- **Procedimiento N.º: E/07796/2020**

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 División de Innovación Tecnológica de esta Agencia de una brecha de seguridad de datos personales por parte del Responsable del Tratamiento REAL MADRID CLUB DE FUTBOL con número de registro de entrada O00007128e2000002465 relativa a hacking en la web de la fundación, 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: A la vista de la citada notificación de quiebra de seguridad de los datos personales, la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación, teniendo conocimiento de los siguientes extremos:
Fecha de notificación de la brecha de seguridad de datos personales: 17 de septiembre de 2020.

ENTIDADES INVESTIGADAS

Durante las presentes actuaciones se han investigado las siguientes entidades:
REAL MADRID CLUB DE FÚTBOL con NIF G28034718 con domicilio en AVDA. CONCHA ESPINA, Nº 1 - 28036 MADRID (MADRID)

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1.- Con fecha 11 de enero de 2021 se solicitó información al REAL MADRID CLUB DE FÚTBOL (en adelante Real Madrid) con objeto de ampliar la documentación recibida en la notificación de brecha. De la respuesta recibida se desprende lo siguiente:

Respecto de la empresa.

- Real Madrid tiene suscrito un contrato de prestación de servicios con ******EMPRESA.1*** para el mantenimiento de los Sistemas de Información. (documento 3 y 3 bis).
- Real Madrid tiene suscrito un contrato con ******EMPRESA.2*** para el servicio de ciberseguridad prestado para la identificación de la brecha y la ejecución de un protocolo de respuesta a la incidencia (documento 4).

Respecto de la cronología de los hechos.

- El día 9 de septiembre de 2020 a las 00:32 UTC, se identifica un acceso desde una dirección IP desde la que no se suele acceder a dicho equipo. Debido a ello, se tratan de identificar todos los accesos realizados y se detectan dos accesos llevados a cabo mediante la cuenta de un usuario de la organización que se encontraba en periodo vacacional por lo que resultan sospechoso y se comprueba que están relacionados con un acceso posterior al servidor.

Se inicia un análisis de las comunicaciones e intentos de conexión establecidos entre el servidor y otros elementos del entorno.

- El día 11 de septiembre, se activa al equipo de Respuesta a Incidentes, con una copia de seguridad realizada sobre el servidor en la madrugada del 9 al 10 de septiembre que resulto no ser la correcta y el día 16 se realiza un nuevo envío con la copia de seguridad correcta al equipo de respuesta a incidentes.
- El análisis determina que, tras el acceso realizado a las 00:32 UTC del 9 de septiembre de 2020, se detecta además un acceso a una unidad de red disponible en el equipo, localizándose información de carácter aparentemente, sensible relativa a presupuestos, información personal e información privada de la entidad.
- En ese momento se alerta al Real Madrid de una posible fuga de información el 16 de septiembre de 2020 a las 18:20.
- El día 17 de septiembre, se detecta una copia de datos desde la unidad de red hacía el servidor y la descarga de dos herramientas a las 1:40 UTC del día 9 de septiembre.

Se detecta la generación de diferentes archivos comprimidos los cuales incluyen los documentos mencionados. Al menos uno de esos ficheros es generado en el equipo sobre las 1:40 UTC y posteriormente eliminado a las 2:06 UTC. El resto de los archivos comprimidos no es posible determinar la fecha exacta de su creación.

Se detecta el uso de diferentes servicios y aplicaciones relacionados con el envío e intercambio de documentos durante el rango temporal en el que el usuario sospechoso se mantiene en el equipo.

Como consecuencia de dichos hallazgos, el 17 de septiembre de 2020 a las 17:20 la empresa que está realizando los análisis informa al Real Madrid que se ha producido una fuga de información.

- El día 18 de septiembre, se correlaciona la información obtenida en el equipo, con los registros de red disponibles, siendo por lo tanto posible detectar un envío de datos hacía fuentes externas (entre las 1:04 y las 3:50 UTC).

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

- Entre otras medidas a corto plazo

  - Reiniciar las credenciales de los usuarios comprometidos
  - Establecer medidas para no permitir el uso de herramientas que permitan la autenticación en sistemas remotos sin requerir la introducción de credenciales.
  - Bloquear el uso de determinadas plataformas.

- Entre las medidas a posteriori

  - Doble factor de verificación
  - Restauración del servidor
  - Bloqueo de las direcciones IP desde las que se produjo el acceso.

Respecto de las causas que hicieron posible la brecha

- La brecha se produce como consecuencia de la utilización de las credenciales de un usuario por un tercero ajeno a la organización. Actualmente se ignora cómo el supuesto atacante obtuvo las credenciales.
- Real Madrid manifiesta que las averiguaciones de los proveedores de ciberseguridad y sistemas han sido infructuosas y que actualmente existe una investigación policial en curso, abierta a raíz de la denuncia interpuesta ante la Policía. (documento 0).

Respecto de los datos afectados.

- Los tratamientos de datos afectados por la incidencia son relativos a:

  FUTBOL - Gestión Administrativa, Relación contractual y seguimiento de jugadores.
  RRHH - Gestión de relación laboral.

- Los datos personales que se han visto afectados son los que se encuentran en los siguientes tipos de documentos: Contratos, licencias federativas, documentos, Excel de presupuestos y Otros documentos. Básicamente datos identificativos y económicos.

- Las categorías de interesados que se han visto afectadas por esta incidencia ha sido personal de la entidad incluido jugadores y técnicos. En total unas 1.000 personas.

