- **Procedimiento Nº: E/05762/2020**

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 Unidad de Evaluación y Estudios Tecnológicos de la Agencia Española de Protección de Datos (en adelante, AEPD) de una brecha de seguridad de datos personales por parte del responsable del tratamiento HEXAMOB, S.L., con número de registro de entrada 021752/2020, relativa a la pérdida de confidencialidad de datos personales en entorno de desarrollo con datos reales, la Directora de la AEPD ordenó el 29/06/2020 a la de Inspección de Datos que valorase 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: jaqueo sufrido en una base de datos de preproducción que ha supuesto la desaparición de todos los datos contenidos en la misma y la extorsión a cambio del rescate de dichos datos.

Documentación aportada:

- Archivo de texto que, según el responsable del tratamiento, supone presunta reproducción de los contenidos de los mensajes remitidos a los usuarios y a los clientes en relación con la brecha de seguridad sufrida.

ENTIDADES INVESTIGADAS

Durante las presentes actuaciones se han investigado las siguientes entidades:

HEXAMOB, S.L. (en adelante, la investigada), con NIF B12929881 y domicilio en C/ MONESTIR DE POBLET, 13 1º B - 12540 VILLAREAL (CASTELLÓN).

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

Respecto de la entidad implicada:

- La investigada se presenta públicamente como una empresa de desarrollo de aplicaciones y juegos para *Android*, *iOS* y *Windows Phone*, así como de diseño profesional y *hosting* web (https://hexamob.com/es/).

- La investigada se identifica como conformada por dos desarrolladores informáticos, en la que cualquier acción acerca de la protección de datos personales se la consultan a una tercera empresa especializada en ese tema.

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

Todo según manifestaciones de la investigada:

- 21/06/2020: la reclamada informa que mientras trabajaba en un proyecto web con una base de datos (en adelante, BBDD), en servidores de producción, que estaba protegida, no había ningún problema ya que toda la gestión estaba delegada en la empresa proveedora de los servicios de almacenamiento de datos que tiene sus propios sistemas de seguridad. Sin embargo, la reclamada reconoce que tuvo que levantar en el servidor web una BBDD en un entorno de preproducción con registros exportados de la BBDD original para trabajar en diseños de pantallas y pruebas de rendimiento.

- 22/06/2020: la reclamada expone que al intentar conectare a la BBDD para continuar con el trabajo comenzado el día anterior, la BBDD de desarrollo estaba borrada y contenía un mensaje de extorsión por parte de un jáquer. La investigada añade que seguía poseyendo en producción los datos de los clientes porque el jáquer no había accedido a la BBDD real, si no a la copia parcial de los mismos utilizada para trabajar en preproducción (diseños de pantallas y pruebas de rendimiento).

  La investigada defiende que, en el momento de detección de la incidencia, procedió a desconectar la BBDD afectada (de desarrollo/preproducción) y la eliminaron de sus equipos, así como procedió a informar a los usuarios de la plataforma web de que se había producido dicha incidencia para que, por seguridad, cambiaran las contraseñas de acceso.

  La investigada manifiesta haber procedido a informar a sus clientes para que, como medida de precaución, solicitaran el cambio de las claves secretas de los TPV (terminal punto de venta) virtuales que utilizan en sus webs. Asimismo, la investigada refiere haber solicitado los cambios de contraseñas de acceso a los paneles de gestión de los TPV virtuales como medida de seguridad.

  La investigada expresa haber contactado telefónicamente con la AEPD antes de notificar la brecha de seguridad, confirmando la necesidad de ser notificada. La investigada informa de haber mantenido conversaciones con la empresa que le gestiona lo referente a la protección de los datos personales para obtener orientaciones sobre cómo proceder.

- 25/06/2020: la reclamada notificó la brecha de seguridad en cuestión a la AEPD.

Respecto de las causas que hicieron posible la brecha

- La investigada explica llevar años trabajando en el desarrollo del proyecto web en el que se produjo la incidencia y que nunca habían tenido alguna similar, puesto que entienden que los datos están protegidos en el entorno de producción con sus medidas de seguridad y las propias del proveedor de servicios contratado.

Respecto de los datos afectados

- La investigada notificó a la AEPD que en esta brecha de seguridad:
    - El número aproximado de personas afectados fue de 10.512.
    - Los datos personales afectados se categorizaron en:
        - Datos básicos
        - DNI, NIE y/o Pasaporte
        - IBAN (número de cuenta bancaria internacional)
    - El perfil de los sujetos afectos se correspondía con el de:
        - Clientes.
        - Usuarios.
        - Menores.
- La investigada señaló que la severidad de las consecuencias para los individuos afectados por la brecha de seguridad era baja.
- La investigada manifiesta no tener conocimiento de la utilización por parte de terceros de los datos personales parciales que pudieron ser sustraídos en la incidencia producida.
- La investigada expone no disponer de indicios respecto a que se haya publicado en Internet o de que se haya indexado en algún buscador la información parcial sustraída en la incidencia.

