- **Procedimiento Nº: E/00162/2021**

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: Como consecuencia de la notificación a la División de Innovación Tecnológica de esta Agencia de una brecha de seguridad de datos personales por parte de HEALTH TIME S.L. (en adelante HT) con número de registro de entrada O00007128e2000014685 relativa a ransomware que resulta en la exfiltración de datos personales, se 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

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: 14/12/2020. No obstante, se notificó por primera vez el incidente como brecha de disponibilidad el 26/11/2020.

HT es una empresa especializada en Radiología. Un cliente de la compañía les informa que han accedido a información de la entidad a través de la dark web, a través de escaneos rutinarios que llevan a cabo periódicamente. Indican que han comprobado que hay 438 archivos de HT en la dark web y en la dirección ******URL.1***. Su área TIC sospecha que los datos se pudieran haber sustraído en un ciberataque sufrido el 23 de noviembre de 2020. Manifiestan que han resultado comprometidos los 438 archivos. De ellos 129 contienen datos personales.

En principio se notifica que afecta a datos básicos, identificativos, económicos, empleo y salud, inicialmente de aproximadamente 390 personas. Indican que los afectados serán informados.

Documentación aportada:

- Certificado de empresa de seguridad.

- Denuncia del incidente ante la Policía Nacional.

- Informe de la incidencia.

- Registro de la incidencia.

ENTIDADES INVESTIGADAS

Durante las presentes actuaciones se han investigado las siguientes entidades:

HEALTH TIME, S.L. con NIF B82066002 con domicilio en C/ ORTEGA Y GASSET 25, BAJO - 28006 MADRID (MADRID).

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1.- Mediante conexión a Internet, con fecha 15 de enero de 2021 se intenta el acceso a la URL ***URL.1 no encontrándose datos relacionados con HT.

2.- Solicitada información a HT. De la respuesta recibida y de la documentación aportada en la notificación de brecha se desprende lo siguiente:

Respecto de la cronología de los hechos

Los representantes de HT han indicado que:

- A pesar de que el ciberataque que ha provocado la fuga de datos ocurrió en la madrugada del día 23 al 24 de noviembre 2020, no tienen constancia de dicha fuga de datos hasta el viernes 11 de diciembre de 2020.

(Por error en informe área TIC adjuntado a la notificación dice viernes 9 de diciembre cuando debe ser viernes 11, y sábado 10 diciembre cuando es sábado 12 diciembre):

- Esta brecha, catalogada de disponibilidad al sufrir el cifrado de los datos, fue notificada a la AEPD el 26/11/2020

- En ningún momento durante los días previos al conocimiento de la fuga, obtuvieron indicios que hicieran pensar que había ocurrido dicha fuga. Ni observaron rastros identificables del hecho, ni recibimos por parte del atacante ninguna comunicación o intento de contacto, donde se nos informara de la disponibilidad de los datos por su parte.

- El área de Medios y Transformación Digital del Grupo ***EMPRESA.1, es quien tiene constancia inicial de la existencia de archivos correspondientes a información de HT, en la Dark Web (concretamente en el portal ***PORTAL.1) y se lo notifica el viernes día 9.

- Tras esa notificación, proceden a acceder a dicho portal en la “Dark Web” mediante navegador ***NAVEGADOR.1 y observan que existen 438 ficheros expuestos asociados a su grupo empresarial.

- Descargan dichos documentos y el sábado día 10 los examinan observando que en alguno de los archivos (129) aparecen datos personales de 390 personas.

Respecto de las causas que hicieron posible la brecha

El acceso se produjo a través de un equipo (del Área de Administración) cuyo uso es esporádico y que en el periodo que transcurrió entre que arrancó y recibió las actualizaciones del antivirus fue afectado por el virus CONTI, muy posiblemente a través de un correo infectado. Este equipo tenía acceso a la red interna de la empresa y, entre otros, a la carpeta compartida que almacena los ficheros procedentes de un escáner, que han sido los datos afectados por la brecha.

