Expediente Nº: E/07646/2015

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas de oficio por la Agencia Española de Protección de Datos ante la entidad **VTECH** y **ELECTRONICS EUROPE, S.L.**, y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 02/12/2016 la Directora de la Agencia Española de Protección ordenó el inicio de actuaciones previas de investigación con objeto de determinar el posible incumplimiento de la normativa de protección de datos, en relación con las noticias aparecidas, a partir del 27 de noviembre de 2015, en medios de comunicación y publicaciones digitales[1] sobre una supuesta quiebra de seguridad que habría afectado a los usuarios de productos de la marca VTECH, principalmente a usuarios de juguetes.

Las noticias informaban de que la *"compañía VTECH"* habría sido víctima de un ataque informático que habría provocado el acceso ilícito a datos de millones de cuentas de usuarios, adultos y menores, de países de todo el mundo, incluyendo España.

En las declaraciones realizadas por el intruso que accedió a los sistemas de VTECH y por otro experto en seguridad, se informaba de que se había obtenido copia de todos los datos alojados en el sistema y se ponía en cuestión la calidad de las medidas de seguridad aplicadas por la entidad sobre los sistemas afectados.

SEGUNDO: La Subdirección General de Inspección de Datos de esta Agencia procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos contenidos en el informe de actuaciones previas de inspección E/07646/2015, que se transcribe:

"ACTUACIONES PREVIAS

VTECH y las empresas del grupo

1. *Las empresas del grupo VTECH comercializan sus productos en 35 países y su oficina principal se encuentra en Hong Kong.*

   A pesar de que su catálogo de productos incluye otros productos, el grupo es conocido por los juguetes que comercializa, algunos de los cuales son versiones adaptadas para el uso infantil de tabletas y ordenadores.

   Con la finalidad de obtener contenidos o funciones adicionales para los productos adquiridos, algunos de los juguetes permiten la creación de cuentas de usuario en distintos sitios web de la compañía.

1 http://motherboard.vice.com/read/one-of-the-largest-hacks-yet-exposes-data-on-hundreds-of-thousands-of-kids

www.20minutos.es/noticia/2618903/0/ciberataque-vtech/revela-datos-fotografias/seis-millones-menores

www.elmundo.es/tecnologia/2015/12/01/565c85a7ca47416e768b458c.html

2. *Los juguetes de la marca VTECH son comercializados en España por **VTECH ELECTRONICS EUROPE, S.L., en adelante VTECH ESPAÑA.***

VTECH ESPAÑA comercializa los juguetes a comercios mayoristas y minoristas, pero no a particulares.

No se han encontrado evidencias de que VTECH ESPAÑA tenga relación alguna con los sistemas de información afectados por la quiebra.

3. ***VTECH ELECTRONICS EUROPE BV, en adelante VTECH HOLANDA**, es un sociedad del grupo con sede en los Países Bajos que presta servicios a otras sociedades del grupo en Europa.*

VTECH ESPAÑA, con el fin de facilitar el ejercicio de los derechos de acceso, rectificación cancelación y oposición, facilita como domicilio donde ejercerlos los usuarios españoles el suyo pero únicamente redirige dichas solicitudes a VTECH HOLANDA.

Servicios y datos afectados

4. ***Los servicios que contenían datos de usuarios españoles y se vieron afectados son tres: Explor@ Park, Kid Connect y Planet Vtech.***

Los datos de los usuarios, tanto españoles como de otros países, estaban alojados en el momento de la quiebra en servidores de dos proveedores de servicios de computación en la nube ubicados en Estados Unidos: Amazon Web Services e Internap.

5. *Explor@ Park es el nombre comercial del servicio "Learning Lodge" a través del cual los usuarios registrados pueden descargar contenidos extra para algunos de los juguetes comercializados por VTECH ESPAÑA. Fue puesto en marcha en agosto de 2010.*

Los tipos de datos comprometidos para esta plataforma son:

Información del adulto

Nombre y apellidos, dirección de correo electrónico, dirección postal, dirección IP, historial de descargas, contraseña y pregunta y respuesta secreta para recuperarla.

