- **Procedimiento Nº: E/01234/2021**

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 DIGITAL PRESCRIPTION SERVICES, S.A. con número de registro de entrada O00007128e2100003599 relativa a ciberataque sistema de receta médica, 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: 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 la brecha de seguridad de datos personales: 29 de enero de 2021.

Resumen de la notificación:

> Se ha producido una intrusión no autorizada en sus sistemas de información con datos personales, de origen externo y con la intencionalidad de suplantar a alguno de los usuarios. El intruso ha utilizado una vulnerabilidad del sistema que, para una vez ganado el acceso a un usuario, le permite consultar los datos de cualquier profesional. Han accedido a datos básicos de 9.435 usuarios: DNI, nombre y apellidos, dirección de correo electrónico, número de teléfono móvil y número de colegiado.

ENTIDADES INVESTIGADAS

Durante las presentes actuaciones se han investigado las siguientes entidades:

DIGITAL PRESCRIPTION SERVICES, S.A con NIF A88496955

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1.- Respecto de la empresa.

DIGITAL PRESCRIPTION SERVICES S.A, en adelante DPS, tiene como actividad “Otros servicios relacionados con las tecnologías de la información y la informática”.

DPS es titular de una plataforma denominada REMPe que es un sistema de información creado en virtud del Real Decreto 1718/2010 para la receta médica electrónica en el ámbito privado.

2.- Con fecha 18 de febrero de 2021 se solicitó información a DPS. De la respuesta recibida se desprende lo siguiente:

Respecto de la cronología de los hechos.

El día 27 de enero, a las 22:00 horas, las herramientas de monitorización (******HERRAMIENTA.1, ***HERRAMIENTA.2, ***HERRAMIENTA.3***) manifiestan diversas alertas recibidas en el buzón de email correspondiente al equipo de soporte que tras su evaluación es escalado al responsable de seguridad.

Este evalúa la información de las alertas y las peticiones que las originan, observando que se trata de una petición para la consulta de los datos de un profesional cuyo patrón no obedece al comportamiento de una petición estándar.

Al determinar que se trata de una acción irregular y que puede constituir un ataque se limita el acceso al origen de este a las 00:05 horas del día 28.

El responsable de seguridad junto al equipo técnico a las 00:00 horas proceden a un análisis inicial de la situación y se observa que, con las credenciales de un usuario del sistema ganadas por el atacante por algún medio externo al sistema, este ha tenido acceso a información relativa a los datos profesionales de un usuario haciendo uso de la API interna.

Se detecta una vulnerabilidad no conocida en el código del sistema que permite realizar esta acción y se procede a su resolución. El equipo de desarrollo procede a la preparación del hotfix que se despliega a las 2:00 horas, momento en el que la brecha queda resuelta.

Respecto a las acciones tomadas con objeto de minimizar los efectos adversos.

Con carácter inmediato a la detección de las circunstancias expuestas, el día 27 de enero a las 23:00 el responsable de seguridad establece el correspondiente Comité de Seguridad tras la evaluación inicial.

Una vez realizada la evaluación de la situación se tomaron las medidas oportunas, iniciándose esa misma madrugada, la implementación de las medidas de mitigación recogidas en el plan de acción que también se comienza a elaborar, y que ha consistido en:

Madrugada del 27 al 28 de enero:

a) Análisis y evaluación del impacto inicial. 27/1- Finalizado a las 23:59

b) Limitación de acceso integral al sistema. 28/1 a las 00:05

c) Securización correcta del método de obtención de datos de profesionales de la API correspondiente. Desplegado en producción el 28/1 a las 2:00 horas

d) Implementación de monitorización exhaustiva de la actividad sobre el sistema. Iniciada el 28/1 a las 2:00 horas.

e) Búsqueda, detección e identificación de posibles usuarios cuyo acceso haya podido ser ganado por el atacante. Finalizada la tarea el día 28/1 a las 4:00 horas.

f) Bloqueo de los posibles usuarios a los que el atacante ha ganado el acceso y que el intruso ha utilizado para realizar el ataque y acceder al sistema. Finalizada la tarea el día 28/1 a las 4:00 horas

<u>Respecto a las medidas adoptadas para su resolución final</u>

28 y 29 de enero:

a) Actualizar la monitorización y alertas con alertas específicas para los parámetros particulares y herramientas que está utilizando el atacante de forma que se identifique al mismo en caso de reiterar. Actualizada el 28/1 a las 12:00 horas

b) Fortalecer la gestión de contraseñas disminuyendo el número de intentos para el bloqueo de la cuenta con objeto de reducir las posibilidades ante ataques de fuerza bruta para obtener contraseñas. Ejecutada el 28/1 a las 12:00

c) Desactivar profesionales que no han hecho uso de la aplicación en un tiempo inferior a tres meses, aunque lo habitual es un año. Se han desactivado a 6243 usuarios que han quedado en estado bloqueados. Ejecutada el 28/1 a las 22:00

d) Contactar con los proveedores de servicios tienen asociadas las direcciones IP utilizadas por el atacante. Ejecutada el 28/1 a las 20:00

e) Evaluación y determinación del mecanismo usado por el intruso para ganar el acceso a los usuarios. Finalizada el 29/1 a las 15:00 horas.

