- **Procedimiento Nº: E/00216/2021**

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 Agencia Española de Protección de Datos (en adelante, AEPD), de una brecha de seguridad de datos personales por parte del Responsable del Tratamiento INGBANK N.V. SUCURSAL EN ESPAÑA (en adelante ING), con número de registro de entrada O00007128e2000013610, relativa a un ciberincidente que afecta la confidencialidad de las cuentas de clientes, 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:

Resumen de la notificación:

Con fecha 4 de diciembre de 2020 se recibe en la Agencia una reclamación presentada por ING en la que se pone de manifiesto que, el día 3 de diciembre, se ha detectado un número masivo e inusual de solicitudes de contratación de productos de potenciales clientes (unas 100.000), a través de la web. Se utilizaron DNIs reales y direcciones de email que han podido ser obtenidos a través de alguna fuga de datos producida en otra compañía. Estas contrataciones no han llegado a formalizarse. Asimismo consideran que el objetivo de los intentos de contratación ha sido identificar clientes reales de ING incluidos en la base de datos de los atacantes. Este ataque se realizó a través de diferentes direcciones IP comprometidas procedentes de Italia, Argentina, Francia y Reino Unido. ING declara que el proceso de contratación prevé que cuando un potencial cliente facilita sus datos en la web, automáticamente, se le envía un email para informarle de la política de protección de datos. Este mail ha supuesto que algunos de los afectados, al no entender la razón de su recepción, se hayan puesto en contacto con ING. Manifiestan haber tomado medidas para detectar este ataque y bloquearlo, así como medidas tendentes a informar tanto a los potenciales clientes afectados (100.000 aprox.) como a 815 clientes sobre los que se ha tenido constancia de que los atacantes han conocido que sí son clientes de ING, con el fin de evitar que sean víctimas de actividades fraudulentas posteriores.

El 28 de diciembre de 2020 se recibe una ampliación de la reclamación y se aporta denuncia presentada ante el Grupo de Delitos Telemáticos de la Policía Nacional, en fecha 19 de diciembre de 2020, sobre estos mismos hechos, solicitando la investigación de un listado de direcciones IP origen del ataque.

ENTIDAD INVESTIGADA:

Durante las presentes actuaciones se ha investigado la siguiente entidad: ING BANK N.V., SUCURSAL EN ESPAÑA con NIF W0037986G con domicilio en C/ SEVERO OCHOA N.º 2 - 28232 LAS ROZAS DE MADRID (MADRID)

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1.- Con fecha 19 de enero de 2021 se solicitó información a ING BANK N.V., SUCURSAL EN ESPAÑA (en adelante el responsable) y de la respuesta recibida se desprende lo siguiente:

Respecto de la empresa.

- La aplicación a través de la cual se encuentra la funcionalidad de alta de solicitudes de contratación ha sido desarrollada internamente por el responsable.

Respecto de la cronología de los hechos:

Acciones tomadas con objeto de minimizar los efectos adversos y medidas adoptadas para su resolución final:

El responsable ha aportado informe con el resumen de los hechos en el que figura:

- Durante los días 2 y 3 de diciembre de 2020 se detecta un número masivo e inusual de tráfico proveniente de multitud de direcciones IPs procedentes de Italia, Argentina, Francia y Reino Unido. A través de dichas IPs se estaban realizando numerosos intentos de alta de clientes. Todas esas IPs estaban asociadas a routers residenciales que se ha detectado tenían una vulnerabilidad que permite tomar el control de dichos routers para crear “botnets” desde los que realizar ataques por fuerza bruta.

- El responsable comenzó a recibir comunicaciones de personas que informaban estar recibiendo un correo electrónico porque habían aportado datos en la web, indicando que no habían realizado dicha acción. La remisión del mail del responsable forma parte del proceso de solicitudes de contratación.

- Inmediatamente se procedió a llevar a cabo, entre otras, las siguientes acciones:

    - o Cierre temporal del proceso de contratación a través de la web para evitar nuevos intentos y cierre si el acceso se realiza desde IPs geolocalizadas fuera de España.