Información del menor: Nombre, sexo, fecha de nacimiento

Registro de las ventas por descarga de contenidos.

Registro del progreso de los menores en los juegos.

En esta plataforma figuran los datos de 115.155 adultos y 138.847 menores españoles.

El responsable de los datos personales incluidos en esta plataforma es VTECH HOLANDA.

6. *"Kid Connect" es una aplicación que permite intercambiar mensajes de texto, imágenes y grabaciones de audio entre los niños que disponen de algunos de los juguetes comercializados por VTECH y los teléfonos móviles de sus padres.*

Fue puesto en marcha en julio de 2013. Únicamente dos de los juguetes comercializados en España permiten el uso de esta aplicación y comenzaron a comercializarse en España a lo largo del año 2015.

Los tipos de datos comprometidos para esta plataforma son:

Información del adulto:

Dirección de correo electrónico, contraseña, las fotos de perfil y nombre de usuarios de padres e hijos.

Los mensajes de texto enviados entre dos usuarios no entregados se conservaban hasta que fueran entregados o por un periodo máximo de 30-40 días.

Los últimos 20 mensajes de texto enviados a un grupo.

Los mensajes de voz y fotografías enviados entre dos usuarios se conservan un año.

En esta plataforma figuran los datos de 2.336 adultos y 2.338 menores españoles.

El responsable de los datos personales incluidos en esta plataforma es VTECH ELECTRONICS LIMITED, con sede en Hong Kong, en adelante VTECH HONG KONG.

7. *PlanetVtech es una plataforma a través de la cual los clientes que adquirieron el producto "Ciberespía PC" a lo largo del año 2009 podían registrarse para acceder a un juego virtual.*

Fue puesto en marcha en 2008.

Los tipos de datos comprometidos para esta plataforma son:

Información del adulto:

Nombre, dirección de correo electrónico, contraseña, pregunta y respuesta secreta para la recuperación de la contraseña, domicilio postal, dirección IP e historial de descargas.

Información del menor:

Nombre, nombre de su avatar, contraseña, género, fecha de nacimiento y puntuación en los juegos.

En esta plataforma figuran los datos de 10.482 adultos y 9.514 menores españoles.

VTECH ESPAÑA manifiesta que debido al reducido número de ventas se solicitó el cierre de la plataforma para España en el año 2010.

VTECH HONG KONG manifiesta que la plataforma se cerró el 29 de noviembre de 2015 y que destruirá los datos tan pronto como la investigación y los litigios iniciados en relación a la quiebra de seguridad hayan finalizado.

La política de privacidad proporcionada para los usuarios registrados identifica como responsable a "VTECH ELECTRONICS EUROPE" sin especificar el tipo de sociedad.

El dominio planetvtech.es está registrado a nombre de VTECH HONG KONG.

Es VTECH HONG KONG quien facilita la información sobre la finalidad de la recogida de datos y los datos más precisos sobre la puesta en marcha y parada del sistema.

8. *El registro en cualquiera de las tres plataformas es voluntario ya que los*

productos comercializados por VTECH ESPAÑA funcionan sin necesidad de ser usuarios registrados. El registro en las plataformas únicamente aporta un valor añadido al producto.

Parte de los contenidos accesibles desde Explor@ Park pueden adquirirse en forma de cartuchos, por lo que no es necesario tener conectividad para acceder a ellos.

9. *VTECH ESPAÑA tiene declarados una serie de ficheros en el Registro General de Protección de Datos, que no tiene relación con los sistemas afectados por la quiebra, sino que contienen datos de diferentes campañas de fidelización realizadas con los clientes que adquieren productos de VTECH.*

Cronología de los hechos

10. *Según la información facilitada por el grupo VTECH y las publicaciones halladas en sus sitios web, los hechos relativos a la quiebra ocurrieron según en el siguiente orden:*

23/11/2015

VTECH HONG KONG recibe un correo electrónico de un periodista que alerta de la quiebra. En ese momento comienza una auditoría interna de sus sistemas.

