- **Procedimiento Nº: E/03613/2021**

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 del Responsable del Tratamiento ACER COMPUTER IBERICA, S.A. (en adelante Acer) con número de registro de entrada ******REGISTGRO.1*** relativa a ransomware y que afecta a 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:

Fecha de notificación de la brecha de seguridad de datos personales: ******FECHA.1***.

Resumen de la notificación: "*El* ******FECHA.2*** *a las 00.34 de la mañana, el departamento de IT descubrió que un ataque de ransomware estaba afectando a los servidores locales de la región de* ***XXXX (XXXXXX, XXXXXX*** *y* ***XXXXXXX XXXXX)****. Como resultado del ataque, los datos incluidos en la red local de Acer fueron parcialmente encriptados, haciéndolos indisponibles. Aunque la causa raíz del ataque y las consecuencias actuales del mismo siguen siendo investigadas, parece que los sistemas globales de marketing y recursos humanos los cuales almacenan datos personales de residentes en la UE no fueron afectados. Parece ser que alrededor del 50% de los sistemas en* ***XXXX*** *han sido afectados, aunque aún no está claro si los datos personales almacenados se han visto afectados por una violación de integridad y/o confidencialidad. la disponibilidad de los datos se ha visto afectada a nivel local, pero existen copias de seguridad.*"

En una notificación adicional posterior Acer ha manifestado: "*Esta es una notificación adicional a la presentada en fecha* ******FECHA.1*** *en relación a la brecha de seguridad de los datos descubierta por Acer el* ******FECHA.2****. Las investigaciones sobre el incidente han continuado desde entonces y Acer ha recuperado más y más sistemas, devolviéndolos operativos, sin perjuicio de que las investigaciones siguen en curso. Los datos que se ofrecen a continuación sirven para proporcionar información complementaria sobre la brecha. A pesar de las especulaciones de los medios de comunicación, Acer todavía no ha podido confirmar la exfiltración de datos de carácter personal de sus sistemas y, por tanto, no ha podido concretar los datos de carácter personal efecti-*

*vamente comprometidos en España. Sin embargo, a pesar de la falta de confirmación, Acer ha decidido, de manera proactiva y como medida de precaución, informar a todos sus empleados de la región **XXXX** sobre el incidente y la posibilidad de que sus datos se hayan visto (parcialmente) comprometidos como consecuencia del mismo, para que puedan estar atentos a cualquier irregularidad y tomar las medidas oportunas. En relación a los clientes de Acer, es probable que únicamente los nombres y datos de contacto haya sido (potencialmente) comprometidos, por lo que no existiría un alto riesgo para sus derechos y libertades ex. artículo 34 del RGPD y, por tanto, no se ha realizado ninguna comunicación a los mismos. En aras de la coherencia y la seguridad, Acer ha indicado ahora, en esta notificación adicional, todas las categorías de datos personales que pueden haber sido afectadas en España (como se indica a continuación). Adicionalmente, Acer ha presentado las correspondientes denuncias policiales en varias jurisdicciones europeas y Suiza, donde sus entidades operativas se encuentran."*

Marcan como categorías de datos afectados: datos básicos, credenciales de acceso, datos de contacto, DNI/NIE/Pasaporte, datos económicos/financieros.

ENTIDADES INVESTIGADAS

Durante las presentes actuaciones se han investigado las siguientes entidades:

ACER COMPUTER IBERICA, S.A. (Acer) con CIF A60832706

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

Respecto de la cronología de los hechos. Acciones tomadas con objeto de minimizar los efectos adversos y medidas adoptadas para su resolución final

Los representantes de Acer han manifestado:

*"Este incidente forma parte de un ataque global a los sistemas del Grupo Acer. El *****FECHA.2**, a las 00:34 h (medianoche), el departamento de TI descubrió que un ataque de ransomware estaba afectando a los servidores locales del Grupo Acer en la región **XXXX (XXXXXX, XXXXXXX XXXXX** y **XXXXX)**. El hacker inició el cifrado de múltiples extremos a escala mundial, utilizando los servidores que tenían funciones de autoridad alta y funciones en cada área para interrumpir los servicios internos. Debido a ello, los datos incluidos en la red local del Grupo Acer quedaron cifrados parcialmente y dejaron de estar disponibles. Parece que no se han visto afectados el sistema de marketing global y el sistema de RR.HH. global que almacena los datos personales de residentes en la UE.*