Respecto de las medidas de seguridad implantadas previamente al acontecimiento de la brecha de seguridad:

- La investigada indica que los datos personales en producción se encuentran protegidos por el almacenamiento en servidores de su proveedor de servicios

de BBDD, el cual tiene sus propios sistemas de seguridad. La investigada identificada como proveedor se dichos servicios a ******EMPRESA.1*** y los servicios contratados: ******EMPRESA.2***

- La investigada aporta copia de su registro de actividades del tratamiento referida a las actividades de tratamiento "Usuarios web" y "Clientes y/o proveedores".

- La investigada informa de no disponer de Análisis y Gestión de Riesgos ni de Evaluación de Impacto relativa a la Protección de Datos.

- La investigada expresa que la seguridad está configurada en el servicio que le aporta el proveedor de bases de datos. Por su parte, la investigada manifiesta proteger por IP (protocolo de internet) el acceso a las bases de datos que maneja, disponer de los datos cifrados, utilizar certificados de seguridad y acceder con doble autenticación a los servicios externos. La investigada afirma tomar precauciones durante el proceso de trabajo que se realiza a diario**.**

- La investigada informa no realizar auditorías periódicas debido a que, según su criterio, la seguridad a nivel de BBDD corresponde a la empresa proveedora del servicio. La investigada añade tener constancia de que dicho nivel de seguridad es alto y fiable y que [sic]: *"La brecha de seguridad fue un descuido por parte nuestra."*

Respecto de las medidas de seguridad de tipo correctivo implantadas posteriormente al acontecimiento de la brecha de seguridad:

- La investigada manifiesta haber:

    - Parado el acceso a la BBDD de desarrollo inmediatamente para que no se pudiera acceder a la información.

    - Eliminado la BBDD de desarrollo (al ser una prueba temporal).

    - Avisado a los clientes y usuarios.

    - Solicitado a los usuarios un cambio de contraseñas de acceso.

    - Solicitado a nuestros clientes un cambio de contraseña de TPV.

    - Avisado a la AEPD.

- La investigada asevera que el mantenimiento de seguridad de la BBDD de prueba no existe puesto que era únicamente una copia parcial y modificada, utilizada temporalmente para probar unas pantallas. La investigada añade que dicha BBDD de prueba se elimina al terminar de realizar las pruebas pertinentes en el sistema, con lo que, según su criterio, los datos reales están en producción.

- La investigada aporta las siguientes capturas de pantalla respecto a la comunicación a los afectados: Mensaje enviado a los usuarios según su versión:

De: AMPA DEMO3 <ampademo3@miampa.com>
Fecha: 22 de junio de 2020, 20:42:17 CEST
Para: [redacted]
Asunto: CAMBIO DE CONTRASEÑA URGENTE

Buenas tardes:

Nos han informado que en las últimas horas se han detectado un incremento en los ataques a servidores de Internet intentando acceder a los datos de los usuarios y los expertos recomiendan principalmente que se modifiquen lo antes posible las contraseñas de acceso de usuario como principal medida de seguridad. No tenemos constancia de que nuestra base de datos de producción se haya visto comprometida por este tipo de ataques pero siempre es mejor tomar precauciones y seguir las recomendaciones de los expertos. Por tanto, os pedimos que modifiquéis la contraseña de acceso a la web o APP del AMPA como medida de precaución.

Un abrazo y cualquier duda estamos a vuestra disposición.

- Mensaje enviado a los clientes según su versión:

info@miampa.com <hexamob.miampa@gmail.com> lun., 22 jun. 17:29 Responder
para bcc: AMIPA, bcc: [redacted] bcc: AMPA, bcc: ceip.ampa[redacted], bcc: AMPA, bcc: AMPA, bcc: AMPA, bcc: AMPA, bcc: AMPA, bcc: AMPA

Estimada AMPA:

Os enviamos este correo electrónico para informaros de que tenéis que haber recibido un correo electrónico con una nueva contraseña para acceder al panel del TPV virtual.

En los últimos días se han detectado ataques avanzados a servidores intentando acceder a la configuración de los TPV virtual y **los expertos recomiendan que se realicen las siguientes acciones:**

1.- Cambiar la contraseña de acceso al panel de TPV virtual. (COMPLETADO)

2.- Solicitar a soportevirtual@redsys.es el cambio de claves secretas del TPV virtual.

