- **Procedimiento N.º: E/04740/2020**

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 el responsable del tratamiento de HITACHI EUROPE, S.A., en el que informa a la Agencia Española de Protección de Datos que, con fecha ******FECHA.1***, se detectó un ataque a través de dos Pc de escritorio en la oficina de HITACHI EUROPE LIMITED en ******PAÍS.1*** que permitió el acceso al Directorio activo que contenía datos personales de los empleados y podría haber sido copiado y exportado fuera de la organización.

Se han visto afectados datos básicos (nombre y apellidos) y de contacto (número de teléfono y dirección de correo corporativo) de unos 12 empleados.

Han notificado a Alemania, Gran Bretaña, Francia e Italia.

SEGUNDO: En fecha 2 de junio 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***.

ENTIDAD INVESTIGADA

HITACHI EUROPE, S.A. con CIF A08653834 con domicilio en C/ ******DIRECCIÓN.1*** (Barcelona).

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN:

1.- Con fecha 23 de julio de 2021 se procedió a la apertura de un artículo 56 (Identification of LSA and CSA) con número 133083 a través del sistema IMI sobre la brecha de seguridad sufrida por HITACHI EUROPE LIMITED (en adelante HEU) y HITACHI EUROPE SA (en adelante HE España) donde se proponía como autoridad líder a ******PAÍS.1*** y como autoridad interesada a España. El caso fue cerrado el 23/09/2020.

No consta ninguna autoridad como LSA ya que ******PAÍS.1*** ha contestado que es interesada y solo es principal en lo que respecta al encargado del tratamiento

Se han declarado interesadas: Alemania (Hesse, Berlín, Lower Saxony, Bavaria), Suecia, Bélgica, Italia, Francia, Estonia, Noruega, Países Bajos, Austria, Dinamarca, Luxemburgo, Irlanda, Polonia y Finlandia.

HE España ha aportado documento en el que consta que la Oficina de Información del Comisariado de ***PAÍS.1*** ("UK Information Commissioners Office" - ICO) ha llegado a la conclusión de que no corresponde tomar ninguna acción formal o seguir investigando el incidente (Anexo VII)

1.- Con fechas 16 de diciembre de 2020 y 19 de enero de 2021 se solicitó información a HE España. De la respuesta recibida se desprende lo siguiente:

Respecto de la empresa.

- Hitachi Europa es una organización dedicada a la innovación en tecnologías operativas y de la información y engloba a más de 130 empresas que operan en 22 países europeos.

- Dentro del Grupo, HE España toma decisiones relativas a las finalidades y medios empleados para el tratamiento de datos en el contexto de suministro, por parte de HEU, de infraestructura tecnológica y seguridad a HE (documento Anexo III esquema organizativo de la estructura del Grupo HEU)

- HE España ha aportado copia del Contrato de encargo del tratamiento de datos entre HE España como responsable del tratamiento de datos y HEU, como encargado del tratamiento. Dicho contrato se encuentra relacionado con el suministro por parte de HEU, de sistemas tecnológicos de infraestructura y seguridad. (documento Anexo II).

- HE España manifiesta que el mantenimiento de los sistemas de información afectados no se lleva a cabo por medio de terceras personas.

Respecto de la cronología de los hechos.

- HE España manifiesta que tuvieron dos amenazas distintas y no relacionadas entre sí que se infiltraron en los sistemas de HEU entre noviembre de 2018 y junio de 2020. Las amenazas no se dirigían a HE España específicamente.

- HE España manifiesta que rápidamente se comprobó que los controladores de dominio del Directorio Activo habían sido comprometidos, lo que provocó la notificación inicial por parte de las filiales del Grupo a las Autoridades de Control de la Unión Europea, entre ellas la notificación a la Agencia Española de Protección de Datos.

- Ambos grupos de amenaza obtuvieron una copia del Directorio Activo.

  La investigación llevada a cabo reveló la posible presencia de actores de amenaza durante un periodo de tiempo relevante (Amenaza Avanzada Persistente -AAP-) y las actividades que permitieron el acceso indebido fueron llevadas a cabo por los dos grupos (Grupo de Amenaza A y Grupo de Amenaza B)

La empresa ******EMPRESA.1***, encargado de llevar a cabo la investigación ha informado de que estas actividades podrían considerarse como espionaje industrial, lo que significaría que la intención de los atacantes fue, posiblemente, la de generar una presencia sostenida ("sustained presence") en los sistemas tecnológicos de HEU para así atacar la propiedad intelectual e industrial de HEU.

- Grupo de Amenaza A. La primera fase de actividad por parte del Grupo de Amenaza A ocurrió durante el periodo trascurrido entre febrero y septiembre 2019. Durante este periodo se accedió a las cuentas del administrador local, se ejecutó un malware confeccionado a medida para extraer las contraseñas de los usuarios y el material de autenticación de los sistemas y se estableció conexiones con la infraestructura externa controlada por el atacante.

