- **Procedimiento N.º: E/07447/2020**

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: Las actuaciones de inspección se inician por la recepción de un escrito de notificación de brecha de seguridad de datos personales remitido por el responsable del tratamiento de VERSUS ONLINE, S.A. en el que informa a la Agencia Española de Protección de Datos que, el día ******FECHA.1***, el responsable recibió dos correos electrónicos con idéntico contenido en referencia a un hackeo de su plataforma por parte de un atacante externo. En el mensaje se adjuntaba el esquema de base de datos que se usa en la plataforma, así como una muestra con datos de tres jugadores registrados en dicha plataforma.

Una vez comunicado al encargado de tratamiento y proveedor de plataforma, “Eurobox S.A.” (en adelante el encargado del tratamiento), encargado de alojar y gestionar las bases de datos y los servidores, se comprobó que la información referenciada en el email del hacker corresponde con el esquema de base de datos que se usa en la plataforma del encargado de tratamiento, además, se confirmó que las tres muestras enviadas corresponden con jugadores.

El encargado del tratamiento les informa que el autor del ataque ha sido el grupo "******GRUPO.1***".

SEGUNDO: En fecha 22 de septiembre de 2020, la Directora de la Agencia Española de Protección de Datos 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, teniendo conocimiento de los siguientes extremos:

Fecha de notificación de la brecha de seguridad de datos personales: 12/09/2020

ENTIDAD INVESTIGADA

VERSUS ONLINE, SA con CIF A73733016.

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

Respecto de la cronología de los hechos

Los representantes del responsable han manifestado que:

El día ******FECHA.1*** a las 8:53 am horas el responsable recibe los correos electrónicos a través del correo electrónico de atención al cliente de la entidad.

Tras recibir el mismo, se reenvió el mensaje al encargado de tratamiento.

Se comprueba que la información referenciada en el email del hacker se corresponde con el esquema de base de datos que se usa en la plataforma del encargado de tratamiento. Además, se confirmó que las tres muestras enviadas corresponden con jugadores de su plataforma.

El encargado de tratamiento toma las siguientes medidas de precaución el mismo día ******FECHA.1***:

a. El acceso público al sitio web fue cerrado a las 09:46 am (UTC+2).
b. Las bases de datos comprometidas fueron aisladas (protegiendo la integridad de los datos).
c. Todas las cuentas de acceso a la base de datos fueron modificadas.
d. La plataforma se reconfiguró para que coincidiese con las modificaciones de la base de datos.
e. Todos los servicios sensibles fueron aislados.

El encargado de tratamiento indica que sus herramientas de inyección SQL proceden periódicamente a una prueba de seguridad y no se ha tenido información de ninguna infracción, y que la prueba que se procesó para comprobar después también fue satisfactoria.

El encargado de tratamiento continúa poniendo a salvo la base de datos y preparando la plataforma para poder realizar una reapertura de la web garantizando la seguridad. Además, sigue evaluando donde puede estar la vulnerabilidad de seguridad que ha ocasionado este posible incidente y el alcance de este.

Se exigen al encargado de tratamiento reportes de situación continuos, además, se ha comenzado a realizar los protocolos y comunicaciones exigibles para la correcta actuación ante las autoridades pertinentes y usuarios afectados en este tipo de casos.

El día ******FECHA.2*** a las 12:30 pm horas se recibe por parte del hacker un segundo mensaje al correo electrónico de atención al cliente. Este fue enviado de similar manera que el primero, mismo mensaje recibido dos veces desde dos emisores: ******EMAIL.1*** y ******EMAIL.2***.

Tras la recepción de este segundo e-mail, se volvieron a realizar las oportunas comprobaciones según lo arriba expuesto, no constando, ni al responsable ni al encargado ninguna incidencia en relación con los datos personales contenidos en la base de datos del responsable. Adicionalmente, se verifica que la información contenida en el segundo correo electrónico se refiere al mismo acceso no autorizado del día anterior, anunciado a través del primer correo. Entienden que este segundo correo lo remitió el remitente para cerciorarse de que eran efectivamente conocedores de tal acceso.

Indican que de acuerdo con los hechos identificados y como muestra de su plena transparencia, proactividad y colaboración con la Autoridad de Control, el 21 de junio de 2020 se procede a realizar notificación a la Agencia Española de Protección de Datos sobre la incidencia de seguridad. Se realizaron dos notificaciones de carácter inicial (con apenas una hora de diferencia entre una y otra). Dichas notificaciones iniciales, realizadas el mencionado 21 de junio, tienen número de registro 020958/2020 y 020959/2020.

