- **Procedimiento N.º: E/02732/2020**

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 UBT COMPLIANCE SERVICES, S.L., delegada de protección de datos de la responsable del tratamiento FEU VERT IBÉRICA, S.A., en el que informan a la Agencia Española de Protección de Datos (en adelante, AEPD) que en fecha 10/03/2020, se detectó ataque mediante *phishing* en las opciones de pago de la página web de la responsable del tratamiento, el cual dispone como proveedor de servicios tecnológicos a la encargada del tratamiento HIBERUS TECNOLOGÍAS DE LA INFORMACIÓN, S.L.

Documentación aportada adjunta con la notificación de brecha de seguridad:

- Documento adjunto explicativo en detalle sobre el acontecimiento de la brecha de seguridad y elaborado expresamente para la AEPD a los efectos de notificación de dicha brecha por parte de la delegada de protección de datos del responsable del tratamiento.

- Captura de pantalla de la modificación de las opciones de pago en la página de la responsable del tratamiento que supuso la reseñada brecha de seguridad.

- Copia del email recibido por la responsable del tratamiento desde la encargada del tratamiento en que confirma haber detectado ataque de *phishing* por el cual la pasarela de pago quedaba suplantada y se podían obtener ilegítimamente por un tercero, datos personales de clientes asociados a pagos.

- Listado de los 271 afectados por la brecha de seguridad y modelo de correo electrónico previsto para comunicarles la incidencia.

SEGUNDO: En fecha 17 de marzo 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 de marzo de 2020

ENTIDADES INVESTIGADAS

FEU VERT IBÉRICA, S.A. (en adelante, la investigada), con NIF A79783254 y domicilio en ******DIRECCIÓN.1***.

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

En fecha 01/06/2020 se solicitó información a la investigada sobre los hechos manifestados en su notificación de brecha a esta AEPD. De la respuesta recibida el 11/06/2020 se desprende lo siguiente:

Respecto de la empresa:

- La investigada se identifica como entidad especialista en el mantenimiento de vehículos de tracción mecánica y se corresponde con la responsable del tratamiento en que se ha producido la brecha de seguridad.

- La investigada señala a HIBERUS TECNOLOGÍAS DE LA INFORMACIÓN, S.L. (con NIF B99344319) como encargada del tratamiento interviniente en la brecha de seguridad por proveerle servicios tecnológicos de la información y la comunicación.

- La investigada dispone como delegada de protección de datos a UBT COMPLIANCE, S.L. (con NIF B87114187) y así consta reflejado en la AEPD. Esta delegada de protección de datos de la investigada alega que fue ella quien comunicó a la autoridad de control la presente brecha de seguridad amparada en los artículos 39.d) y e) del *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)*. La delegada de protección de datos de la investigada aporta documento en que refleja entre sus servicios el de cooperar con la autoridad de control y el de actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento.

Respecto de la cronología de los hechos:

Todo según manifestaciones de la investigada:

- La brecha fue detectada con fecha de 10 de marzo de 2020, aunque el 5 de marzo de 2020, se identificó por su personal una modificación de la página web en las opciones de pago. Se pensó inicialmente que era un error y se eliminó este contenido novedoso de formas de pago reindexando la página, volviendo a su aspecto normal. Por lo tanto, se descartó inicialmente que fuera un ataque de *phishing* tras contactar con el proveedor de incidencias. La investigada aporta capturas de la pantalla de pago suplantada (en idioma portugués) en su página web y la pantalla de pago veraz (en idioma castellano).

- Se desactivó de forma cautelar el TPV (terminal punto de venta) la noche del 5 de marzo de 2020 al 6 de marzo de 2020. Se realizaron varias comprobaciones en distintos dispositivos y ubicaciones, no encontrándose nuevamente el error. Al no encontrarse error, el 6 de marzo de 2020 por la mañana se volvió a activar el servicio. No se encontró ninguna brecha de seguridad, en tanto que se pensaba que era un fallo de aplicación externa.

- Durante el fin de semana (días 7 y 8 de marzo de 2020) se realizaron, por el personal técnico, distintas comprobaciones en las que la página web resultaba aparecer correctamente.

- El día 9 de marzo de 2020 por la mañana, se recibió comunicación de un usuario en la que informaba de un posible copiado de sus datos de carácter personal, e identificando que al día siguiente le llegaron mensajes de teléfono pidiéndole autorización para confirmación de pagos por compras que no se habían hecho, sin que a este usuario se le hubiera cobrado nada. La investigada aporta copia de la comunicación del usuario que notificó el robo de sus datos personales a través del enlace de pago de la página web.