24/11/2015

La auditoría interna detecta irregularidades ocurridas el 14/11/2015 en el sitio web de Explor@ Park.

27/11/2015

El periodista que informó a VTECH HONG KONG de la quiebra publica en un diario digital el primero de una serie de artículos[2] informando sobre la quiebra.

Se remite un correo electrónico a los usuarios registrados de Explor@ Park en el que se les informa de que personas no autorizadas habían tenido acceso a la base de datos del sistema y se les proporciona un enlace a la página de notas de prensa[3] en lengua inglesa.

28/11/2015

Se suspenden los servicios Explor@ Park y Kid Connect.

5/12/2015

Se añaden comunicados de prensa en lengua española en la página principal de VTECH ESPAÑA y en una página específica dentro del sitio web[4].

7/12/2015

Se remite un nuevo correo a los usuarios registrados de Explor@ Park en el que se amplía la información ofrecida previamente proporcionándose en este caso además un enlace al sitio web de la compañía en España con información sobre la quiebra. En la comunicación se informa de la suspensión temporal del servicio y recomienda el cambio de las clave de usuario porque éstas podrían haber sido descifradas por el intruso y se informa de la suspensión.

2 http://motherboard.vice.com/tag/VTech

3 www.vtech.com/en/media/press-releases

4 www.vtech.es/comunicado-explorapark

9/12/2015

Se remite un correo a los usuarios registrados de Kid Connect en el que se informa de que una persona no autorizada había tenido acceso a la base de datos del sistema y de la suspensión temporal del servicio, incluyendo el enlace al sitio web de la compañía en España con información sobre la quiebra.

En la comunicación se recomienda el cambio de las clave de usuario en otras páginas o servicios donde se haya utilizado la misma contraseña.

15/12/2015

Se detiene a un hombre en el Reino Unido como sospechoso de la quiebra.

23/01/2016

Se reabre la plataforma Explor@ Park, con sus principales funciones activas.

08/08/2016

Se reabre el servicio Kid Connect en España para algunos de los productos.

Forma en la que se produjo la quiebra

Los detalles sobre la forma en que se produjo la quiebra son proporcionados por VTECH HONG KONG a la autoridad de protección de Datos de Hong Kong, quien los comparte con esta Agencia, en respuesta a la solicitud de colaboración realizada.

11. *El intruso utilizó una técnica denominada "Inyección de SQL" para conseguir acceso al entorno del sistema PlanetVtech alojado en el servicio Amazon Web Services.*

    La Inyección de SQL es un tipo de ataque conocido al menos desde 2003. Ha estado en la lista[5] de las 10 vulnerabilidades más utilizadas entre los años 2003 y 2011 y ha afectado a centenares de miles[6] de sitios web de todo el mundo a pesar de que su solución es conocida y sencilla de implementar.

12. *Posteriormente el intruso forzó la realización de una conexión inversa[7], desde un servidor de pruebas de Hong Kong al equipo del intruso.*

    No se dispone de información sobre cómo el atacante pudo conocer la existencia del servidor o forzar la conexión inversa.

13. *Una vez que el intruso tuvo acceso al servidor de pruebas de Hong Kong, localizó claves de acceso a las bases de datos alojadas en Amazon Web Services e Internap.*

14. *Con las claves de acceso de los servidores en Estados Unidos y una conexión abierta al servidor de pruebas de Hong Kong, el intruso creo una conexión a las bases de datos de los sistemas afectados y tuvo acceso a éstos.*

5 http://cwe.mitre.org/top25

6 https://www.netsparker.com/blog/web-security/sql-injection-vulnerability-history
https://www.ccn-cert.cni.es/en/updated-security/news/92-mas-de-500000-sitios-web-fueron-atacados-en-2008-mediante-un-nuevo-metodo-de-inyeccion-sql.html