Manifiestan que, en el mismo sentido, y con igual criterio de trasparencia y proactividad, y como muestra de buena fe y lealtad contractual, el mismo domingo día 21 de junio de 2020, el responsable procede a comunicar la brecha de seguridad a los interesados, como medida de precaución y pese a que el riesgo sobre los derechos e intereses de sus usuarios registrados, como consecuencia de la incidencia de seguridad había sido mitigado. De acuerdo con este criterio, la mencionada comunicación se remitió a toda la base de datos del responsable (XXXXXX usuarios), a través de correo electrónico.

A partir del día 21 el responsable mantiene contacto continuado con el encargado de tratamiento a fin de esclarecer las características de la brecha de seguridad, los datos personales y las categorías de interesados afectados, así como las posibles consecuencias. El encargado de tratamiento indica de manera preliminar que potencialmente se pueden haber visto afectados datos básicos, datos de contacto, datos de localización y datos económicos y/o financieros pertenecientes a los usuarios registrados. Se desconocía preliminarmente el número exacto de interesados afectados por la brecha, si bien se considera que por precaución deben considerarse la totalidad de usuarios registrados en la plataforma.

El día 23 el encargado de tratamiento recurrió a la contratación de una compañía especializada en materia de ciberseguridad con la finalidad de investigar el incidente, robustecer las defensas tecnológicas frente a ciberataques y restablecer el servicio.

Las operaciones en la plataforma fueron restablecidas con fecha 30/06/2020.

Tras la investigación, el encargado del tratamiento indica al responsable que fueron víctima de un ciberataque altamente sofisticado ejecutado por el grupo "******GRUPO.1***", así como que las medidas implementadas, en principio han sido suficientes para evitar nuevas incidencias. Sin perjuicio de lo anterior, y para la correcta puesta en funcionamiento del servicio del responsable, se identificaron e implementaron medidas reforzadas.

Una vez realizados los análisis en materia de protección de datos y ciberseguridad como consecuencia del incidente y obtenida toda la información necesaria, se procede a realizar la notificación final de la brecha de seguridad el pasado 12 de septiembre de 2020, con número de registro ******REGISTRO.1***.

Indican que la información detallada se incluye en la notificación final de la brecha de seguridad y que no se ha tenido conocimiento posterior en el responsable de la ocurrencia de ningún evento que haya supuesto consecuencias negativas para los interesados afectados por la brecha.

Respecto de las causas que hicieron posible la brecha:

Los representantes del responsable han manifestado que:

*"El encargado de tratamiento Eurobox fue víctima de un ciberataque altamente sofisticado de un grupo que se presentó como "*****GRUPO.1**".*

Una vez que el atacante ingresó a la red, realizó un movimiento lateral muy lento durante semanas para comprometer hosts adicionales, con el objetivo de evitar ser detectado por los sistemas de seguridad.

Como han empleado técnicas de recolección de credenciales y compromiso de Active Directory, los atacantes pudieron iniciar sesión como usuarios sin necesidad de recurrir a ataques de fuerza bruta o a exploit kits específicos.

Como estos inicios de sesión parecían legítimos, también resultó un comportamiento muy difícil de detectar.

Con respecto a la exfiltración de datos, no tenemos evidencia hasta el momento de que se hayan exfiltrado más datos que los proporcionados como muestra por el atacante. No hay evidencia de un uso anormal del ancho de banda, lo cual también dificultó la detección, puesto que todas las métricas parecían legítimas."

Medidas de minimización del impacto de la brecha y medias implementadas con posterioridad la brecha:

Se ha notificado a todos los posibles afectados. La comunicación aportada cita:

"Nos ponemos en contacto contigo en relación con tu cuenta en VERSUS. En este mail y en cumplimento de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales y del Reglamento General de Protección de Datos, queremos informarte de que el día 19/06/2020 sufrimos un ataque informático a nuestros sistemas que ocasionó una violación de seguridad de datos personales. Es posible que tu seudónimo, tu contraseña y otros datos de tu cuenta puedan haber sido recogidos y revelados por personas no autorizadas; pero no así tus balances en nuestra plataforma de juego, que siguen estando protegidos.