- Tras la recepción del email, se le notifica el asunto a HIBERUS TECNOLOGÍAS DE LA INFORMACIÓN para su investigación, y en la mañana del día 10 de marzo de 2020 dicha encargada del tratamiento confirma la brecha de seguridad indicando que se ha procedido a la eliminación del contenido de las opciones de pago de la página web con que se suplantaba su identidad y se obtenían ilegítimamente datos personales de clientes, que han puesto medidas para su detección y aseguramiento de que no vuelva a ocurrir, así como la evaluación del alcance de la incidencia.

- HIBERUS TECNOLOGÍAS DE LA INFORMACIÓN constató que la incidencia había tenido lugar desde el día 2 de marzo de 2020 (fecha estimada) hasta su completa resolución con fecha de 10 de marzo de 2020, aunque durante ese periodo se ejecutaron pruebas para conocer si se trataba de un error o si se estaba frente a un ataque intencionado exterior por medio de *phishing*.

- Posteriormente a la notificación de brecha a la AEPD, HIBERUS TECNOLOGÍAS DE LA INFORMACIÓN detuvo un segundo intento de ataque mediante su bloqueo en el mismo día y obtuvo las siguientes direcciones IP (protocolo de internet) desde las que se lanzaron los ataques:

    - ******IP.1***
    - ******IP.2***
    - ******IP.3***
    - ******IP.4***
    - ******IP.5***

El 2 de junio de 2020 la investigada denunció los hechos ante la Policía Nacional en la dependencia policial de ******LOCALIDAD.1*** bajo atestado nº ******ATESTADO.1***, de lo cual aporta copia firmada y sellada a los efectos. La investigada aporta captura de pantallas en que se constata que el 1 de abril de 2020 trasladó los hechos a la Brigada de Investigación Tecnológica de la Policía Nacional mediante correo/buzón electrónico y que dicho organismo acusó su recibo el 14 de abril de 2020, aunque no se considerase denuncia formal de los hechos.

La investigada expresa que no existen eventos análogos ni hechos similares acontecidos en el tiempo a esta brecha de seguridad de datos personales sufrida por su parte.

Respecto de las causas que hicieron posible la brecha de seguridad:

- La investigada relata que la incidencia afectó a la confidencialidad de los datos y que se realizó por medio de *phishing* (suplantación de identidad para la obtención ilegítima de datos) de manera externa e intencionada o dolosa.
- La investigada manifiesta que el atacante inyectó código malicioso en su servidor centrándose en el fichero JavaScript, el cual interviene en el proceso de la compra (validation.js), aunque el atacante no modificó la fecha y hora del fichero.
- La investigada informa de que dicho código JavaScript se ejecuta en el navegador del cliente, por lo que desde su servidor no se tienen registros de las peticiones que se han realizado desde el *iframe* que presenta el *malware* (código malicioso) en el momento de la suplantación.
- La investigada expresa que el *malware* en cuestión sustrae códigos de número de tarjeta de pago, fecha de caducidad de ésta y CVV (*Card Verification Value* – código de seguridad de la tarjeta), tales que se envían a un tercer sistema propiedad del atacante por medio de un error falso que se presenta en el navegador, pero sin romper la cadena del certificado SSL (*Secure Sockets Layer* – capa de puertos seguros) en momento alguno.
- La investigada detalla que los datos de pago terminan siendo enviados a su servicio de procesamiento de pago ("Redsys"*)* para que la transacción se ejecute, por lo que se dificulta en ese momento la detección de la anomalía si finalmente la compra se acaba realizando por el cliente. La investigada añade que el ataque tiene comportamiento aleatorio que complica su detección, ya que durante sus pruebas pudo comprobar que en ocasiones se mostraba la página de pago suplantada y en otras no lo hacía.

Respecto de los datos afectados:

- La investigada expone que los datos afectados se corresponden con:
    - Datos de identificación.
    - Datos económicos/bancarios: números de tarjetas, CVV y fechas de caducidad de las tarjetas.
- La investigada establece que sus sistemas de información no conservan datos relativos al pago de sus clientes y que sus bases de datos internas no se vieron afectadas por el incidente. La investigada defiende que desde septiembre de 2019 se exige factor de autenticación doble o múltiple para la validación de toda operación por lo que alega que los datos obtenidos del ataque no pueden usarse para realizar cargos o pagos fraudulentos.

- La investigada informa de que los datos afectados corresponden a 271 usuarios y clientes suyos. La investigada aporta copia de un listado con dichos afectados por la brecha seguridad elaborada a partir de quienes usaron como método de pago el TPV y pudieran ser susceptibles de robo de sus datos económicos/bancarios (la pantalla de pago suplantada con *malware* aparecía aleatoriamente, a unos accesos de clientes sí y otros no).

