Procedimiento Nº: E/06276/2019
940-0419

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: Las actuaciones de inspección se inician con la recepción de un escrito de notificación de quiebra de seguridad remitido por ENGLISH WORLDWIDE SL (en adelante ENGLISH) en el que informan a la Agencia Española de Protección de Datos que, con fecha 29 de mayo de 2019, han recibido un correo electrónico de un *"hacker ético"* informando sobre una brecha de seguridad que permite el acceso a la base de datos de la compañía a través de la técnica "*inyecciones de SQL".* El hacker podría haber tenido acceso al nombre y apellidos, dirección de mail y contraseña cifrada de unos 3.533 usuarios.

El 30 de mayo de 2019, a las 9:30, ENGLISH confirma la brecha y se identifican los datos accedidos por el *hacker.* Concluyen que el ataque ha sido por "*inyección de SQL*" a un sistema de información antiguo.

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:

ANTECEDENTES

Fecha de notificación de quiebra: 31 de mayo de 2019

ENTIDADES INVESTIGADAS

ENGLISH WORLDWIDE, S.L. con NIF B64401482 con domicilio en ARIBAU, NUM 240, PISO 7 - 08006 BARCELONA (BARCELONA)

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1. Con fecha 4 de julio de 2019 se requiere información a ENGLISH y desprende lo siguiente :

   Respecto de la cronología de los hechos

   - El 29 de mayo de 2019 a las 15:50 la entidad ha recibido un correo electrónico de la empresa de seguridad BULWARKERS que oferta servicios para reparar una vulnerabilidad detectada en una de sus webs (abaenglish.com) y le remiten un extracto de las bases de datos a las que han tenido acceso donde figuran los datos personales y de credenciales de usuarios de ENGLISH.

A este respecto, han aportado correos intercambiados con dicha compañía (dominio *bulwarkers.com*).

- El 30 de mayo de 2019 a las 9:30 ENGLISH confirma la brecha y se identifican los datos accedidos por el *hacker.* Concluyen que el ataque ha sido a través de la técnica de "*inyección de SQL*" a un sistema de información antiguo.

  En este momento contratan con el Instituto Nacional de Ciberseguridad (INCIBE) para la elaboración del informe sobre la brecha de seguridad detectada.

- El 31 de mayo de 2019 a las 17:00 se finaliza la reparación de los archivos que han sufrido el ataque y se implanta una herramienta para impedir nuevos ataques por *inyección de SQL.*

  Ese mismo día se comunica la incidencia a los 3.533 afectados. La compañía ha aportado a esta Agencia escrito remitido a los afectados donde se les informa del incidente de seguridad y se recomienda el cambio de contraseña para el acceso a las Plataformas de ENGLISH.

  Se procede a la notificación de brecha a la Agencia Española de Protección de Datos

- El 7 de junio de 2019, INCIBE hace entrega del informe elaborado con motivo de la incidencia, y entre otros aspectos, indica que el número de registros afectados corresponde a 43.538 (datos de 39.427 personas)

  Por ello, proceden a notificar la incidencia a las 39.427 personas y, debido al volumen, se realizan en tres envíos durante los días del 7 al 9 de junio de 2019.

- El 10 de junio de 2016, se comunica una notificación adicional a la Agencia.

<u>Respecto de la categoría de los datos afectados</u>

- Los datos a los que se ha tenido acceso corresponden a: Nombre y apellidos, dirección de correo electrónico y contraseñas de los usuarios y la contraseña y datos personales de un empleado de la entidad (CEO de ENGLISH).
- ENGLISH manifiesta no tener conocimiento de que la información filtrada haya sido utilizada por terceros
- ENGLISH manifiesta no tener conocimiento de que los datos personales obtenidos a causa del incidente de seguridad hayan sido indexados por buscadores.