  En el periodo transcurrido entre el 20 de abril de 2020 y el 23 de mayo de 2020, comenzó una fase de infiltración obteniéndose acceso a los sistemas de tecnología de HEU y se extrajeron las bases de datos del Directorio Activo en relación con dominios específicos.

  La evidencia más reciente procedente de este Grupo ocurrió el 23 de mayo 2020.

  En el análisis de la empresa ******EMPRESA.1*** indica que el Grupo de Amenaza A podría ser una organización localizada en ******PAÍS.2*** y especializada en espionaje industrial.

- Grupo de Amenaza B. La actividad más temprana por parte del Grupo de Amenaza B fue identificada el 5 de noviembre de 2018 y durante el periodo de tiempo trascurrido entre noviembre de 2018 y junio de 2020 se obtuvo acceso a las cuentas del administrador local y un reconocimiento de los sistemas tecnológicos de HEU, extrajeron la base de datos del Directorio Activo para un dominio y se estableció acceso remoto a los sistemas tecnológicos de HEU.

  La evidencia más reciente de actividad por parte del Grupo de Amenaza B tuvo lugar el 5 de junio de 2020, cuando realizó un intento fallido a los terminales de trabajo utilizados por HEU.

  El análisis de ******EMPRESA.1*** indica que este Grupo es probablemente una organización ubicada en ******PAÍS.3*** y conocida por llevar a cabo actividades de espionaje industrial.

- ******FECHA.1***: HEU detectó por primera vez una actividad potencialmente sospechosa en los servidores que opera e inmediatamente contrataron a la empresa ******EMPRESA.1*** FireEye para llevar a cabo una investigación y medidas de corrección.

- 15 de mayo de 2020: notificación preliminar presentada por HEU ante la Oficina de Información del Comisariado de ******PAÍS.1*** (ICO) y el 18 de mayo 2020 HEU informa a HE España de la detección de la intrusión, la cual presenta notificación a la Agencia el día 27 de mayo.

- 23 de mayo de 2020 y el 26 de junio se aplican medidas correctoras derivadas del análisis de ******EMPRESA.1*** para eliminar al atacante y procurar la detección de futuros intentos de acceso.

- De junio a agosto de 2020: prosigue la investigación de ******EMPRESA.1***, con supervisión adicional en relación con posibles intentos por parte del atacante de recobrar acceso.

- 14 de julio de 2020: recepción de la carta procedente de la Oficina de Información del Comisariado de ******PAÍS.1*** ICO confirmando la no intención de proseguir con acciones regulatorias.

- 21 de agosto de 2020: ******EMPRESA.1*** cesa en la investigación activa de la red de HEU.

- Agosto– noviembre de 2020: ******EMPRESA.1*** completa un detallado informe del incidente.

Respecto de las causas que hicieron posible la brecha.

- No se ha podido identificar cómo se iniciaron las intrusiones por parte de los dos grupos de atacantes. Sin embargo, se descubrió que ambos grupos de amenaza, con el tiempo, fueron aumentando su capacidad para acceder a un amplio rango de sistemas tecnológicos. Se estima que ambos grupos de amenaza son sofisticados y están bien equipados, haciendo uso de un nuevo malware configurado a medida para ejecutar sus actividades mediante el uso de técnicas complejas de ofuscación para evitar ser detectados.

- Las medidas de seguridad implementadas no previnieron el incidente de seguridad debido a la sofisticación de los atacantes, que usaron malware hecho a medida y técnicas de ofuscación que eliminaron, en ciertos casos con alto grado de precisión y efectividad, la evidencia del acceso a los sistemas de HEU.

Medidas de minimización del impacto de la brecha y acciones tomadas para la resolución final de la brecha.

HE España ha manifestado que se han introducidos medidas en HEU, entre ellas:

- HEU al ser conocedor de la incidencia de seguridad aisló los ordenadores afectados, cambió las contraseñas y deshabilitó la cuenta de gestión del dominio.

- HEU contrató a ******EMPRESA.1*** como especialista en respuestas frente a incidentes cibernéticos.

  Se desarrolló un plan estratégico con ******EMPRESA.1*** para localizar y eliminar completamente todos los posibles puntos de acceso del atacante.

- HEU realizó actividades de corrección desde el 23- 24 de mayo de 2020 y el 6-7 de junio de 2020, destinadas a eliminar el acceso por parte del atacante a los sistemas tecnológicos correspondientes, incluyendo el reinicio de numerosas contraseñas de tal forma que se evitara alertar al atacante.

- Todos los sistemas identificados como potencialmente comprometidos fueron limpiados del malware del atacante.

- Rastreo y seguimiento de la actividad de la red para supervisar indicios de cualquier actividad sospechosa.

- Algunos sistemas han sido desactivados.

- Revisar y mejorar la seguridad, incluyendo protección adicional avanzada contra amenazas.