Medidas de minimización del impacto de la brecha

Han reportado las siguientes actuaciones:

- Viernes 11/12/2020 14,00 H. El área de Medios y Transformación Digital del Grupo ***EMPRESA.1,** informa de la existencia de archivos correspondientes a información de HT, en la Dark Web (concretamente en el portal ***PORTAL.1**). Tras esa notificación, HT procede a acceder a dicho portal en la "Dark Web" mediante navegador ***NAVEGADOR.1** y observan que existen 438 ficheros expuestos asociados a su grupo empresarial.

- Sábado y domingo 12 y 13/12/2020. Se procede al análisis de los 438 archivos publicados detectando que, de estos archivos, 129 archivos son los que contiene datos personales y que afectaban a alrededor de 390 interesados; posteriormente comprueban que existían duplicidades de interesados y que el número de afectados se ha reducido a 260 interesados. Significan que en HT tratan más de 1.700 pacientes diarios.
- 13/12/2020 10,56 H. El DPD de HT informa a la Dirección del análisis de los archivos publicados y de las medidas que desde la óptica del RGPD hay que adoptar como desde la óptica de la Seguridad de la Información. Detallan lo informado.

- 14/12/2021 09,22 H. Se procedió a denunciar los hechos ante la Policía (copia aportada en notificación a la AEPD).

- 14/12/2020 14,00 h. Se procedió a notificar a la AEPD la brecha de confidencialidad.

- 15/12/2020 y siguientes y como establece el Art. 33 y 34 RGPD se procedió a comunicar a los Responsables del Tratamiento (en aquellos tratamientos que actuamos como Encargados del Tratamiento), así como a los interesados la violación de seguridad sobre el tipo de datos que se han hecho públicos. Se aportan modelo de comunicación realizada a interesados y correo de comunicación a Responsables del Tratamiento"

- 15/12/2020 El responsable Área TIC procedió a comunicar a INCIBE el incidente. Se adjunta correos con INCIBE "Comunicación INCIBE"

- Se procedió a denunciar ante el proveedor de servicios al dominio ***URL.1**. Respuesta que el pasado 29 de enero nos llegó (ya aludida anteriormente).

Respecto de los datos afectados.

Tipo de datos afectados:

- Datos identificativos: nombre y apellidos.

- Datos con detalles de empleo: hoja de objetivos de dos empleados.

- Datos económicos: certificado de retenciones de profesionales independientes.

- Datos de la salud: nombre de la prueba realizada en el concepto de las facturas.

Como se ha indicado, de los 438 archivos publicados, 129 archivos contienen datos personales, con 390 interesados. Al existir duplicidades de interesados se reducen a 260 interesados.

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

Los representantes de la entidad han declarado que se ha realizado una aproximación de defensa en profundidad y aumento de la seguridad para la solución de la brecha, consistente en:

- Se han creado reglas de salida denegando todo el tráfico no esencial en los sistemas de seguridad perimetral para evitar la salida de más datos personales de la entidad.

- Se ha aumentado la seguridad de las carpetas compartidas, especialmente las dependientes de sistemas como escáneres e impresoras.

- Se ha revisado la configuración del antivirus de acuerdo con el fabricante.

- Se ha realizado una auditoría de seguridad perimetral de la entidad.

- Se está llevando a cabo en este momento una auditoría de seguridad interna de todas las redes y sedes de la entidad.

Indican también que las autoridades policiales no les han comunicado ninguna información respecto a las investigaciones.

Aportan un certificado de ******EMPRESA.2*** con ***CIF ***CIF.1*** de fecha 10/12/2020 en el que

se lee:

“Después de los análisis realizados entre las fechas 24 y 27 de noviembre, con nuestros técnicos certificados en ******EMPRESA.3*** España comprobando el estado de la implementación, configuración y aplicación de políticas de seguridad, podemos confirmar que las soluciones de seguridad ******EMPRESA.3*** están correctamente instaladas y configuradas en todos los Equipos y Servidores en la empresa HEALTI-I TIME, S.L.

