Expediente Nº: E/03846/2016

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad **ENDESA ENERGÍA, S.A.U.** en virtud de varias denuncias presentadas ante la misma y teniendo como base los siguientes

HECHOS

PRIMERO: Entre el 7 de junio y el 6 de julio de 2016 se registran de entrada en esta Agencia un total de cuatro escritos formulados por otros tantos denunciantes, cuya identidad figura en el Anexo I de esta resolución, poniendo de manifiesto una posible quiebra de seguridad por parte que ENDESA ENERGÍA, S.A.U., (en lo sucesivo la denunciada o ENDESA), en la custodia de los datos personales de los mismos obrantes en los ficheros de dicha empresa.

Las denuncias recibidas, en síntesis, se centran en los siguientes hechos:

El Denunciante nº 1, que se identifica como cliente de la denunciada, indica que ha recibido en su cuenta de correo electrónico dos correos de facturas de ENDESA sospechosos de ser un fraude. Tras contactar con dicha compañía ésta le confirma que muchos clientes están recibiendo este tipo de correos electrónicos fraudulentos. El denunciante aporta copia de dos correos electrónicos de 6 de junio de 2016 con dos resúmenes de facturas distintas con dos CUPS (código universal de punto de suministro) diferentes en cada una de ellas, ninguno coincidente con el del denunciante.

El Denunciante nº 2, que indica es cliente de la denunciada, informa que ha recibió un correo electrónico de una entidad que se identifica como ENDESA adjuntando una factura electrónica que al abrirla le infecta el ordenador, cifrando sus ficheros. Posteriormente recibe una notificación solicitando una cantidad de dinero para enviarle la clave para descifrar los ficheros. El denunciante aporta copia del correo electrónico de 29 de junio de 2016 con el resumen de la factura y de la notificación el pago para poder recuperar sus archivos..

El Denunciante nº 3 informa que quince días después de contratar el suministro de luz y gas con la denunciada recibió en su correo electrónico una factura con el logotipo de ENDESA, la cual resultó ser falsa según le indicó la citada compañía tras remitírsela. Posteriormente recibió una llamada en su línea de teléfono móvil en nombre de ENDESA comunicándole que, por la referida contratación, tenía cinco noches de hotel, remitiéndole para más información a un nº de teléfono 800. El denunciante aporta copia del correo electrónico de 21 de junio de 2016 con el resumen de la factura.

El Denunciante nº 4, que afirma no haber contratado con la denunciada, informa que ha recibido tres correos electrónicos correspondientes a diferentes facturas electrónicas de ENDESA, con origen en cuentas de correo distintas y desconocidas y con datos de CUPS diferentes en cada una de las facturas. El denunciante aporta copia de los tres correos electrónicos de fechas 7, 8 y 27 de junio de 2016 con resumen de tres facturas distintas.

SEGUNDO: Tras la recepción de la denuncia la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento a raíz de la información facilitada por ENDESA en relación con los hechos denunciados de los siguientes extremos:

1. No ha existido una fuga de información o quiebra de seguridad alguna en los ficheros de ENDESA ya que se ha verificado la existencia de receptores de correos electrónicos maliciosos que no son clientes de ENDESA, así como que las facturas fraudulentas contienen datos falsos y no incluyen el nombre del titular del punto de suministro sino, tan sólo, el alias del correo electrónico.

   Se adjunta una muestra de correos electrónicos enviados a ENDESA por personas que no son clientes de la compañía comunicando que habían recibido un email malicioso con un resumen de factura electrónica de Endesa. Se puntualiza que en sus sistemas no estaba registrado dato alguno de dichas personas.

2. La compañía procedió a colaborar con el Instituto Nacional de Ciberseguridad de España (INCIBE) desde el momento en que conoció del envío de correos electrónicos de avisos de facturas falsas de ENDESA invitando a los destinatarios a descargarlas para que, una vez abiertos los correos y hecho "clic" sobre el enlace de consulta de las facturas, redirigir a los destinatarios a una página web con código malicioso ("virus") que bloqueaba los archivos personales de los equipos de los afectados para solicitarles, posteriormente, el pago de una cantidad a cambio de recuperar la información secuestrada.

3. Se trata de un ataque informático combinación de phising y ransomware que no ha afectado a ninguna infraestructura del Grupo ENDESA, sino que ha sido dirigido indistintamente a personas (clientes y no clientes) utilizando la identidad corporativa de la compañía y listas de distribución que posiblemente provengan del mercado negro de datos ya que los envíos son indiscriminados.

