- **Procedimiento Nº: E/10375/2019**

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: Con fecha 21 de octubre de 2019, la entidad WALLAPOP S.L. (en adelante, WALLAPOP) notificó a esta Agencia (AEPD) una violación de la seguridad de los datos personales (en adelante, quiebra de seguridad) tras haber tenido conocimiento, con fecha 18 de octubre de 2019, de un ciberataque por el cual se habían obtenido las credenciales de un empleado de la entidad y se había procedido a realizar una copia de los repositorios de los códigos fuentes de las aplicaciones que contenían, además, contraseñas de proveedores encargados del tratamiento con acceso a las bases de datos de usuarios de Wallapop. Se informó también que podrían estar afectados más de un millón de usuarios.

Con fecha de 28 de octubre de 2019, la Directora de la AEPD acordó iniciar actuaciones de investigación para determinar una posible vulneración de la normativa de protección de datos.

Con fecha 1 de noviembre de 2019, WALLAPOP presentó una notificación adicional ante esta Agencia en la que se ponía de manifiesto que en el estudio de la brecha notificada habían verificado que el día 19 de octubre, utilizando unas credenciales de Amazon Web Services, se había creado un usuario y una nueva base de datos que había estado activa durante 7 horas, por lo que en esa misma fecha se tomó la decisión de cerrar todas las sesiones de la Web y obligar a todos los usuarios al cambio de contraseña. Se aportaba copia de un mail remitido desde la dirección info@info.wallapop.com en cuyo asunto figuraba *Información de Seguridad* y en el que se informaba de que, por seguridad, se tenía que reiniciar las contraseñas debido a que se había detectado un acceso indebido, se había cerrado la sesión y se había deshabilitado la contraseña por lo que tendría que cambiarla. WALLAPOP manifestó que este correo había sido remitido a los posibles afectados.

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 notificación, teniendo conocimiento de lo siguiente:

ENTIDADES INVESTIGADAS

WALLAPOP S.L. con NIF B66049057 con domicilio en c/ Meridiana 89, planta 6ª - 08026 BARCELONA (BARCELONA)

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1.- Con fecha 4 de noviembre de 2019 se solicitó información a WALLAPOP y de la respuesta recibida se desprende lo siguiente:

Respecto de la empresa.

- WALLAPOP es una plataforma de compraventa de productos de segunda mano.
- WALLAPOP tiene como proveedores a GitHub Inc. y Amazon AWS en calidad de encargados del tratamiento. A este respecto, se ha aportado los términos del servicio de ambas entidades.

Amazon AWS es una plataforma de servicios de nube que proporciona una variedad de servicios de infraestructura, entre otros, almacenamiento, bases de datos, …

GitHub es una plataforma para alojar proyectos (código fuentes de aplicaciones y herramientas) y mantiene un control de versiones.

Respecto de la cronología de los hechos

- Con fecha 18 de octubre de 2019, se recibe en la entidad un correo enviado por GitHub Inc. en el que se informa que un atacante ha obtenido las credenciales de un miembro del equipo de Wallapop que le ha permitido el acceso a un sistema en el que se almacenaba el código fuente del software de la compañía y las credenciales de acceso a los Sistemas de Información (Wallapop ha aportado correo electrónico remitido desde la dirección no-reply@github.com).
- Ese mismo día se analizaron las claves de acceso comprometidas y se organizó un equipo técnico para renovar todas las claves. Este proceso se llevó a cabo desde el viernes 18 de octubre al lunes 21 de octubre.
- El lunes 21 de octubre se inicia un procedimiento de solicitud de información a terceros propietarios de las claves comprometidas y se notifica la brecha de seguridad a la Agencia.
- El 24 de octubre de 2019 se contrata a NCC Group (FORTLAND A/S), entidad consultora de ciberseguridad para la realización de un análisis forense.
- El miércoles 30 de octubre de 2019, la consultora NCC Group confirma el ataque por el cual el atacante hace uso de una credencial de acceso a la infraestructura de Wallapop en la nube de Amazon Web Services, Inc. (AWS) creando un nuevo usuario y duplicando la base de datos a partir de una copia de seguridad que incluía datos de clientes, usuarios, *hash* de credenciales.
- El jueves 31 de octubre de 2019 se decide cerrar las sesiones obligando a crear nuevas contraseñas.
- El 1 de noviembre se remite una notificación adicional de brecha a la Agencia.

Wallapop ha aportado copia del informe emitido por NCC Group en el que se ponen de manifiesto los hechos mencionados y se indica que ***(…)***.