La infección de Ransomware Filecoder,Conti que fue detectada el pasado 24 de noviembre fue aislada y eliminada de manera correcta. Detectando el origen del ataque por Fuerza Bruta y procediendo a su bloqueo e implementación de mejoras de seguridad para que esta no pueda volver a producirse.

El cliente ha implementado todas las recomendaciones realizadas por nuestros desarrolladores. Adicionalmente ha mejorado la Segmentación de la Red y configurado políticas de contraseñas más robustas. Se han creado nuevos usuarios con los permisos limitados a sus actuaciones. Se ha aumentado la seguridad en la conexión de usuarios externos a la empresa mediante \/PN al aplicar una configuración más restrictiva de puertos. Por lo que podemos afirmar que la empresa se encuentra libre de infecciones.”

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

Aportan copia del Registro de Actividades de Tratamiento, de un Análisis de Riesgo previa a la Evaluación de Impacto de 2018 y otro post-evaluación de impacto de 2020 y evaluación de impacto.

Sobre las Medidas técnicas y organizativas adoptadas para garantizar un nivel de seguridad adecuado a los riesgos detectados en los tratamientos afectados por la brecha, indican que se adoptan medidas de seguridad en la organización acordes con el RGPD para los datos afectados:

- Planes anuales de formación en materia de protección de datos.

- Circulares al personal autorizado al tratamiento advirtiendo sobre este tipo de incidentes.

Aportan al respecto de los dos primeros puntos “Documentación soporte formación e intranet: circulares, Plan de acogida, decálogo de PP.DD. para personal HT, Compliance”

- El sistema se actualiza automáticamente.

- El sistema está protegido por antivirus y este se actualiza automáticamente.

- El sistema se monitoriza mediante una solución provista por el fabricante del antivirus para garantizar la vigencia de las firmas de virus y la integridad del mismo.

- La carpeta en la que se almacenan los datos afectados solo es accesible a usuarios con credenciales válidas en el sistema.

- La carpeta en la que se almacenan los datos afectados se borra periódicamente.

- El sistema es objeto de auditorías de seguridad periódicas.

En este caso las medidas fallaron porque el sistema objeto de la intrusión llevaba tiempo sin utilizarse, y antes de que el sistema tuviera el antivirus actualizado, abrió un correo conteniendo un virus que pasó inadvertido al sistema de detección, infectando el ordenador y accediendo a los recursos a los que el usuario cuyas credenciales se utilizaron para iniciar la sesión tenía acceso en la red, en este caso, la carpeta compartida del escáner.

Aportan copia de la política de seguridad indicando que se hace llegar a todo el personal autorizado al tratamiento de datos personales. Manifiestan que se está llevando a cabo la planificación al Esquema Nacional de Seguridad (Real Decreto 3/2010, de 8 de enero), en adelante ENS, lo que implicará la redacción de una Política de Seguridad de la información, que de igual manera se hará llegar a todo el personal que interviene en el procesamiento de esta.

Respecto de las medidas implementadas con posterioridad la brecha

Manifiestan tomar las siguientes medidas:

- Realización de acciones correctivas tanto sobre el equipo en cuestión como revisión tanto interna como externa de toda la seguridad de la organización.

- Contratación de Consultora en materia de Ciberseguridad con el objetivo de:

·Planificación de la adaptación de la organización al ENS, lo que implicará la implantación de las medidas de seguridad previstas en el Anexo II del Real Decreto 3/2010, de 8 de enero que regula el ENS.

·Auditoría de seguridad de todos los sistemas de la empresa. Aportan “Auditoria de sistemas y adecuación ENS”

·Auditoría de los sistemas expuestos al exterior de la empresa. Aportan “Informe ejecutivo de informe de exposición”.