- La investigada manifiesta que sobre las posibles consecuencias para los afectados con la presente brecha de seguridad se consideran divulgados a un tercero, el atacante que podría usarlos con fines delictivos, aunque entiende que no se completó el ataque puesto que toda compra en su web requiere de confirmación que no se pudo producir.

- La investigada informa de no tener certeza de la utilización por parte de terceros de los datos personales de sus clientes obtenidos ilegítimamente en la brecha de seguridad a fecha 10 de junio de 2020.

Respecto de las medidas de seguridad implantadas con anterioridad la brecha de seguridad:

- La investigada aporta RAT (registro de las actividades de tratamiento) en que señala como actividad de tratamiento afectada por la brecha se seguridad:

Categoría de interesados	Categoría de datos	Medidas de seguridad	EIPD	Cesiones-categoría de destinatarios	Encargados del tratamiento	Subencargados de tratamiento	TID	Periodo máximo de conservación
Clientes e-Commerce	Datos identificativos Datos económicos-financieros Información comercial.	Copias de seguridad y recovery. Firewall, antivirus. Equipos protegidos usuario y contraseña. Permisos y roles restringidos.	No aplica	No son comunicados a terceros salvo obligación legal.	HIBERUS MAGENTO MAILCHIMP	No aplica	No aplica	5 años

- La investigada aporta un AR (análisis de riesgos) con base en un sistema de gestión de riesgos en el que aparece evaluada la actividad de tratamiento afectada por la presente brecha de seguridad. En dicho AR, el nivel de criticidad del riesgo asociado a la actividad “Clientes e-commerce” está catalogado como alto (en una escala de bajo/medio/alto) conforme a los siguientes cuatro criterios:

    - ¿Qué tipo de dato queda afectado al tratamiento?

    - Alcance del tratamiento.

- Contexto.
- Tipología de interesados.

- La investigada manifiesta que, tras evaluación de la actividad de tratamiento involucrada en la brecha de seguridad, el ciclo de vida del dato, la gestión de vida del dato, el número de afectados y la tipología de afectados, valoró y consideró que no era necesaria la realización de una EIPD (evaluación de impacto relativa a la protección de datos) sobre la actividad de tratamiento implicada en la brecha de seguridad.
- ***La investigada expone que disponía de las siguientes medidas antes del acontecimiento de la brecha de seguridad:***
  - ***A nivel técnico: sistema de monitorización "Nagios" de manera activa sobre el servidor.***
  - ***Monitorización del certificado de manera activa desde Nagios comprobando la cadena de seguridad.***
  - ***Sistema de firewall, actualmente se utiliza el sistema de iptables.***
  - ***Medidas propias del proveedor externo de alojamiento web "OVH".***
  - ***A nivel jurídico: procedimiento de notificación de incidencias de seguridad y registro de estas.***

Respecto de las medidas posteriores tomadas para la minimización del impacto de la brecha de seguridad y su resolución final:

- ***La investigada informa de que las medidas adoptadas inmediatamente fueron:***
  - ***Detección de los ficheros en los que se introdujo el código malicioso.***
  - ***Pasos del manual de buenas prácticas el continuous deployment (CI/CD): tomar Branch master como repositorio del código seguro y versionado, por lo que cualquier diferencia con el mismo se marca como malware y se pone en cuarentena.***
  - ***Creación de un sistema de control específico sobre ficheros involucrados para detectar que volvieran a ser infectados (activado desde el mismo momento en el que se eliminaron los ficheros en la detección).***
  - ***Lanzamiento de una herramienta de seguridad (OWAS ZAP) para la detección de problemas de seguridad adicionales.***

- ***Solicitud de la relación de peticiones al servidor en la última semana al proveedor externo de alojamiento web "OVH".***

- La investigada aporta copia del correo electrónico remitido por su parte el 12 de marzo de 2020 a los 271 afectados en que se les comunica el incidente ocurrido.

Respecto de las medidas implementadas con posterioridad la brecha para evitar su repetición:

- La investigada explicita haber procedido a realizar una auditoría sobre el activo afectado por la brecha de seguridad durante la semana del 20 de abril de 2020. Se aporta copia de resultados de dicha auditoría en que se detallan las acciones concretas a implantar, algunas de las cuales están resueltas, otras en curso y otras pendientes.

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 suplantación de identidad para la obtención ilegitima de datos de manera externa e intencionada o dolosa.

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 Registro de Actividades de Tratamiento y Análisis de Riesgo según se indica en los antecedentes y se han tomado las acciones posteriores oportunas para evitar la repetición del incidente.

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 notificar, 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 causada previsiblemente por un error puntual.

III

A la vista de las actuaciones practicadas, se ha acreditado que la actuación del FEU VERT IBÉRICA, S.A. 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 al FEU VERT IBÉRICA, S.A., con NIF A79783254 y domicilio en ******DIRECCIÓN.1***.

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