*Según los resultados de la investigación forense, se sospecha que la causa original del incidente fue un mensaje de correo electrónico malicioso de phishing, recibido el 18 de febrero de 2021. El mensaje de correo electrónico de phishing no se puede recuperar como consecuencia del ataque de ransomware. Por lo tanto, hay cierta incertidumbre sobre si ese mensaje de correo electrónico fue realmente la causa original, pero es posible que el mensaje de phishing permitiera al hacker instalar una puerta trasera que, finalmente, dio lugar al ataque de ransomware del *****FECHA.2**.*

*La investigación sobre el incidente comenzó ese mismo día (*****FECHA.2**). La investigación se llevó a cabo por parte de la sociedad del grupo de Acer especializada en ciberseguridad Acer Cybersecurity Inc., así como externamente por parte de la firma especializada en ciberseguridad TrendMicro. De los resultados preliminares de la investigación se puede concluir que el Grupo Acer recibió las primeras señales de comportamiento sospechoso en su sistema el día 3 de marzo de 2021. Dado que el sistema de detección, por lo general, detecta todo comportamiento irregular, inició sus actividades de respuesta normales (tal como se indica más adelante, en «Acciones emprendidas para minimizar el efecto de la vulneración»). Antes del ataque de ransomware en sí, el Grupo Acer no tenía conocimiento, y no tenía razones para tener conocimiento, de que hubiera ransomware oculto en el entorno del Grupo Acer, que conduciría al ataque y, finalmente, al cifrado de los archivos.*

*Como todos los datos de las copias de seguridad estaban disponibles para Acer en la región **XXXX**, los datos no se perdieron y solamente dejó de poderse acceder a ellos temporalmente, a saber, durante el plazo de tiempo necesario para restaurar los datos a partir de las copias de seguridad o para limpiar los servidores afectados, y el acceso se restauró, aproximadamente, a finales de marzo. Todos los sistemas críticos para la empresa volvieron a estar operativos la primera semana después del 14 de marzo. Por orden de criticidad, otros sistemas volvieron a estar operativos durante la semana siguiente. Los sistemas afectados almacenan datos relacionados con Recursos Humanos (RR.HH.) localmente en los países, datos relacionados con la atención al cliente y datos personales necesarios para suministrar productos comprados de manera online (pero no se vieron afectados los datos personales tratados en la transacción en línea en sí, por ejemplo, datos de tarjetas de crédito).”*

Los representantes de Acer enumeran ocho acciones emprendidas para minimizar el efecto de la vulneración, entre las que se encuentran investigaciones con la participación de *Acer Cybersecurity Inc.* y el proveedor de seguridad externo *TrendMicro*, bloqueo de direcciones IP y dominios sospechosos, instalación de parches en los servidores, restablecimiento de contraseñas críticas, análisis de seguridad de todos los servidores y los sistemas afectados, cambios de contraseñas de todos los usuarios y otras tareas técnicas con los servidores informáticos.

Sobre las implicaciones de la brecha y si finalmente ha existido vulneración de la integridad y la confidencialidad.

Los representantes de Acer han manifestado:

“La investigación sigue en curso; sin embargo, hasta la fecha no hay pruebas concluyentes de que se produjera una vulneración de integridad y/o confidencialidad. A este respecto, cabe señalar lo siguiente: el ataque fue un ataque de ransomware. Los responsables del ataque fijaron un plazo de pago hasta el 28 de marzo y amenazaron con publicar los datos si el Grupo Acer no realizaba el pago a tiempo.

El Grupo Acer no pagó el rescate pedido y ha estado pendiente de la posible publicación de los datos. Aunque el plazo finalizó hace tiempo, y a pesar de la exhaustiva supervisión por parte del Grupo Acer, la única información encontrada fue un anuncio en la «dark web» relacionado con datos de empleados del Reino Unido (así como Japón e India).

Asimismo, cabe destacar que en la actualidad, no se ha confirmado la extracción de datos personales. El Grupo Acer no ha podido determinar si la información limitada que se facilitaba en el anuncio se obtuvo realmente en el contexto del ataque. El ataque se dirigió a los servidores […], algunos de los cuales estaban cifrados. Sin embargo, no hay pruebas de que las bases de datos de esos servidores (en las que se almacenan los datos personales) se vieran afectadas por el ataque."