Como medida de precaución hemos incrementado el nivel de seguridad en nuestro WAF (Firewall) y, cuando nuestra web vuelva a estar disponible, te recomendamos que en tu próximo acceso modifiques tu contraseña. Para facilitarte ese proceso, recibirás una notificación al inicio de tu primera sesión y deberás introducir tu nueva clave, que deberá contener específicamente al menos 3 caracteres y no deberá incluir ni tu seudónimo, ni tu nombre, ni tu apellido.

Dicho esto, debes tener en cuenta que este tipo de incidencias pueden provocar que te contacten, vía email o teléfono, terceros ajenos a VERSUS que podrían simular una identidad relacionada con nosotros. En ese caso, te pedimos

que no facilites ningún dato personal. Nosotros siempre te contactaremos a través de nuestros canales oficiales: mail, chat o teléfono. (…)"

Los representantes del responsable han manifestado:

El acceso a los sitios se cerró durante el tiempo del incidente, para aislar y asegurar los componentes de todos los accesos externos no autorizados.

El acceso interno ha sido altamente restringido durante el tiempo de la investigación, sólo al equipo técnico de respuesta a incidentes.

Respecto de los datos afectados.

La tipología de los datos afectados es: datos básicos, de contacto, y datos económicos y/o financieros pertenecientes a los usuarios registrados:

Datos identificativos.
Datos de contacto.
Datos de localización (domicilio postal).
Datos de carácter económico y financiero pertenecientes a los usuarios registrados en la plataforma de VERSUS y, concretamente, el IBAN de la cuenta corriente de los usuarios.

Indican que no existen categorías especiales de datos involucradas.

Se desconoce el número exacto de afectados por la brecha. Los representantes del responsable han indicado que se ha señalado como posibles afectados el total de clientes de la base de datos, que asciende a XXXXXX personas, pero en el correo del hacker solo aparecen tres.

Respecto de las medidas de seguridad implantadas con anterioridad la brecha

Aportan copia de un Análisis de Riesgos y una Evaluación de impacto.

Los representantes del responsable han manifestado:

La plataforma cumple con la norma ISO 27001.

La auditoría bienal del sistema técnico de juego (Seguridad y Funcionalidad) se completó con éxito el pasado 17 de noviembre de 2018 por el laboratorio de tecnología Asensi.

El acceso a los sistemas y aplicaciones está restringido a personal autorizado basado en el directorio de acceso.

El acceso a los servidores de alojamiento está protegido por contraseñas y acceso restringido

El acceso a las bases de datos está protegido por contraseñas y acceso restringido

Las contraseñas de las cuentas de los clientes se almacenan en formato cifrado.

Existen sistemas de respaldo para preservar la integridad de los datos.

Los sistemas de auditoría y registro registran todos los accesos o cambios relevantes.

Todos los datos que no son de producción son anónimos.

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 y disponibilidad, como consecuencia de un ciber ataque sobre la plataforma de juego on line y apuestas deportivas, que derivó en la encriptación de la información por parte de los atacantes y en el acceso a la misma por estos. Se han visto afectados los datos básicos, de contacto y datos económicos y/o financieros de los usuarios registrados.

De las actuaciones de investigación se desprende que, con anterioridad a la brecha de seguridad, la entidad investigada disponía de medidas de seguridad razonables en función de los posibles riesgos estimados. Aporta análisis de riesgos y evaluación de impacto. Además, la plataforma cumplía con la norma ISO 27001 y se encontraba sujeta a auditorías bienales del sistema de juego, habiendo completado con éxito la última realizada.

Asimismo, contaba con protocolos de actuación para afrontar un incidente como el ahora analizado, lo que ha permitido de forma diligente la identificación, análisis y clasificación de la brecha de seguridad de datos personales así como la diligente reacción ante la misma al objeto de minimizar el impacto e implementar nuevas medias razonables y oportunas para evitar que se repita la incidencia en el futuro a través de la puesta en marcha y ejecución efectiva de un plan de actuación por las distintas figuras implicadas como son el responsable del tratamiento y el Delegado de Protección de Datos.

No constan reclamaciones ante esta Agencia por parte de terceros.

En consecuencia, se debe concluir que la entidad investigada disponía de medidas técnicas y organizativas razonables para evitar este tipo de incidencia y que al resultar insuficientes han sido actualizadas de forma diligente. 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

A la vista de las actuaciones practicadas, se ha acreditado que la actuación de la entidad investigada 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 VERSUS ONLINE, S.A. con NIF A73733016.

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