    - o Bloqueo de las direcciones IP desde las que se estaba recibiendo el ataque.

    - o Bloqueo de las cuentas bancarias de los 815 clientes respecto de los cuales los atacantes habrían conseguido ser redirigidos a la página de Área de cliente (sin acceder a la misma), con el fin de que no pudieran operar y que, en el caso de que lo hicieran, se les mostrara un mensaje de error. A su vez, a estos clientes, se les envió un correo electrónico solicitándoles que se pusieran en contacto con la entidad por motivos de seguridad

    - o Monitorización de logs.

    - o Creación de nuevas alertas de denegación de servicios.

• Posteriormente se realizaron acciones para desbloquear las cuentas de los 815 clientes y extracciones de las solicitudes realizadas los días 2 y 3 de diciembre bloqueando los datos.

Respecto de las causas que hicieron posible la brecha:

• El responsable manifiesta que, tras el análisis, han concluido que estos hechos han sido posibles porque los atacantes disponían de una base de datos ajena a la entidad, y estuvieron intentando hacer uso y explotar el proceso de solicitudes de contratación en la página web, con el fin de identificar del listado completo cuáles de ellos eran clientes para, presumiblemente, llevar a cabo un uso malicioso posterior

• Se confirmó que ninguno de los intentos de alta masiva de contratación de productos logró finalizarse ni se detectó ninguna actividad fraudulenta o sospechosa en relación con los ya clientes, y que sus datos ya obraban también en la base de datos de los atacantes.

• La conclusión de la entidad es que se produjo un ataque de fuerza bruta dirigido y distribuido con el objetivo de intentar identificar clientes del responsable, de la base de datos que ya disponían los atacantes.

Respecto de los datos afectados:

• Se crearon 185.058 códigos de cliente entre el 2 y el 3 de diciembre, es decir, se produjeron ese número de intentos de alta del producto Cuenta Nómina, pero ninguna se formalizó.

• De todos los intentos realizados, los atacantes disponían ya del DNI y de la fecha de nacimiento correcta de 815 clientes.

• Los datos corresponden a DNI, fecha de nacimiento (en alguno de los casos) y dirección de correo electrónico. Estos datos no fueron obtenidos de la entidad ING sino que ya obraban en poder de los atacantes. Tras el intento de ataque, los atacantes no obtuvieron más datos ni información adicional.

• La entidad manifiesta que los hechos producidos no han tenido ninguna consecuencia grave para los afectados más allá de la recepción del correo electrónico con la política de privacidad.

• Para los 815 clientes se puso en marcha un proceso de monitorización específica y no se ha detectado ninguna acción fraudulenta sobre sus cuentas. El responsable manifiesta que les contactó para informarles de la situación y de cómo proceder en el caso de que detectaran algún movimiento o actuación sospechosa en sus cuentas.

• Asimismo manifiestan que desconocen el origen de los datos utilizados por los atacantes y confirman que no fueron obtenidos de la entidad.

• Los atacantes no han obtenido ninguna información de los clientes, por lo que no se ha publicado información en Internet.

• La entidad ha aportado todas las comunicaciones que se remitieron a los afectados como consecuencia de este incidente, explicando el canal por el que se remitieron: información publicada en redes sociales; mail informativo remitido a empleados del

responsable; mail informativo remitido a todos los clientes afectados con la resolución de la incidencia y consejos de seguridad; modelo de contestación para aquellos clientes o afectados no clientes que se dirigieron al responsable a través de los buzones del Delegado de Protección de Datos para informarse de lo ocurrido o ejercitar sus derechos de acceso o supresión.