Respecto de las causas que hicieron posible la brecha

Los representantes de Acer han manifestado:

*Según los resultados de la investigación forense, los registros del sistema de detección indican que se introdujo de forma maliciosa el malware «*****MALWARE.1**» en los sistemas del Grupo Acer. Según la investigación llevada a cabo por TrendMicro, y sobre la base de las acciones de los hackers y las acciones de cifrado, se confirmó que fue el ransomware *****RANSOMWARE.1** el que permitió el cifrado. Los hackers instalaron varias herramientas de piratería informática e instalaron el malware *****MALWARE.1** en determinados servidores […SO determinado…].*

*Los responsables del ataque piratearon varios servidores utilizando *****MALWARE.1** y prepararon el servicio para el ataque de ransomware. El hacker utilizó distintas herramientas para familiarizarse con los servidores y el entorno del Grupo Acer, con el fin de enviar el programa de cifrado.*

El hacker ejecutó la herramienta de sincronización de discos de red […marca determinada…]. Esta herramienta puede transmitir datos a un disco de red, que un hacker puede utilizar como método para robar datos. Sin embargo, no hay pruebas directas de que dicha exfiltración de datos tuviera lugar. Además de intentar poner en pausa el servicio de software antivirus de […marca determinada…], el hacker también canceló […programa de seguridad determinado…] mediante archivos de lotes, para poder instalar el programa malicioso sin obstáculos ni ser detectado. El hacker revisó la configuración del escritorio remoto y del firewall para invadir el servidor posteriormente.
La disponibilidad de los datos se vio afectada, pero la Compañía contaba con copias de seguridad. Algunos servidores […SO determinado…] del Grupo Acer se vieron afectados. No hay pruebas de acceso directo a los datos de las bases de datos ni a otros datos personales. Los datos se han restaurado a partir de los servidores de copias de seguridad; por lo tanto, actualmente las bases de datos están disponibles y se han restaurado."

Respecto de los datos afectados.

Los representantes de Acer indican que no hay pruebas concluyentes de que las bases de datos de los servidores atacados se vieran afectadas como tampoco los servidores del marketing ni de RRHH, que almacena los datos personales de residentes en la UE. El número potencial de personas que podrían haberse visto afectadas en relación con Acer (Acer Computer Ibérica, S.A.) es, aproximadamente: Consumidores: 1.066.637 y Empleados: 139

Sobre la distribución del número afectados por tipo de datos de afiliación sindical, datos de salud y credenciales de acceso. Número potencial de personas cuyos datos de salud y datos de acceso se han visto afectados (si dichos datos se hubieran efectivamente exfiltrado) sería de, aproximadamente:

-Datos sanitarios: 139. Aplica únicamente a los empleados como interesados de datos afectados; el número de empleados afectados de Acer (Acer Computer Ibérica, S.A.).

-Datos de acceso: 3 (aplica únicamente a los empleados como interesados de datos afectados, y solo a los empleados con acceso a los servidores; para Acer (Acer Computer Ibérica, S.A.), esto solo supone solo 2 o 3 personas).

-Adicionalmente, indican que se ha confirmado que ningún dato de afiliación sindical se hubiera visto afectado (si los datos se hubieran exfiltrado).

Información sobre la utilización por terceros de los datos personales comprometidos.

Los representantes de Acer indican que hasta la fecha no hay pruebas concluyentes de que se produjera una vulneración de integridad y/o confidencialidad. La única información que se encontró en línea después del ataque de ransomware fue un anuncio en la «*dark web*» relativo a datos de los empleados del Reino Unido (así como Japón e India). No se han encontrado información ni datos personales relativos a Acer (Acer Computer Ibérica, S.A.), ni ha habido indicios hasta la fecha de que se hayan usado esos datos o hayan sido objeto de otro tratamiento por terceros no autorizados.

Notificación a los afectados.

Los representantes de Acer han manifestado:

"A pesar de la falta de confirmación de exfiltración de los datos personales, el Grupo Acer ha decidido —como medida de precaución y de manera proactiva—, informar a todos sus empleados de la Región ***XXXX*** *acerca del incidente y de la posibilidad de que sus datos se hayan visto comprometidos (parcialmente) como consecuencia del mismo, para que puedan estar pendientes de cualquier irregularidad y permitirles tomar las medidas adecuadas en caso necesario[…].*

Con respecto a los clientes, solamente se pudieron ver comprometidos los nombres y datos de contacto. El análisis realizado por Acer indica que esto no da lugar a un alto riesgo según el art. 34 del RGPD y, por lo tanto, indican que no se comunicó el incidente a los clientes."

Adjuntan copia de la notificación enviada por email a los empleados de Acer.