Respecto de las causas que hicieron posible la brecha

- WALLAPOP manifiesta que, a pesar de la investigación llevada a cabo, no se ha podido determinar cómo se produjo la obtención de credenciales por parte del atacante.

- WALLAPOP manifiesta que, pese a la política de passwords de GitHub Inc., el atacante tuvo la capacidad de suplantar la identidad de uno los ingenieros de la empresa y, al acceder al código fuente y las credenciales almacenadas en él, el atacante pudo sortear los firewalls y acceder a la infraestructura de la entidad en la nube.

A este respecto se ha incluido información sobre gestión de passwords de GitHub a través de la diligencia de fecha 8/07/2020, en la que se pudo comprobar que en la página web https://docs.github.com/es/enterprise/2.18/user/github/authenticating-to-github/updating-your-github-access-credentials la empresa GitHub indica al "Actualizar tus credenciales de acceso de GitHub" que: "*Las credenciales GitHub no solo incluyen tu contraseña, también los tokens de acceso, las claves SSH y los tokens API de la aplicación que utilizas para comunicarte con GitHub. Si lo necesitas, puedes restablecer todas estas credenciales de acceso tú mismo*".

Y que en el sitio web https://git-scm.com/book/es/v2/Herramientas-de-Git-Almacenamiento-de-credenciales, en el apartado 7.14, relativo al almacenamiento de credenciales, la empresa GitHub indica que:

"*Si usa protocolo SSH para conectar a los remotos, es posible tener una llave sin clave, lo que permite tranferir la data sin tener que escribir el nombre de usuario y la clave cada vez. Sin embargo, esto no es posible por el protocolo HTTP - cada conexión necesita usuario y contraseña. Incluso se vuelve más complicado para sistemas con autenticación de dos pasos, donde el token que se usa para la clave es generado al azar y no puede ser reutilizado.*

Afortunadamente, Git tiene un sistema de credenciales que lo ayuda con esto. Git tiene las siguientes funciones disponibles:

- *El "default" es no guardar cache para nada. Cada conexión solicitará el usuario y contraseña.*
- *El modo "cache" mantiene las credenciales en memoria por un cierto período de tiempo. Ninguna de las claves es guardada en disco, y son borradas del cache tras 15 minutos.*
- *El modo "store" guarda las credenciales en un archivo de texto plano en disco, y nunca expiran. Esto quiere decir que hasta que se cambie la contraseña en el host Git, no se necesitará escribir las credenciales de nuevo. La desventaja de este método es que sus claves son guardadas en texto plano en un archivo dentro de su máquina.*
- *Si está usando Mac, Git viene con el modo "osxkeychain", el cual guarda en cache las credenciales en el llavero que está conectado a su cuenta de sistema. Este método guarda las claves en disco, y nunca expiran, pero están encriptadas con el mismo sistema que guarda los certificados HTTPS y los auto-completar de Safari.*
- *Si está en Windows, puede instalar un ayudante llamado "winstore." Éste es similar al ayudante de "osxkeychain" descrito arriba, pero usa Windows Credential Store para controlar la información sensible. Se puede encontrar en https://gitcredentialstore.codeplex.com.*

Se puede elegir cualquiera de estos métodos mediante el valor de configuración de Git."

Medidas de minimización del impacto de la brecha

- Identificación de claves a las que tuvo acceso el atacante. Estas credenciales no son de los usuarios sino las que utiliza el software para acceder a los sistemas de información.
- Renovación de estas credenciales una vez identificadas y que pudieran ser accesibles desde fuera de la red.
- Renovación de las credenciales de servicios utilizados dentro de la red.
- Recuperación de información de los logs de acceso para conocer el impacto del incidente.
- Borrar todas las sesiones y resetear las contraseñas de usuarios, lo que obliga al cambio de contraseña para poder acceder de nuevo.
- Campaña de comunicación a los usuarios.
- Se aumenta el número de personas de atención al usuario con objeto de contestar las consultas que se puedan realizar.
- Se interpone denuncia ante la unidad UCO de la Guardia Civil el día 13 de noviembre de 2019.