El primer paso **lo hemos realizado por vosotros pero el segundo tenéis que hacerlo desde el correo electrónico que disteis a vuestro banco al dar de alta el TPV virtual.**

A día de hoy, no tenemos constancia de que nuestra base de datos de producción se haya visto afectada por este tipo de ataques. Aún así, es mejor seguir las recomendaciones de los expertos por seguridad.

Por favor, realizad esta segunda acción lo antes posible y **en cuanto tengáis la respuesta de redsys indicando que ya tenéis las nuevas claves nos aviséis enviándonos la nueva contraseña de acceso al panel de TPV virtual para poder coger las claves secretas y configurar vuestra web y APP con ellas** para que podáis recibir los pagos de vuestras familias.

Aquí os dejamos un texto de ejemplo sobre cómo solicitar a redsys el cambio de claves secretas:

Estimado equipo de soporte de Redsys:

Nuestro proveedor de servicios ha hablado con vosotros y tal y como le han confirmado por temas de seguridad solicitamos el cambio de las claves secretas de nuestro TPV virtual a la mayor celeridad posible.

Saludos

Respecto de las medidas de seguridad de tipo preventivo implantadas posteriormente al acontecimiento de la brecha de seguridad:

- La investigada expone que:

  - Eliminó la BBDD de preproducción y en lugar de descargar copias parciales para realizar pruebas, en adelante, hará consultas que se traigan ciertos datos a la pantalla en cuestión. De ese modo, según su versión, los datos seguirán en el entorno seguro del proveedor de BBDD.

  - Ha migrado los servidores de desarrollo.

  - Actualizó los servidores de producción.

  - Ha añadido cortafuegos para elevar el sistema de seguridad en el acceso a los servidores.

  - Ha bloqueado el acceso por IP a los servidores, por lo que tan sólo pueden acceder los dos desarrolladores.

  - Se realizan copias automáticas de los datos

  - Los datos de preproducción son anónimos generados automáticamente.

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

- La investigada manifiesta que en su entidad no se han producido hechos similares a lo largo del tiempo

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.

La investigada aporta copia del RAT referida a las actividades de tratamiento "Usuarios web" y "Clientes y/o proveedores." Asimismo indica que aunque los datos personales en producción se encuentran protegidos por el almacenamiento en servidores de su proveedor de servicios de BBDD, no obstante protege el acceso a BBDD con varias medidas, entre ellas con el cifrado de datos y con el uso de certificado de seguridad. De todo ello se desprende que, con anterioridad a producirse la brecha, la investigada disponía de medidas de seguridad razonables en función de los riesgos estimados.

La brecha fue posible al tener que levantar en el servidor web una BBDD en un entorno de preproducción con registros exportados de la BBDD original para trabajar en diseños de pantallas y pruebas de rendimiento y al intentar conectarse el día siguiente a la BBDD para continuar con el trabajo, estaba borrada y contenía un mensaje de extorsión por parte de un jáquer.

La investigada añade que seguía poseyendo en producción los datos de los clientes porque el jáquer no había accedido a la BBDD real, si no a la copia parcial de los mismos, utilizada para trabajar en preproducción (diseños de pantallas y pruebas de rendimiento).

Tras conocerse el incidente se actúa con diligencia, procediendo a desconectar la BBDD afectada (de desarrollo/preproducción) y a eliminarla de sus equipos, así como a informar tanto a los usuarios de la plataforma web para que cambiaran las contraseñas de acceso, como a los clientes para que solicitaran el cambio de las claves secretas de los TPV. Asimismo, la investigada refiere haber solicitado los cambios de contraseñas de acceso a los paneles de gestión de los TPV virtuales como medida de seguridad.

Se han visto vulnerados datos básicos, DNI, y el IBAN, referidos a 10512 personas entre clientes, usuarios y menores. Aunque., no se tienen, indicios de la utilización por parte de terceros de la información.ni de que esta se haya publicado en internet o

indexado en buscadores, considerando la investigada que el impacto para los afectados es bajo.

Para evitar que estos hechos se repitan, se han tomado una serie de medidas, entre ellas, la eliminación de la BBDD de preproducción pasando a hacer consultas que traigan los datos a la pantalla. manteniendo así los datos en el entorno seguro del proveedor de BBDD, se bloquea el acceso por IP a los servidores de modo que solo puedan acceder los desarrolladores, se realizan copias automáticas de datos y los datos de preproducción son anónimos generados automáticamente.

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, notificar a la AEPD y organizar la comunicación a los distintos tipos de afectados.

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 HEXAMOB, S.L., con NIF B12929881

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