Respecto de las medidas de seguridad implantadas

Con anterioridad a la brecha en la respuesta de Acer se detallan las medidas de seguridad implementadas. Como resumen y entre otras medidas se incluyen cortafuegos, antimalware y antivirus, controles de acceso con revisiones periódicas, aplicación de minimización de datos y uso de cifrado cuando corresponde, supervisión

de los sistemas, copias de seguridad, análisis periódicos de vulnerabilidades y pruebas de penetración.

Sobre el motivo por el cual estas medidas de seguridad implantadas no han impedido el incidente los representantes de Acer han indicado: *"El Grupo Acer utilizaba tecnologías de seguridad estándar en la industria y comercialmente razonables. El Grupo Acer aplicó medidas técnicas y organizativas adecuadas para proteger la seguridad, la integridad y la confidencialidad de los datos de clientes y demás datos personales, así como para protegerlos de toda divulgación, corrupción o acceso no autorizado o ilícito. A pesar de este hecho, los responsables del ataque consiguieron acceder a los sistemas, presuntamente a través de un correo electrónico malicioso de phishing. El Grupo Acer contaba con copias de seguridad en la región* ***XXXX*** *adecuadas y separadas, que ayudaron a mitigar las consecuencias del ataque."*

Con posterioridad a la brecha los representantes de Acer detallan un listado de medidas que incluyen, entre otras, la revisión completa de la administración de dominios, reinstalación de servidores, restauración y verificación de las copias de seguridad, realización de análisis de vulnerabilidades, eliminación de perfiles y contraseñas de administración, actualizaciones de productos de seguridad, revisión del directorio activo.

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 disponibilidad.

La investigada indica que previamente a la brecha, además de disponer de cortafuegos, antimalware y antivirus, así como de copias de seguridad, procede a la supervisión constante de los sistemas y de la actividad inusual de la red con el fin de detectar anomalías, realiza revisiones periódicas de los controles de acceso, análisis periódicos de vulnerabilidades y pruebas de penetración, aplicando también la minimización de datos y el cifrado. De todo ello se desprende que, con anterioridad a

producirse la brecha, la entidad investigada disponía de medidas de seguridad razonables en función de los riesgos estimados.

La investigación forense de los hechos, realizada tanto por la sociedad perteneciente al grupo Acer especializada en ciberseguridad, como por una empresa externa, sospecha que el origen estuvo en un mensaje de correo electrónico malicioso de phishing, lo que permitió el pirateo de varios servidores y la preparación del servicio para el ataque de ransomware. Además los atacantes ejecutaron la herramienta de sincronización de discos de red, lo que puede permitir la exfiltración de datos, no obstante no existen pruebas directas de que ésta se haya producido. Tampoco existen pruebas de acceso directo a los datos contenidos en las BBD, ni a otros datos personales.

Tras conocerse el incidente se actúa con diligencia, aparte de iniciar rápidamente la investigación, se procede entre otras medidas, al restablecimiento de contraseñas críticas, a cambios de contraseñas de todos los usuarios, a bloquear las IP y los dominios sospechosos, al análisis de seguridad de todos los servidores y los sistemas afectados y a la instalación de parches en los servidores. Asimismo y dado que contaba con las copias de seguridad, se procede a restaurar el servicio.

En cuanto al impacto, la investigada afirma que no hay pruebas concluyentes de que las bases de datos de los servidores atacados se vieran afectadas, como tampoco los servidores de marketing ni de RRHH, no obstante potencialmente podrían verse afectados 1.066.637 consumidores y 139 empleados. En cuanto a la tipología de los datos potencialmente afectados respecto a los clientes son, los nombres y datos de contacto, considerándose que no da lugar a un alto riesgo y por tanto se decide no comunicar a los afectados. En cuanto a los empleados, los datos que potencialmente podrían verse afectados son, datos de salud y los datos de acceso, en este último caso, únicamente afecta a tres personas, confirmando además que no se ha visto afectado ningún dato referente a la afiliación sindical***.*** No obstante y como medida de precaución se decide comunicar a todos sus empleados de la región ***XXXX***.
Asimismo no existen indicios de que se hayan usado los datos por terceros, ni de que se haya producido la publicación o indexación en buscadores.

Para evitar que estos hechos se repitan, la investigada adopta una serie de medidas, entre otras, revisión completa de la administración de dominios, reinstalación de servidores, restauración y verificación de las copias de seguridad, realización de análisis de vulnerabilidades, actualización de productos de seguridad y la revisión del directorio activo.

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 mitigar los efectos y restablecer rápidamente el servicio, notificar a la AEPD y comunicar a los empleados el incidente.

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

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 a ACER COMPUTER IBERICA, S.A. (Acer) con CIF A60832706

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