- **Procedimiento Nº: E/09205/2020**

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: 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 ENDESA, S.A. con número de registro de entrada O00007128e2000008458 relativa a ransomware que afecta a la confidencialidad de los 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: A la vista de la citada notificación de quiebra de seguridad de los datos personales, la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación, así como a trasladar al responsable del tratamiento, la orden de la Directora de la AEPD en la que se le insta a comunicar dicha quiebra a los afectados, teniendo conocimiento de los siguientes extremos:

ENTIDADES INVESTIGADAS

Durante las presentes actuaciones se han investigado las siguientes entidades:

ENDESA, S.A. con NIF A28023430

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1.- ENDESA, S.A., en adelante ENDESA, pertenece al grupo de empresas Enel, multinacional productora y distribuidora de energía eléctrica y de gas y tiene su sede central en Roma (Italia). El Estado italiano, a través del Ministerio de Economía y Finanzas, es el principal accionista.

2.- Con fecha 14 de diciembre de 2020 se solicitó información a ENDESA De la respuesta recibida se desprende lo siguiente:

El ciberataque objeto de comunicación ha sido un ataque de carácter global dirigido directamente contra el grupo Enel.

Con fecha 23 de diciembre de 2020, la autoridad italiana de protección de datos (Garante per la Protezione dei Dati Personali) ha dictado una resolución por la que acuerda el archivo del expediente iniciado a raíz de la notificación del presente incidente ante la autoridad italiana. Aportan copia de dicha resolución.

La autoridad italiana acuerda el archivo del expediente teniendo en cuenta, entre otras, las siguientes circunstancias:

(i) El ataque no ha tenido impacto sobre la continuidad operativa de los servicios afectados,

(ii) Enel ha acordado adoptar medidas técnicas y organizativas para poner remedio a la violación, incluyendo la monitorización de la red de internet para evitar una difusión de los datos,

(iii) Enel ha adoptado medidas técnicas y organizativas para prevenir incidentes futuros similares al ocurrido, incluyendo la introducción de una autenticación multifactorial para el acceso a todos los sistemas del grupo, la sustitución del antivirus y la introducción de una solución de gestión de acceso privilegiada.

Según, la información que ha sido trasladada por la matriz, Enel, la dinámica del ataque de rescate "Netwalker" sufrido por Enel fue la siguiente:

- A las 3.34 AM horas del lunes 19 de octubre, Enel detectó un ataque con rescate en su red informática interna de tipo Netwalker y, activando todos los procesos vigentes para la gestión de incidentes, tomó todas las medidas necesarias para eliminar cualquier riesgo residual, verificar y, en su caso, restablecer el funcionamiento normal de los sistemas en cuestión. Las conexiones a la red de la compañía fueron restauradas de forma segura a las 9:20 A.M. del mismo día.

- El ataque fue lanzado utilizando credenciales robadas de algunos empleados del grupo Enel en Perú que contaban con permisos de administración, que fueron rápidamente identificadas y neutralizadas. El ataque no afectó a la continuidad operacional del servicio y, según nos ha sido trasladado por parte de Enel, aprovechando la velocidad, flexibilidad y resistencia de la infraestructura de la nube del grupo Enel, fue posible restaurar en pocas horas el contenido de algunos servidores cifrados en las primeras etapas del ataque, sin ninguna pérdida de información.

- El atacante hizo pública, a través de su blog en la web profunda, una primera petición de rescate de 7 Millones de Dólares a pagar en un plazo de 7 días para recibir las claves de desencriptación de los sistemas de Enel (según nos trasladan desde Enel, no fue necesario pues se restauró, de forma autónoma e inmediata, el funcionamiento regular de sus sistemas) y para evitar la publicación de la documentación que el atacante afirma haber conseguido filtrar.

- Después de los primeros siete días, el atacante anunció que había incrementado la solicitud de rescate a 14 millones de dólares, ampliando el plazo en otros siete días. El atacante mostró entonces una nueva lista de carpetas que supuestamente poseía, sobre la base de la cual se notificó una posible violación de datos a la autoridad supervisora rumana y a las autoridades supervisoras italianas y españolas

- Enel no pagó el rescate solicitado. Por lo tanto, el 2 de noviembre de 2020, aproximadamente a las 22.00 horas, el atacante publicó en el sitio de intercambio de archivos pCloud (con sede en Suiza) un enlace a un archivo que contenía 58 GB de

archivos filtrados. Según la información trasladada por Enel, entre los archivos publicados, no se identificó información que afectara a Endesa.