<u>Respecto del informe del INCIBE.</u>

- Se procede al estudio de los registros de accesos (logs) detectando que el 29 de mayo de 2019 entre las 9:00 y las 15:00 se realiza un volumen de peticiones mayor que la media desde la misma dirección IP.
- El análisis de los logs durante este periodo de tiempo demuestra que el atacante utilizó diversas herramientas en busca de una vulnerabilidad a *inyección de SQL,* y una vez encontrada construye la petición de acceso a

las bases de datos descargándose la información. Asimismo, verifican que el atacante realiza peticiones para acceder a la contraseña de un empleado, así como a sus datos personales por lo que concluyen que también se ha podido obtener esta información.

- También se procede al estudio de las contraseñas y comprueban que el acceso a estos datos en la *extranet* es complicado ya que se encuentran protegidas por una herramienta criptográfica.

  No obstante, en una de las tablas a las que se ha accedido en el incidente, las contraseñas se encuentran codificadas (*hash*) sin una herramienta adicional para su protección por lo que pueden ser recuperables.

- Descartan otras acciones que no estén vinculadas a *inyecciones SQL.*

- El INCIBE propone las siguientes recomendaciones.

  - ✓ Revisión código aplicación web
  - ✓ Revisión de peticiones y almacenamiento de la dirección IP desde la que se hace la petición.
  - ✓ Alertas vinculadas a actividad anómala.
  - ✓ Revisión de seguridad de las aplicaciones webs.

Respecto de las medidas de seguridad implantadas con anterioridad al incidente

- ENGLISH tiene suscrito un contrato de almacenamiento en *cloud* con Amazon para el servicio AWS que necesariamente obliga, entre otros, a mantener un protocolo de seguridad SSL (protocolo criptográfico que proporciona comunicaciones seguras).

- ENGLISH mantenía las bases de datos de las contraseñas cifradas y las contraseñas para el acceso a través de la *extranet* se encontraban protegidas adicionalmente con una herramienta de seguridad criptográfica.

- ENGLISH ha aportado copia del Registro de Actividad del fichero de Estudiantes y de actividad formativa y del procedimiento en caso de violaciones de seguridad.

- Respecto del análisis de riesgo, la compañía concluyó que no estaban obligados a realizarlo ya que los tratamientos eran prexistentes al 25 de mayo de 2018.

Otros aspectos

- La dirección IP desde la que se hacen las peticiones de acceso el 29 de mayo de 2019 se encuentra asociada a una entidad ubicada en Australia (Melbourne).

- La empresa BULWARKERS tiene su domicilio en la India.

  Tal y como consta en su página web bulwarkers.com, la empresa se dedica a temas de seguridad informática.

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

En el presente caso, tras el requerimiento de información llevado a cabo por la inspección de esta AEPD, la entidad ENGLISH ha informado de las investigaciones internas realizadas y resultado de las mismas.

Hay que destacar del análisis realizado la detección del método de intrusión utilizado, *sql inyection*, lo que ha permitido configurar el sistema de información de forma adecuada para evitar su repetición. Se debe señalar, que la vulnerabilidad se ha detectado en un antiguo sistema de información actualmente inactivo, con datos básicos de usuarios.

Consta que la entidad mantenía implantado en el Sistema de Información atacado un protocolo de seguridad SSL (protocolo criptográfico que proporciona comunicaciones seguras), cifradas las bases de datos de contraseñas y protegidas adicionalmente con una herramienta de seguridad criptográfica, y el 31 de mayo de 2019 se finaliza la reparación de los archivos que han sufrido el ataque implantándose una nueva herramienta de seguridad para impedir nuevos ataques por *inyección de SQL.*

No consta que los datos personales de los usuarios hayan sido nuevamente objeto de tratamiento por terceros y debidamente informados de la incidencia y de la necesidad de actualizar sus contraseñas de acceso a la plataforma abaEnglish.com

III

Por lo tanto, se ha acreditado que la actuación de la entidad ENGLISH, como entidad responsable del tratamiento, ha sido diligente y 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 ***ENGLISH WORLDWIDE, S.L. con NIF B64401482 con domicilio en ARIBAU, NUM 240, PISO 7 - 08006 BARCELONA (BARCELONA)***

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.

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