·Consultoría en gestión de perfil para la contratación de un Responsable de Ciberseguridad en la empresa.

- Seudonimización, en la medida que el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento lo permitan de las bases de datos de los sistemas de información.

- Mayor implicación de dirección en la implantación de políticas de seguridad activa.

- Políticas de formación de usuarios en cuanto al uso de equipos de uso eventual.

- Concienciación a los usuarios del uso correcto de las carpetas compartidas por escáneres e impresoras

- Aumento de las restricciones en el tráfico perimetral para limitar la salida accidental de ficheros no autorizados.

- Llevar a cabo simulacros de este tipo de incidentes.

Respecto de la empresa.

Según la información consultada en AXESOR, HT es una PYME constituida en 1998 con 34 empleados y un volumen de facturación de algo más de 3 millones doscientos mil euros.

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 inicialmente como brecha de disponibilidad, hasta que el descubrimiento de fuga de información, obliga a calificarla como brecha de confidencialidad.

De la documentación aportada por la empresa, en el curso de estas actuaciones de investigación, copia del RAT, copia AR previo a la Evaluación de Impacto 2018 y otro post-evaluación de impacto de2020 , copia de evaluación de impacto, copia de las políticas de seguridad compuesta por un plan de seguridad de sistemas y una política de seguridad al personal, se desprende que con anterioridad a la brecha, la entidad investigada disponía de medidas de seguridad razonables en función de los posibles riesgos estimados.

La brecha fue posible a través del acceso a un equipo (del Área de Administración) cuyo uso es esporádico y que en el periodo que transcurrió entre que arrancó y recibió las actualizaciones del antivirus, fue afectado por el virus CONTI, posiblemente a través de un correo infectado. Este equipo tenía acceso a la red interna de la empresa y, entre otros, a la carpeta compartida que almacena los ficheros procedentes de un escáner, que han sido los datos afectados por la brecha.

En cuanto al impacto, los datos que se han visto vulnerados contienen información identificativa, económica, laboral y también relativa a la salud, ya que se detalla el nombre de la prueba realizada.

El volumen de Datos se encuentra en el rango de 260, el único conocimiento que se tiene de utilización por parte de terceros de la información es el intento de extorsión al responsable y la publicación en la dark web y la URL ******URL.1***. En lo referente a los accesos, el 12 de diciembre de 2020 constaban 2.700 accesos, la gran mayoría son del responsable del tratamiento, al acceder para comprobar los datos publicados.

Para evitar que estos hechos se vuelvan a repetir y en lo relativo al ataque de Ransomware, se aporta un certificado de empresa especializada en la que se afirma que la entidad investigada se encuentra libre de infecciones, que se han implementado las medidas de seguridad para que un ataque similar no pueda volver a producirse y que se han realizado mejoras adicionales en la seguridad. Posteriormente y entre otras medidas, afirma proceder a la contratación de una consultora en materia de Ciberseguridad con los objetivos de planificar la adaptación de la organización al ENS, realizar auditoría de seguridad de todos los sistemas de la empresa y de los sistemas expuestos al exterior de la empresa además de actuar como consultora en la gestión del perfil para la contratación de un Responsable de Ciberseguridad.

En consecuencia, consta que disponía de medidas técnicas y organizativas razonables para evitar este tipo de incidencia, no obstante y una vez detectada ésta, se produce una diligente reacción al objeto de notificar a la AEPD, comunicar a los interesados, realizar las denuncias procedentes tanto a la policía como al INCIBE incluyendo también la presentada ante el proveedor de servicios de la URL citada e implementar medias para eliminarla.

III

Por lo tanto, se ha acreditado que la actuación del reclamado 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 al reclamado.
HEALTH TIME, S.L. con NIF B82066002 con domicilio en C/ ORTEGA Y GASSET 25, BAJO - 28006 MADRID (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