Respecto de los datos afectados

- Los datos afectados corresponden a nombre y apellidos. Dirección de mail, número de teléfono, datos postales, dirección IP, identificador de dispositivo y datos de compra aunque no hay constancia de que se haya accedido a datos financieros.
- WALLAPOP manifiesta que en la base de datos a la que tuvo acceso el atacante se almacenaba los hash de contraseñas de unos 21 millones de usuarios. No obstante, no hay constancia de la utilización de las credenciales.
- WALLAPOP manifiesta que no tienen constancia de la utilización de los datos personales comprometidos por terceros, ni tampoco de la indexación por los buscadores.
- WALLAPOP ha comunicado a los afectados de diversas formas:
    - El viernes 1 de noviembre de2019, al entrar en la *app* se informa de que se debe restaurar las contraseñas. También por medio de este canal se emite una comunicación indicando que se ha procedido a reiniciar la cuenta por un acceso indebido y que es necesario cambiar la contraseña.
    - A través de correo electrónico a toda la base de datos de usuarios registrados se envía un correo informando del acceso indebido y de la necesidad de cambiar las contraseñas.

- A través de las redes sociales se contesta a las peticiones de información sobre el cierre de las cuentas.

WALLAPOP ha aportado ejemplo de todas estas actuaciones.

Respecto de las acciones tomadas para la resolución final de la brecha

- Se activa un sistema de doble factor de autenticación.
- Renovación de todas las credenciales a las que el atacante tuvo acceso.
- Análisis forense completo.

Respecto de las medidas de seguridad implantadas con anterioridad la brecha

WALLAPOP ha aportado informe sobre las medidas de seguridad alrededor de los sistemas de información afectados por el incidente, entre las que cabe destacar:

- Utilización de firewalls en la infraestructura de AWS.
- Acceso a la red del exterior que se realiza a través de VPN con credenciales personales.
- Auditoría de seguridad de los sistemas en la nube cada dos años.
- Sistemas automáticos de copia de seguridad de las bases de datos.
- Accesos a la infraestructura en la nube se almacenan en logs.
- Contraseñas de los usuarios no se almacenan en claro, solo un *hash* de la misma para la validación

Wallapop ha aportado la siguiente documentación:

- Registro de actividad de los tratamientos, entre los que se encuentran los relativos a tratamientos de usuarios (registro de usuarios, acceso de los usuario, reporting de productos y usuarios…)
- Análisis de Riesgos de los tratamientos, entre ellos, de tratamientos de usuarios descritos den el en el registro de actividades. Todos ellos con un nivel de impacto resultante *Bajo o Medio.*

Respecto de las medias implementadas con posterioridad la brecha

- ***(…)***
- ***(…)***
- ***(…)***
- ***(…)***
- ***(…)***
- ***(…)***
- ***(…)***
- ***(…)***

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 una brecha de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como una posible brecha de confidencialidad, como consecuencia del acceso indebido por terceros ajenos a la base de datos de WALLAPOP.

De las actuaciones de investigación se desprende que WALLAPOP disponía de razonables medidas técnicas y organizativas preventivas a fin de evitar este tipo de incidencias y acordes con el nivel de riesgo.

Asimismo, WALLAPOP ha afrontado de forma diligente la identificación y corrección de la brecha, análisis y clasificación del supuesto incidente de seguridad de datos personales así como la diligente reacción ante la misma al objeto de notificar, minimizar el impacto, comunicar a los afectados e implementar nuevas medidas razonables y proporcionales para evitar que se repita la supuesta incidencia en el futuro.

En consecuencia, WALLAPOP disponía de forma previa de medidas técnicas y organizativas razonables y proporcionales en función del nivel de riesgo para evitar este tipo de incidencia.

No constan reclamaciones ante esta AEPD por parte de los clientes afectados.

Por último, cabe señalar que la documentación generada de todo el proceso de detección, contención, respuesta, recolección y custodia de evidencias ante una posible brecha de seguridad de los datos personales es importante de cara a comunicaciones a las posibles partes interesadas tanto de carácter interno o externo, y para la elaboración de un informe final que tras su análisis permita extraer conclusiones. Este informe final, elaborado tras el seguimiento y cierre de este tipo de incidentes y su impacto, es una valiosa fuente de información con la que debe

alimentarse el análisis y la gestión de riesgos futuros. El uso de esta información servirá para prevenir la reiteración de hechos similares.

III

En el presente caso, la actuación de WALLAPOP, como entidad responsable del tratamiento, ha sido razonable y proporcional con la normativa sobre protección de datos personales e implantó nuevas medidas de seguridad proporcionales al riesgo evaluado para evitar la repetición de incidentes similares en el futuro.

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 NOTIFICAR la presente resolución a WALLAPOP S.L. con NIF B66049057 y con domicilio en c/ Meridiana 89, planta 6ª - 08026 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.

940-0419

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