- El Real Madrid manifiesta que no considera que la información afectada en la incidencia, puedan producir suplantaciones de identidad, perjuicios económicos ni denegación de servicios. Y, tampoco se estima que con tal información se puedan ocasionar daños al honor o reputación de las personas afectadas en caso de hacerse pública, ni afectar a su dignidad ni producirles ningún tipo de discriminación por lo que no van a comunicar la incidencia a los afectados.

Asimismo manifiestan que evaluada la incidencia y concluido que existe un riesgo para los derechos y libertades de los interesados en función de lo indicado en el Anexo 1 y conforme al criterio reflejado por el Grupo de Trabajo del art. 29 (GT29), ahora Comité Europeo de Protección de Datos (CEPD) en sus Directrices sobre notificaciones de incidentes de datos personales adoptadas el 3 de octubre de 2017 y revisadas y finalmente adoptadas el 6 de febrero de 2018 se procede a la notificación a la Agencia, no así a la comunicación a los interesados siguiendo el mismo criterio.

- Real Madrid manifiesta que se ha estado supervisando en Internet, incluida la Deep Web, actividad que pudiera reflejar el uso ilegítimo por parte de terceros de la información afectada por la brecha, sin que hasta la fecha se haya detectado nada al respecto. Asimismo, manifiestan que no les consta ningún tipo de utilización por parte de terceros de la información afectada por la brecha.

Se realizan continuas búsquedas automáticas y manuales de información del Real Madrid a través de diferentes fuentes, como son las redes sociales, foros de la web y de la Deep web, … para detectar posibles activos expuestos y en lo que se refiere a

este incidente se ha utilizado búsquedas más específicas y no se ha encontrado evidencia alguna de que se haya utilizado la información comprometida por parte de terceros.

Respecto de las medidas de seguridad implantadas

Con anterioridad a la brecha:

- Medidas generales

o Políticas de protección de datos o seguridad de información.
o Medidas de control de acceso lógico para usuarios autorizados.
o Medidas de control para prevenir ataques, intrusiones e infecciones.
o Monitorización, detección, análisis y reporte de eventos de incidentes de seguridad.
o Formación y concienciación al personal en materia de protección de datos.
o Marco normativo de la seguridad de la información.
o Modelo de gobierno de la seguridad.

- Especificas

o Análisis de accesibilidad a redes.
o Actualización de aplicaciones y sistemas.
o Revisión del código fuente.
o Gestión de crisis cyber.
o Monitorización eventos y logs de auditoria.
o Servicio de envío seguros de ficheros.
o Control general de la seguridad y seguimiento.

- Documentos:

o Registro de Actividades de Tratamiento relativo a los tratamientos afectados por la brecha notificada (documento 7)
o Análisis de Riesgos de los dos tratamientos afectados. Se adjuntan dos proyecciones realizadas de Análisis de Riesgos de ambos tratamientos que se han llevado a cabo a fin de comprobar que efectivamente las medidas adicionales que se están implementando a raíz de la brecha acaecida, contribuyen a minorar aún más el riesgo residual (documentos 8, 8 bis, 9 y 9 bis)
o Análisis sobre la necesidad de realizar Evaluaciones de Impacto (documentos 10 y 11).
o Entorno de trabajo corporativo en el que se detallan medidas de seguridad aplicadas sobre los tratamientos afectados (documento 13).
o Política de seguridad de la Información (documento 14).
o Guía de Identificación y comunicación de incidentes de seguridad (documento 15).
o Informe de revisión sobre el cumplimiento del Título VIII del Reglamento de desarrollo de la LOPD (RD1720/2007) (documento 16) que corresponde con el último informe de auditoría de protección de datos, de 30 de junio de 2016.
o Informe de ciberseguridad del año 2020 (documento 17) sistema de evaluación continua.

o Nuevas medidas de ciberseguridad (documento 12).

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

No existe recurrencia y no hay eventos análogos acaecidos conocidos.

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, como consecuencia de la fuga de información detectada.

De la documentación aportada por la empresa en el curso de estas actuaciones de investigación, entre ella, RAT y AR de los dos tratamientos afectados, análisis sobre la necesidad de realizar Evaluaciones de Impacto, el documento sobre el entorno de trabajo corporativo en el cual se detallan medidas de seguridad aplicadas sobre los tratamientos afectados y la guía de Identificación y comunicación de incidentes de seguridad, se desprende que con anterioridad a la brecha, la entidad investigada disponía de medidas de seguridad razonables en función de los posibles riesgos estimados.

En cuanto al impacto, los datos que se han visto vulnerados son los contenidos en los siguientes tipos de documentos: Contratos, licencias federativas, documentos, Excel de presupuestos y Otros documentos, que contienen básicamente datos identificativos y económicos, encontrándose el volumen de datos afectados en el rango de 1000.

Se realiza una supervisión continua de Internet incluyendo la Dark Web, así como búsquedas de información sobre el Real Madrid, tanto de manera automática como manual, sin que haya constancia del uso ilegítimo por parte de terceros de la

información ni tampoco constan reclamaciones ante esta Agencia relativas a esta brecha.

Para evitar que estos hechos se repitan, se adopta lo prescrito en el documento Nuevas Medidas de Ciberseguridad, entre otras, el doble factor de autenticación y el cambio en las normas de uso de los portátiles.

En consecuencia de lo anterior, consta que se disponía de las 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 notificar a la AEPD e implementar medias para eliminarla.

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

En el presente caso, la actuación de la investigada como entidad responsable del tratamiento, ha sido diligente y proporcional 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 REAL MADRID CLUB DE FÚTBOL con NIF G28034718 con domicilio en AVDA. CONCHA ESPINA, Nº 1 - 28036 MADRID (MADRID)
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