7 Reverse shell

Sobre las medidas de seguridad previas

15. *Según manifiestan los responsables de VTECH HOLANDA y VTECH HONG KONG, los sistemas afectados tenían implementados numerosas medidas de seguridad entre las que se encontraban cortafuegos, controles que impedían el acceso de personal no autorizado, políticas de minimización en la recogida, tratamiento y retención de datos y la formación del personal responsable en materia de seguridad.*

16. *Según manifiesta VTECH HONG KONG, el servidor que aloja los datos de los usuarios de Explor@ Park disponía de un cortafuegos (firewall) a nivel de red, pero no de un cortafuegos a nivel de aplicación.*

Al conectarse el intruso desde el servidor de pruebas de Hong Kong, el cortafuegos a nivel de red no bloquea la conexión ya que la entiende válida. El uso de un cortafuegos a nivel de aplicación podría haber prevenido la intrusión, pero el servidor no disponía de dicho sistema.

17. *VTECH HONG KONG elabora entre 2002 y 2015 un conjunto de guías y documentos de políticas de seguridad con el fin de incrementar la seguridad en los tratamientos de datos personales.*

Dos de los documentos son guías para el desarrollo de aplicaciones web y para la seguridad de los entornos web de producción.

La guía de seguridad de los entornos web de producción establece que en los servidores deberían de instalarse cortafuegos a nivel de aplicación pero VTECH HONG KONG manifiesta que la guía, implementada el 25 de agosto de 2015, no tiene efecto retroactivo y no se aplicó a los sistemas que sufrieron la quiebra, que estaban desarrollados previamente.

La guía para el desarrollo de aplicaciones web establece que deberán de realizarse pruebas para evitar ataques comunes entre los cuales cita la inyección de SQL. Nuevamente VTECH HONG KONG manifiesta que la guía, implementada el 2 de junio de 2014, no tiene efecto retroactivo y no se aplicó a los sistemas que sufrieron la quiebra, que estaban desarrollados previamente.

18. *En junio de 2015 se contrata un proveedor de servicios externos la realización de una serie de pruebas de penetración[8] en los servicios del grupo VTECH. La realización de pruebas en los servidores que alojan Explor@ Park y Kid Connect estaba planificada pero en el momento de ocurrir la quiebra no había sido ejecutada.*

Sobre las medidas correctivas adoptadas antes de la reapertura de los servicios

19. *VTECH HONG KONG solicitó la realización de un informe a una empresa auditora externa denominada Mandiant[9] al que esta Agencia no ha tenido acceso.*

20. *VTECH HONG KONG manifiesta que ha realizado las siguientes mejoras sobre las medidas de seguridad para evitar que se produzca una nueva quiebra.*

    a. *Se ha implantado una política que asigna a cada miembro del equipo una*

8 Es un tipo de prueba realizada sobre un sistema informático, red o aplicación web cuya finalidad es encontrar vulnerabilidades que un atacante podría explotar.

9 https://www.fireeye.com/services.html

cuenta única de acceso al servidor y una política de claves que contempla la caducidad de estas y exige un determinado nivel de complejidad. Antes no existía un mecanismo específico.

b. *Se ha implementado una política que bloquea las cuentas de usuario si se produce un número determinado de intentos de acceso fallidos. Antes no existía mecanismo alguno.*

c. *Se han implementado controles, que antes no existían, para que las cuentas de administrador local no puedan ser utilizadas en otros servidores y evitar así la propagación de una quiebra a otros servidores.*

d. *Anteriormente no se revisaba el tráfico saliente con origen en servidores internos, ahora todas las conexiones salientes pasarán a través de un único punto que sólo permitirá el tráfico legítimo.*

e. *Se ha mejorado el diseño de la red para separar los entornos de pruebas y los que tienen los datos reales y minimizar y controlar los accesos entre ambos.*

f. *Instalación de un cortafuegos a nivel de aplicación."*

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)

II

El Reglamento de desarrollo de la LOPD, aprobado por RD 1720/2007, de 21 de diciembre, establece lo siguiente respecto a las actuaciones previas:

"Artículo 122. Iniciación.