Afirman que las medidas adoptadas por el Comité de Seguridad tras la detección de la brecha y detalladas en el apartado 1.6 han sido oportunas y eficaces, toda vez que no se ha materializado ningún ulterior ataque desde la fecha del incidente hasta el día de hoy.

Respecto de las causas que hicieron posible la brecha

El atacante ha conseguido credenciales de un usuario (usuario, contraseña y PIN de verificación) de manera externa a la plataforma. Con esas credenciales, el intruso ha utilizado una vulnerabilidad no conocida del sistema que, para una vez ganado el acceso a un usuario, le permite consultar un conjunto de datos profesionales de cualquier profesional.

Respecto de los datos afectados.

Tipo de datos y número de afectados:

Si bien se ha detectado que se realizaron 332.184 peticiones aproximadamente de estas llamadas, 9.435 han conseguido acceder a los datos de profesionales. Las llamadas a este servicio se han basado en hacer peticiones secuenciales al identificador de profesionales. Al no ser un secuencial puro, ya que contiene un factor de entropía, muchas de ellas han sido fallidas, pero otras han tenido éxito y por lo tanto han podido obtener datos asociados al profesional.

La brecha de seguridad detectada únicamente ha afectado al conjunto de las siguientes tipologías de datos de algunos de los profesionales que utilizan la plataforma: N.º DNI, nombre y apellidos, dirección de correo electrónico, número de teléfono y número de colegiado.

Aunque en la comunicación inicial se informó que se había accedido al código de usuario para la identificación del sistema, en realidad se accedió al atributo “userId” que sólo es un identificador interno de la plataforma y no el del usuario para el acceso a la misma, por lo que se confirma que no se tuvo acceso a ningún tipo de credencial.

Comunicación a los afectados:

Manifiestan que la severidad de las consecuencias para las personas afectadas es muy baja, razón por la cual los interesados no serán finalmente informados de la brecha, aunque han iniciado una campaña con ellos para reforzar la seguridad de la cuenta de usuario, sugerencias para la protección y acceso al sistema, e información sobre seguridad para evitar el phishing.

Utilización por terceros, publicación, indexación:

No se tiene conocimiento de la utilización por terceros de los datos personales obtenidos a través de la brecha.

Posibles consecuencias:

Los datos, aunque de carácter personal, tienen un ámbito eminentemente profesional. De hecho, en la mayoría de los casos los profesionales los ponen disponibles en sus propias webs como contacto, en plataformas o marketplaces donde ofrecen sus servicios profesionales, etc. Esto hace que el potencial impacto para los afectados sea bajo o muy bajo. Además, casi todos los datos accedidos forman parte de los Registro de colegiados a los que pertenecen los usuarios afectados, y en virtud del art. 10.2.a) de Ley 2/1974, de 13 de febrero, sobre Colegios Profesionales, son accesibles a cualquier persona que acuda por Internet a la ventanilla única del Colegio Profesional, Consejos Autonómicos Generales o Superiores.

<u>Respecto de las medidas de seguridad implantadas</u>

Con anterioridad a la brecha:

Indican que la política de seguridad y guía de seguridad para la solución, desde el punto de vista organizativo y procedimental, recogen el conjunto de procedimientos, las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente. Aportan guía de seguridad.

La organización tiene establecidas unas políticas de continuidad del negocio que le permiten la operación 24x7x365, así como la gestión y recuperación de los sistemas en caso de incidentes y compromiso de sus operaciones, asegurando los servicios críticos de sus procesos. Aportan el documento “Análisis impacto y continuidad del negocio”.

La plataforma cuenta con la correspondiente Evaluación del Impacto en la Protección de Datos donde se analiza la necesidad, se evalúa el impacto y presenta el análisis de riesgos correspondiente tanto en cumplimiento del RGPD como en los diferentes ámbitos de la seguridad. En ella se concluye que el nivel de cumplimiento de protección de datos es completo. Aportan copia del a evaluación de impacto, análisis de riesgos y arquitectura de implementación y salvaguardias.

Las últimas pruebas de ciberseguridad y hacking ético a las que se ha sometido la aplicación con carácter externo han sido realizadas en noviembre de 2020 con un resultado favorable.

En diciembre de 2020, la plataforma se ha recertificado como solución de receta electrónica homologada por la OMC bajo un proceso de auditoría con un conjunto de puntos de control específicos y que son relativos a la gestión de la seguridad de la información de los sistemas de información en los siguientes ámbitos: Seguridad y confidencialidad, Interoperabilidad y Protección de datos de carácter personal. Aportan el documento “Auditoría de certificación de sistemas de receta médica privada electrónica. REMPe”

Aportan el documento “PROCEDIMIENTO DE GESTIÓN Y NOTIFICACIÓN DE BRECHAS DE SEGURIDAD. PROTECCIÓN DE DATOS”

Motivo por el cual las medidas de seguridad implantadas no han impedido el incidente:

El intruso se ha valido de vulnerabilidad no conocida de la aplicación que permitía a un tipo de usuario consultar, a través del API interno, no sólo sus datos profesionales sino también los de otros.