- Enel, en colaboración con la Policía Postal, puso en marcha de forma previa iniciativas para vigilar la red de Internet mediante, entre otras cuestiones, la notificación a los proveedores de servicios de intercambio de archivos, a fin de organizar una respuesta adecuada a la posible difusión de datos. A las 22:20 h, se logró el bloqueo del enlace que permitía la descarga de la información.

- El 4 de noviembre de 2020, alrededor de las 4:30 A.M., se detectó una nueva publicación del mismo archivo de datos en el mismo proveedor (pCloud). Enel repitió inmediatamente la solicitud de supresión de los datos, que fue realizada por pCloud alrededor de las 7.20 A.M. horas. De nuevo, según la información que nos ha sido trasladada, no se detectó publicación de información que pudiera afectar a sociedades del grupo Endesa.

- En lo que al perímetro España se refiere y sobre la base de la información que trasladó Enel a Endesa, el incidente fue comunicado al INCIBE y Guardia Civil, además de la Agencia Española de Protección de Datos.

Según la información que fue trasladada por el área de Ciberseguridad de Enel, se detectó el acceso por parte del atacante al Directorio Activo del grupo Enel, en el que se encuentran los datos personales de empleados del grupo, incluyendo empleados de Endesa S.A. (“Endesa”) y sociedades controladas, así como de usuarios de proveedores externos. Concretamente, dicho Directorio contiene los siguientes datos: nombre, apellido, dirección de correo electrónico, teléfono de la empresa y área o departamento al que pertenece de usuarios internos y externos relacionados con varias empresas del grupo Endesa. El número total de datos de usuarios internos y externos incluidos en el Directorio Activo es de 81.579, de los cuales 12.125 son empleados internos y 69.459 usuarios externos. No se han detectado consecuencias para los afectados. A su vez, en relación con los 96 usuarios respecto de los que se detectó el acceso a la identificación de usuario, user Id, se procedió a restablecer, de forma inmediata, la contraseña y, de forma preventiva, se hizo lo mismo con el resto de cuentas.

En cumplimiento del requerimiento remitido el 4 de noviembre de 2020 por la Agencia Española de Protección de Datos y artículo 34 del Reglamento General de Protección de Datos, se realizó, a su vez, con fecha 6 de noviembre, la correspondiente comunicación a los interesados afectados- comunicación que fue remitida a esa Agencia con fecha 6 de 5 noviembre de 2020. Dicha comunicación se realizó también a nivel de grupo Enel a todos los afectados.

Respecto a las medidas adoptadas, el día 19 de octubre a primera hora de la mañana se tomaron una serie de medidas urgentes encaminadas a evitar la propagación del incidente. Concretamente, se adoptaron las siguientes medidas:

o Desconexión del acceso externo (VPN) o Comunicación del incidente al INCIBE.

o Identificación y bloqueo del mecanismo de propagación.

o Reactivación de equipos y de conexiones externas.

En días posteriores, desde Enel se ejecutaron nuevas actividades para identificar el origen del incidente y para evitar que volviera a producirse, incluidas las siguientes actuaciones:

o Restauración de equipos afectados.

o Ejecución de un análisis forense en los servidores utilizados por los atacantes.

o Reseteo de contraseñas de los usuarios del Directorio Activo comprometidos, así como todos aquellos usuarios con perfil administrador.

o Despliegue de un mecanismo de doble factor de autenticación en el Directorio Activo para los accesos externos.

o Instalación de un nuevo Security Endpoint en los servidores Windows del Directorio Activo.

o Despliegue de nuevas reglas de monitorización en el Directorio Activo, para la identificación de accesos indebidos.

Desde Enel se ha indicado que el incidente ha permitido identificar las vulnerabilidades explotadas por los atacantes y adoptar medidas para mejorar las medidas de seguridad destinadas a reducir el riesgo de que se repitan en el futuro ataques cibernéticos similares. En particular, el "robo de credenciales" es una amenaza vinculada principalmente al factor humano, fenómeno que ha crecido enormemente durante los últimos meses.