1. Con anterioridad a la iniciación del procedimiento sancionador, se podrán realizar actuaciones previas con objeto de determinar si concurren circunstancias que justifiquen tal iniciación. En especial, estas actuaciones se orientarán a determinar, con la mayor precisión posible, los hechos que pudieran justificar la incoación del procedimiento, identificar la persona u órgano que pudiera resultar responsable y fijar las circunstancias relevantes que pudieran concurrir en el caso.

2. Las actuaciones previas se llevarán a cabo de oficio por la Agencia Española de Protección de Datos, bien por iniciativa propia o como consecuencia de la existencia de una denuncia o una petición razonada de otro órgano.

3. Cuando las actuaciones se lleven a cabo como consecuencia de la existencia de una denuncia o de una petición razonada de otro órgano, la Agencia Española de Protección de Datos acusará recibo de la denuncia o petición, pudiendo solicitar cuanta documentación se estime oportuna para poder comprobar los hechos susceptibles de motivar la incoación del procedimiento sancionador.

4. Estas actuaciones previas tendrán una duración máxima de doce meses a contar desde la fecha en la que la denuncia o petición razonada a las que se refiere el apartado 2 hubieran tenido entrada en la Agencia Española de Protección de Datos o, en caso de no existir aquéllas, desde que el Director de la Agencia acordase la realización de dichas actuaciones.

El vencimiento del plazo sin que haya sido dictado y notificado acuerdo de inicio de procedimiento sancionador producirá la caducidad de las actuaciones previas" (el subrayado es de la AEPD).

En el presente caso, con objeto de determinar la existencia de infracción a lo dispuesto en el artículo 9 de la LOPD, al tener conocimiento de la existencia de una quiebra de seguridad que habría afectado a compradores de productos de la marca VTECH que se habían registrado (aportando sus datos personales) en diferentes páginas web de la compañía, en fecha 2 de diciembre de 2015 la Directora de la Agencia acordó el inicio de las actuaciones previas **E/07646/2015,** resultando que ha transcurrido el plazo de 12 meses señalado en el párrafo segundo del referido artículo 122.4, lo cual determina la caducidad de las mismas.

No obstante lo anterior, la AN en sentencia de 21/10/2014 señala que: *"El artículo 92 de la LRJPAC, al que se remite su artículo 44.2 al prever la caducidad de los procedimientos en los que la Administración ejercite potestades sancionadoras, entre otros, establece los efectos de la caducidad que, con independencia de provocar el archivo del procedimiento, "no producirá por si sola la prescripción de las acciones del particular o de la Administración pero los procedimientos caducados no interrumpirán el plazo de prescripción". Por consiguiente, declarada la caducidad de unas actuaciones previas de investigación iniciadas por la Agencia Española de Protección de Datos, no se encuentra imposibilitada la Administración actuante para iniciar otras actuaciones previas de investigación sobre los mismos hechos, siempre y cuando no hubiere transcurrido el plazo de prescripción de la infracción administrativa objeto de investigación".*

Por tanto, habiéndose producido la caducidad de las actuaciones previas E/07646/2015, pero no encontrarse prescrita la supuesta infracción objeto de investigación por esta Agencia, procede el inicio de nuevas actuaciones previas de inspección en el marco del expediente **E/06601/2016.**

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 **E/07646/2015**.

INICIAR las actuaciones previas **E/06601/2016.**

NOTIFICAR la presente Resolución a **VTECH ELECTRONICS EUROPE, S.L.**

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.

Cotra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, 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.

Sin embargo, el responsable del fichero de titularidad pública, de acuerdo con el artículo 44.1 de la citada LJCA, sólo podrá interponer 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 LJCA, 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