4. Respecto de la cronología del fraude indican:

   A las 16:16 horas del día 30 de mayo de 2016 se detecta por parte de los servicios de monitorización del Grupo ENDESA un envío de correos electrónicos masivos potencialmente dañinos desde un presunto dominio fraudulento. Posteriormente, el CERT de Seguridad e Industria -CERT-SI- (organismo de seguridad cibernética del Estado dependiente de los Ministerios de Interior e Industria) puso en conocimiento del Departamento de Seguridad de la empresa la misma situación.

5. Respecto de las actuaciones realizadas señalan:

   Que desde el Grupo ENDESA se ha respondido de forma inmediata, recabando un análisis y evaluación de impacto de lo sucedido y llevando a cabo distintas actuaciones a efectos de mitigar el riesgo y efectos del ataque.

   En este sentido, se han acometido las siguientes actuaciones:

   Se ha procedido a denunciar los hechos delictivos, tal y como acredita la copia adjuntada de la denuncia interpuesta el 3 de junio de 2016 por el Apoderado de las empresas del Grupo.

   Se han realizado actuaciones técnicas consistentes, básicamente, en la bloquear los dominios de Internet fraudulentos desde los que se remitían los correos electrónicos aparentemente enviados por ENDESA.

   Se han atendido las comunicaciones, consultas y reclamaciones tanto de clientes como de no clientes asociadas a la recepción de los citados emails fraudulentos.

   Se ha realizado una campaña de comunicación masiva a todos los niveles alertando sobre esta acción fraudulenta :

   Redes sociales: Facebook, Twitter y, en menor medida, Linkedin..

   Páginas corporativas (Intranet y página web endesaclientes). Señalan que en el sitio web www.endesaclientes.com se ha incluido, en forma destacada, un aviso informando que no de una factura real emitida y enviada por ENDESA sino un fraude, modo cómo opera el virus y advirtiendo que debe pulsarse ningún enlace de los correos electrónicos recibidos. Igualmente, se informa sobre cómo se puede intentar recuperar los datos a través del INCIBE.

   Medios de comunicación: Agencias EFE y Europapress.

   Se han remitido correos electrónicos informativos individualizados tanto a los empleados como a los clientes con el texto cuya impresión se aporta, en el que se recomienda "*no hacer clic en los enlaces de ningún eMail de factura que no cumpla que el remitente sea "Endesa Online" gestiononline@endesaonline.com".*

   Se ha desarrollado un trabajo conjunto con el INCIBE para dar soporte a los usuarios afectados. Se adjunta impresión del comunicado remitido a los medios de comunicación en el que se informa de cómo actuar en caso de infección del virus.

6. Respecto de contactos, consultas y reclamaciones ENDESA indica:

   Los contactos recibidos en "Canales Digitales" de clientes con motivo del virus no han sido para presentar reclamaciones, sino para solicitar información sobre el correo electrónico fraudulento y el modo de actuar. En todos estos casos, se ha facilitado la información ya expuesta.

   Desde la Dirección General de Atención al Cliente (ATC) se ha comunicado a los responsables de las distintas Unidades de Reclamaciones la información necesaria (argumentarios) para atender cualquier consulta o reclamación relativa al mismo.

   Se han atendido telefónicamente las reclamaciones registradas en el documento

que se adjunta conforme los argumentarios elaborados al efecto.

7. Por último, presentan las impresiones de pantalla solicitadas por la AEPD en su requerimiento de información referentes a los cuatro Denunciantes. Se destaca que sólo el Denunciante 1 tiene activada la factura digital y que el Denunciante 2 no es cliente desde septiembre de 2012.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver la Directora de la Agencia Española de Protección de Datos, conforme a lo establecido en el artículo 37.d) en relación con el artículo 36, ambos de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD).

El artículo 126.1, apartado segundo, del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, aprobado por Real Decreto 1720/2007, de 21 de diciembre, (en lo sucesivo RLOPD), de protección de datos de carácter personal establece:

Si de las actuaciones no se derivasen hechos susceptibles de motivar la imputación de infracción alguna, el Director de la Agencia Española de Protección de Datos dictará resolución de archivo que se notificará al investigado y al denunciante, en su caso.

II

El artículo 9 de la LOPD establece:

"1. El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley."

En el Título VIII del Reglamento de desarrollo de la LOPD, aprobado mediante Real Decreto 1720/2007, de 21 de diciembre, se detallan los requisitos de seguridad que han de reunir los ficheros y tratamientos de datos de carácter personal, en función de la tipología de los datos involucrados.