Según ha sido trasladado por el área de Seguridad de la Información a ENDESA:

- No se dispone de evidencias de que se hayan utilizado los datos personales que pudieran haber estado afectados por la brecha.

- No se ha detectado publicación, ni indexación alguna en los buscadores de datos personales que pudieran estar afectados por la brecha. Dicho análisis se ha realizado a través del servicio de búsqueda de información en fuentes abiertas que puedan suponer una amenaza para los activos de Endesa. En este caso, y dada la tipología de datos filtrados se buscó esa tipología concreta, mediante el monitoreo en fuentes abiertas con herramientas que automatizan la búsqueda utilizando consultas, estas se realizan sobre la información disponible en fuentes abiertas, independientemente de que la información esté o no esté indexada en los buscadores.

- Éste sería el primer incidente con filtración de información provocado por un Ransomware

<u>Respecto de las medidas de seguridad</u>

- Aportan copia del Registro de Actividad de los tratamientos donde se ha producido la brecha notificada.

- Se trata de un ataque contra una infraestructura sin impacto específico sobre ninguna actividad de tratamiento. La actividad de tratamiento que se lleva a cabo con relación al Directorio Activo no ha sido objeto de evaluación de impacto porque no se cumplen los requisitos establecidos en la Guía del Grupo de Trabajo del Artículo 29, ni tampoco los criterios establecidos por el Comité Europeo de Protección de Datos.

- A nivel de grupo, existen las siguientes políticas de seguridad aplicables al presente ciberataque que tiene una dimensión global.

- Concretamente, se trataría de las siguientes políticas de seguridad del grupo cuya copia adjuntan:
o Policy 17 – Cyber Security Framework;

o Policy 24 – Critical Event Management;

o Policy 36 – Solutions Development & Release Management;

o OP 204 – Cyber Emergency Readiness Team;

o PL 1026 – IT Service Continuity Management;

o OI 944 – Cyber Security Risk Management Methodology.

- Manifiestan que a nivel de grupo Enel, existe un procedimiento general de brechas de seguridad

- Aportan copia de la Instrucción Operativa local 1.430 de protección de datos personales, relativo a la Gestión de Incidentes de Seguridad. Dicho Anexo aplicable a España para incidentes de nivel local, se refiere a los procesos y acciones necesarios para gestionar los Incidentes de Seguridad relacionados con los Datos Personales y las acciones requeridas para cumplir con los requisitos establecidos en la normativa aplicable en relación con una violación de la seguridad de los datos personales, incluidos los requisitos de comunicación a la Autoridad de Control y a los Interesados. Se aporta, asimismo, la Instrucción Operativa local 131 sobre Gestión de Eventos Críticos.

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 y disponibilidad, como consecuencia de un ciber ataque sobre al Directorio Activo del grupo Enel, en el que se encuentra un número considerable de usuarios respecto del que son responsables del tratamiento varias sociedades del grupo ENDESA. Se han visto afectados los datos básico y de contacto (nombre, apellido, dirección de correo electrónico, teléfono de la empresa y área o departamento al que pertenece) tanto de usuarios internos como externos relacionados con varias empresas del grupo Endesa. 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. Aportando copia del RAT, de las políticas de seguridad aplicadas por el grupo y manifestando que a nivel de grupo Enel, existe un procedimiento general de brechas de seguridad.

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 rápida reacción ante la misma al objeto de restaurar el servicio, minimizar el impacto e implementar nuevas medias razonables y oportunas para evitar que se repita la incidencia en el futuro. Entre ellas, la instalación de un nuevo Security Endpoint en los servidores del Directorio Activo, el establecimiento de un doble factor de autenticación para los accesos externos, así como nuevas reglas de monitorización para la detección de accesos indebidos en el Directorio Activo.

Además se ha procedido a la correspondiente comunicación a los afectados, en cumplimiento del requerimiento remitido el 4 de noviembre de 2020 por la Agencia Española de Protección de Datos. Dicha comunicación se realizó también a nivel de grupo Enel a todos los afectados.

No hay evidencias del uso de los datos personales afectados, ni se ha detectado su publicación o indexación en buscadores.

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

Por lo tanto, se ha acreditado que la actuación del investigado 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 ENDESA, S.A. con NIF A28023430.

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