Con posterioridad a la brecha:

Para el caso de la incidencia junto con la vulnerabilidad detectada se ha procedido a una revisión exhaustiva de los aspectos referidos a la securización de los componentes software del aplicativo para identificar patrones similares al que han dado lugar a la vulnerabilidad (permitir a los usuarios mayores privilegios de los permitidos necesarios a través del acceso mediante APIs). Después de la revisión no se ha detectado ninguna otra vulnerabilidad. Adicionalmente, se va a realizar un nuevo pentesting.

Se ha realizado una campaña de comunicación entre los usuarios con objeto de potenciar las medidas de seguridad que estos deben usar tanto en sus equipos locales como a la hora de proteger sus credenciales, tanto en el sistema en cuestión como en otros que puedan servir para obtener información de los usuarios para poder luego acceder a este.

se ha planificado la inclusión de medidas adicionales como la inclusión de autenticación incremental en varios pasos en algunos puntos del sistema con objeto de restringir el acceso a funciones del sistema consideradas de carácter relevante en caso de accesos no autorizados.

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

Se trata de la primera y única ocurrencia de un ataque de esta tipología.

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.

De la documentación aportada por la investigada en el curso de estas actuaciones de investigación, entre ella, copia de la evaluación de impacto, en la que se concluye que el nivel de cumplimiento de protección de datos es completo, el análisis de riesgos , la guía de seguridad que recoge el conjunto de procedimientos y las medidas técnicas y organizativas, acorde a la normativa de seguridad vigente. Asimismo aporta el documento, Auditoría de certificación de sistemas de receta médica privada electrónica. REMPe, que acredita, que la plataforma se ha recertificado como solución

de receta electrónica homologada por la OMC, lo que implica, que se ha realizado una auditoria en los ámbitos de seguridad y confidencialidad, interoperabilidad y protección de datos de carácter personal. De todo ello se desprende que, con anterioridad a producirse la brecha, la entidad investigada disponía de medidas de seguridad razonables en función de los riesgos estimados

Tras conocerse el incidente a través de las alertas enviadas por las herramientas de monitorización, se procede al análisis de la situación y se determina que puede tratarse de un ataque, procediéndose a la limitación de acceso integral al sistema, posteriormente y tras haberse detectado una vulnerabilidad, se prepara el hotfix por el equipo de desarrollo, quedando la incidencia resuelta. A partir de este momento, se procede a una monitorización exhaustiva de la actividad y a la detección de posibles usuarios cuyo acceso haya podido ser ganado por el atacante, con el fin de bloquearlos.

La brecha fue posible tras conseguir el atacante las credenciales de un usuario de manera externa a la plataforma, pudiendo así explotar una vulnerabilidad no conocida del sistema, lo que le permitió consultar los datos de cualquier profesional.

Los datos que se han visto afectados son el DNI, nombre y apellidos, dirección de correo electrónico, número de teléfono y número de colegiado, confirmándose que en ningún momento se tuvo acceso por parte del atacante a campos que permitan el acceso al sistema. En lo que hace referencia al número de afectados es de 9435, no teniéndose constancia del uso por terceros de los datos afectados por la brecha. La investigada considera que la severidad de las consecuencias para los afectados es muy baja, motivo por el cual decide no comunicar a los afectados.

Para evitar que estos hechos se repitan, se ha procedido a una revisión exhaustiva de los aspectos referidos a la securización de los componentes software del aplicativo, para identificar patrones similares al que ha dado lugar a la vulnerabilidad (permitir a los usuarios mayores privilegios de los permitidos necesarios a través del acceso mediante APIs), sin que se haya detectado ninguna otra vulnerabilidad. Además tiene previsto realizar un nuevo pentesting. en el plazo de dos meses. Dado que el origen de la brecha estuvo en la obtención de las credenciales de un usuario, se ha realizado una campaña de comunicación con objeto de potenciar las medidas de seguridad que éstos deben aplicar. Asimismo se ha planificado la introducción de medidas adicionales como la inclusión de autenticación incremental en varios pasos, en algunos puntos del sistema, con objeto de restringir el acceso a funciones del sistema consideradas de carácter relevante, en caso de accesos no autorizados.

En consecuencia, consta que disponía de medidas técnicas y organizativas razonables para evitar este tipo de incidencia, reflejada en el hecho de la rápida detección del incidente a través de las herramientas de monitorización, produciéndose una diligente reacción al objeto de eliminar la brecha y notificar a la AEPD.

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 DIGITAL PRESCRIPTION SERVICES, S.A con NIF A88496955.

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