilizan la herramienta comercial *Globalsuite,* del proveedor *Audisec*, Seguridad de la Información, S.L., Esta herramienta también se utiliza como herramienta de análisis de riesgos y para la realización de las evaluaciones de impacto.

Aportan la siguiente información exportada de dicha herramienta:

- Actividades de Tratamiento.

- Mapa de Riesgos asociados a los Tratamientos como encargado afectados y sus componentes.

Conclusiones:

No existe en ningún componente asociado a estos tratamientos con un riesgo que exceda del Nivel de Riesgo Admisible (NRA=Medio), por lo que no es necesario realizar ningún plan especial sobre estos componentes.

Aportan copia del procedimiento establecido por ACENS ante una 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

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."*

El artículo 33 del RGPD señala lo siguiente:

"Notificación de una violación de la seguridad de los datos personales a la autoridad de control

1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento."

En el presente caso, consta una quiebra de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como una brecha de disponibilidad,

como consecuencia del encriptado de la información residente en el sistema de información de ACENS, entidad esta que actúa en calidad de encargado del tratamiento de veintiséis entidades responsables del tratamiento que alojan sus respectivos sistemas de información en los servidores de ACENS.

De las actuaciones de investigación se desprende que la entidad ACENS 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 ACENS 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 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. En este sentido, se debe señalar que ACENS, en calidad de encargada del tratamiento, actuó acorde con lo dispuesto en el art 33.2 del RGPD y, a su vez, los responsables conforme lo dispuesto en el art 33.1 del citado reglamento.

No constan reclamaciones ante esta Agencia de personas afectadas.

En consecuencia, consta que la entidad ACENS y las entidades Responsables de los datos afectados por la quiebra de seguridad, disponían de forma previa de medidas técnicas y organizativas razonables en función del nivel de riesgo para evitar este tipo de incidencia. No obstante, se recomienda a todas las entidades afectadas 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 ACENS en calidad de encargada del tratamiento y las otras entidades responsables ha sido acorde y proporcionada 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:

- ACENS TECHNOLOGIES, S.L.U., con NIF B84948736 y con domicilio en C/ San Rafael nº 14, 28108 Alcobendas (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