Respecto de las medidas de seguridad implantadas:

- Con anterioridad a la brecha, el responsable, a nivel de Grupo, dispone de un "Marco normativo" relativo a riesgos información que se compone de dos Políticas, una de "Procesamiento de la Información" y otra de "Seguridad IT".
- Asimismo, tenía implantadas medidas de seguridad cuyo listado completo consta en la documentación aportada. Estas medidas se agrupan en los siguientes apartados:
    - o Gestión de riesgos de la información: clasificación de la información, BIA (Business Impact Assesment), formación y concienciación.
    - o Gestión de la configuración.
    - o Gestión de identidades y acceso, entre ellas, mecanismo de autenticación y almacenamiento seguro de credenciales.
    - o Seguridad de la plataforma.
    - o Gestión de cambios respuesta a incidentes de ciberseguridad, entre ellas, análisis y prueba de amenazas y denegación de servicios.
    - o Monitorizaciones de seguridad.
- Ponen de manifiesto que realizan test de penetración, el último en diciembre 2020, realizado por una tercera entidad especializada. También se realizó un test de penetración con anterioridad, en mayo 2020, por un empresa del Grupo especializada en auditorías de seguridad. En ninguno de los dos test de penetración se realizaron recomendaciones relevantes.
- Documentos aportados
    - o Registro de actividad del tratamiento Gestión de la información relativa a clientes para la contratación de productos.
    - o Evaluación de Impacto realizada en relación con el proceso de contratación de productos
    - o Procedimiento de identificación, gestión y notificación de Brechas de Seguridad de Datos Personales.
    - o Guía simplificada de actuación ante brechas de seguridad.
- El responsable manifiesta que no ha habido ningún incidente de seguridad ya que los procesos de monitorización a nivel de seguridad funcionaron y alertaron de la situación, y que con posterioridad a la brecha no ha sido necesario tomar medidas técnicas ni organizativas para evitar incidentes de este tipo ya que no se ha tratado de un incidente de seguridad. Sin embargo, de cara a poder identificar este tipo de hechos que suponen ataques masivos con mayor rapidez, se han creado unas alertas asociadas al proceso de alta.

Respecto de la notificación con posterioridad a las 72 horas:

ING manifiesta que no se ha notificado a la AEPD como brecha de seguridad ya que consideran que los hechos ocurridos no han sido consecuencia de un incidente de seguridad, sino que ha sido una actividad llevada a cabo por terceros que obtuvieron una base de datos externa e introdujeron los datos de los que disponían en el proceso de contratación de productos de la web, posiblemente para verificar si dichas personas eran o no clientes. Asimismo manifiestan que contactaron con la propia Agencia la cual también considero que no era una brecha de seguridad pero que sería conveniente ponerlo en conocimiento de la AEPD, motivo por el cual y de forma proactiva se presentó una denuncia el 4 de diciembre y posteriormente se amplió aportando la denuncia presentada ante la Policía con fecha 28 de diciembre de 2020.

Información sobre la recurrencia de estos hechos y número de eventos análogos acontecidos en el tiempo:

No han tenido con anterioridad, casos de esta magnitud, análogos a los aquí descritos.

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 artículo 4 apartado 12 del 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.”*

Hay que señalar, que la notificación de una quiebra de seguridad no implica la imposición de una sanción de forma directa, ya que es necesario analizar la diligencia de responsables y encargados y las medidas de seguridad aplicadas.

La seguridad de los datos personales viene regulada en los artículos 32, 33 y 34 del RGPD, que regulan tanto la seguridad del tratamiento, la notificación de una violación de la seguridad de los datos personales a la autoridad de control, así como la comunicación al interesado.

En el presente caso, consta una brecha de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como una brecha de confidencialidad,

como consecuencia del acceso indebido por terceros ajenos a la base de datos de ING.
Tras el requerimiento de información llevado a cabo por la Inspección de esta AEPD, la entidad investigada ha informado de todas las actuaciones llevadas a cabo para paliar el incidente.

De la documentación aportada por la entidad investigada en el curso de estas actuaciones de investigación se desprende que, con anterioridad a producirse la brecha, ING disponía de medidas de seguridad y organizativas preventivas razonables a fin de evitar este tipo de incidencias, y acordes con el nivel de riesgo.

Con posterioridad al incidente, y de cara a poder identificar este tipo de hechos que suponen ataques masivos con mayor rapidez, se han creado unas alertas asociadas al proceso de alta.

No constan reclamaciones ante esta AEPD por parte de posibles clientes afectados

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 INGBANK N.V. SUCURSAL EN ESPAÑA con NIF W0037986G.

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