- Despliegue inmediato de sistemas de Detección y respuesta.

- Implementar una solución de contraseña para Administrador Local

- Revisión de las estructuras de seguridad del Directorio Activo.

- Migración de los servidores a soluciones en la nube con configuraciones adicionales de seguridad a nivel de la red.

Respecto de los datos afectados.

- En España han sido afectados 12 personas.

  En HEU (Reino Unido) 358 afectados.

  Y un total de aproximadamente 240 en el resto de los países afectados.

- HEU ha notificado la brecha de seguridad al Reino Unido, Francia, Italia, y Alemania (Westfalia).

- Los datos accedidos corresponden con datos de la cuenta profesional del usuario (detalles de contactos de trabajo, - direcciones de correo electrónico y números de teléfono-) contenidos dentro del Directorio Activo.

- El acceso a servidores de archivos podría contener datos personales relacionados con los empleados y otras personas, aunque las políticas de uso de la tecnología implementadas por HEU recomiendan a los usuarios no guardar datos personales en los ordenadores de la empresa.

  Todos los usuarios de HEU (incluyendo empleados de HE España), que podrían haber guardado información personal en estos servidores de archivos, fueron notificados de la intrusión.

HE España manifiesta que no se puede descartar la posibilidad de que accediesen a contraseñas encriptadas.

- HEU no está al corriente del uso por terceros de datos personales obtenidos durante el incidente.

- HEU no está al corriente de ninguna publicación en Internet o de indexación por motores de búsqueda de los datos personales obtenidos en este incidente.

- HEU no notificó formalmente a los interesados, ya que sus intereses y libertades no se pusieron en alto riesgo, teniendo en cuenta las categorías de datos personales accedidas y el objetivo global de los grupos de amenazas. No obstante, HEU notificó informalmente a sus empleados por si habían usado los sistemas de trabajo para almacenar datos personales, a pesar de que los empleados no están autorizados a hacerlo.

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

- HEU tenía implementadas, entre otras, las siguientes medidas en el momento del incidente:

    - Revisiones de seguridad de la aplicación de los sistemas operativos, aplicaciones y red.

    - Protección mediante antivirus proporcionada a todos los clientes y servidores.

    - Políticas complejas de contraseñas. Limitación de los derechos de administración.

    - Sistema de seguimiento tecnológico de HEU con alertas automáticas para eventos concretos.

    - Pruebas externas de vulnerabilidad de direcciones de IP

    - Acceso remoto protegido

- HEU ha aportado los siguientes documentos:

    - Registro de las actividades de tratamiento de datos personales en relación con el Directorio Activo (Anexo IV).

    - Política de seguridad global (Anexo V).

    - Política de Brechas de seguridad (Anexo VI).

- Respecto del Análisis de Riesgo, HE España manifiesta que HEU tiene un extenso paquete de protección contra la intrusión externa y el tratamiento donde se ha producido la brecha (Directorio Activo) no representó un riesgo particular que hubiese justificado la implementación de medidas de seguridad adicionales a dicha protección extensa.

  De forma similar, HE España no realizó ninguna Evaluación de Impacto con respecto a este tratamiento, considerando que no suponía un alto riesgo para los derechos y libertades de los interesados afectados.

Respecto de las medidas implementadas con posterioridad la brecha.

- HEU lleva a cabo pruebas de penetración sobre IPs públicas, por lo menos, una vez al mes. Estaba previsto llevar a cabo una evaluación presencial de la infraestructura tecnológica en enero de 2020 que se realizará en 2021.

Motivo por el cual no se ha notificado la brecha antes de las 72 horas de que sucediera.

- HEU notificó a la Oficina de Información del Comisariado de ***PAÍS.1** ICO dentro del plazo de 72 horas desde su conocimiento, la cual ha llegado a la conclusión de que no corresponde tomar ninguna acción adicional o seguir investigando el incidente.

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, como consecuencia de un ataque mediante un malware configurado a medida para ejecutar sus actividades mediante el uso de técnicas complejas de ofuscación que permitió el acceso desde el exterior al Directorio activo que contenía datos personales de los empleados, pudiendo haber sido copiado y exportado fuera de la Organización. Se han visto afectados datos básicos (nombre y apellidos) y de contacto (número de teléfono y dirección de correo corporativo) de unos 12 empleados.

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 Registro de Actividades de Tratamiento en relación con el Directorio activo, Política de Seguridad Global y Política de brechas de seguridad. Respecto al Análisis de Riesgo, HEU tiene un extenso paquete de protección contra la intrusión externa y el tratamiento donde se ha producido la brecha (Directorio Activo) no representa un riesgo particular que justifique la implementación de medidas de seguridad adicionales.

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.

No constan reclamaciones ante esta Agencia por parte de terceros.

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 HITACHI EUROPE, S.A. con CIF A08653834 con domicilio en C/ ******DIRECCIÓN.1*** (Barcelona).

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