En el presente caso de las actuaciones practicadas se desprende que no hay elementos de prueba que permitan afirmar que los correos electrónicos de los denunciantes tratados para la remisión de los envíos maliciosos aportados por los

denunciantes procedan, en forma indubitada, de los ficheros de clientes, o de otros sistemas informáticos, de la entidad denunciada.

Por el contrario, ENDESA ha justificado que dichos envíos, aparentemente realizados por esa entidad, se enmarcan en una campaña fraudulenta de envío masivo de correos electrónicos simulando avisos de facturas de ENDESA que se remitieron desde dominios fraudulentos a destinatarios indiscriminados.

Como prueba fundamental de sus manifestaciones, ENDESA ha indicado que dichos envíos maliciosos se realizaron tanto a clientes o antiguos clientes de la denunciada- caso de los Denunciantes 1, 2 y 3, como a personas físicas que no habían mantenido relación contractual con la supuesta remitente de los envíos, caso del Denunciante 4 y de otros afectados que también reclamaron ante la entidad. Asimismo, conforme ha advertido ENDESA, las facturas fraudulentas contienen datos falsos, dándose la circunstancia de que en el caso de los Denunciantes 1 y 4 que el dato del CUPS de facturación eléctrica reflejado en cada resumen de las facturas aportadas es distinto, ocurriendo, además, en el caso del Denunciante 1 que ninguno de los CUPS reflejados en los resúmenes de las facturas presentadas coincide con el realmente asociado a su contrato de suministro. Igualmente, se ha comprobado que los datos relativos al código de cliente que figuran en los citados resúmenes son diferentes en cada uno de los envíos recibidos por los Denunciantes 1 y 4. Además, se ha verificado que en los resúmenes de las facturas aportadas por los cuatro Denunciantes no se identifica con nombre y apellidos al titular del punto de suministro, amén de que de los cuatro Denunciantes únicamente uno tiene activada la factura digital, a pesar de que los envíos se refieren a la "Factura electrónica de Endesa".

Por lo que de lo actuado no se evidencian elementos de prueba de que el tratamiento de las direcciones de correo electrónico de los denunciantes por el tercero remitente de los envíos simulando avisos de facturas electrónicas de ENDESA haya tenido su origen en una quiebra de las medidas de seguridad aplicables a los ficheros de esa compañía, ya que además de los razonamientos expresados, no está acreditado que terceros hayan accedido a la información obrante en los ficheros titularidad de esa empresa o que desde los mismos se haya producido una fuga de información.

Por otra parte, consta que ENDESA ha denunciado ante la Dirección General de la Policía el uso fraudulento y suplantación de la marca de las empresa del grupo con el fin de propagar una campaña fraudulenta de alta repercusión social, desconociéndose, en todo caso, la identidad del remitente responsable de la campaña en la que se enmarcan los envíos denunciados.

Paralelamente, consta documentado en el expediente la rápida actuación desplegada por la denunciada tan pronto como tuvo conocimiento de la existencia de dicha campaña, adoptando una batería de medidas tendentes a informar a los posibles afectados a través de diversos medios y ofrecer posibles alternativas de solución, atendiendo también las consultas y reclamaciones de los afectados, fueran o no clientes de la empresa.

En conclusión, no se advierte vulneración a lo previsto en el artículo 9 de la LOP por parte de ENDESA ENERGÍA, S.A.U., procediendo, por tanto, el archivo de las actuaciones practicadas.

Por lo tanto, de acuerdo con lo señalado,

Por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PROCEDER AL ARCHIVO de las presentes actuaciones.

NOTIFICAR la presente Resolución a **ENDESA ENERGÍA, S.A.U. junto con el Anexo I** y a los **Denunciantes 1, 2, 3 y 4 junto con sus respectivos Anexos II, III, IV** y **V.**

De conformidad con lo establecido en el apartado 2 del artículo 37 de la LOPD, en la redacción dada por el artículo 82 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, la presente Resolución se hará pública, una vez haya sido notificada a los interesados. La publicación se realizará conforme a lo previsto en la Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones y con arreglo a lo dispuesto en el artículo 116 del Reglamento de desarrollo de la LOPD aprobado por el Real Decreto 1720/2007, de 21 diciembre.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en los artículos 112 y 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, 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 del referido texto legal.

Mar España Martí
Directora de la Agencia Española de Protección de Datos