Procedimiento Nº: E/05724/2019
940-0419

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 quiebra de seguridad remitido por CENTROS COMERCIALES CARREFOUR, S.A. (en adelante CARREFOUR) en el que informan a la Agencia Española de Protección de Datos (en adelante AEPD) haber sufrido un ciberataque, que son clientes de la entidad.

Indican que han tenido conocimiento de la quiebra el 21/05/2019 a través de reclamaciones de sus clientes en las que manifiestan la imposibilidad de redención de los cheques ahorro por compras acumuladas con la tarjeta de fidelización CARREFOUR, al desaparecer sus saldos con compras de tarjetas BITNOVO.

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 quiebra: 23 de mayo de 2019

ENTIDADES INVESTIGADAS

CENTROS COMERCIALES CARREFOUR, S.A. con NIF A28425270 con domicilio en CARRETERA DE BURGOS Km. 14,500 - 28108 ALCOBENDAS (MADRID)

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

HECHOS:

De la información facilitada por CARREFOUR en la notificación de la brecha de seguridad así como en la contestación al requerimiento de información efectuado por esta Inspección de datos se desprende la siguiente cronología de hechos:

- El 17/05/2019 se detectó un gran número de intentos fallidos de acceso a cuentas de usuario informando la entidad GIGYA-SAP (encargado de tratamiento y proveedor de credenciales de usuario) de que estaban recibiendo un ataque, pero cerrando el caso al encontrarse la plataforma estable.

GIGYA-SAP recomienda implementar medidas para minimizar el impacto y decide aplicarlas.

- El 21/05/2019 desaparecen saldos de cheques ahorro con compras de tarjetas BITNOVO, reabriendo la entidad el caso. Se detectan intentos de conexión (aprox. 5000/segundo) desde orígenes sospechosos.
- El 22/05/2019 se comprueba que el 100% de las cuentas de usuario utilizadas fraudulentamente en línea de cajas con las que se ha efectuado compras y las de clientes que han puesto reclamación, se encuentran expuestas en repositorios de acceso públicos en Internet.
- El 22/05/2019 se denuncian los hechos ante la Unidad de Ciberdelincuencia de la Policía Nacional.
- El 23/05/2019 se notifica la brecha a la AEPD.
- El 27/05/2019 se amplía la denuncia ante la Policía Nacional con más información.

  En esta misma fecha se notifica a los afectados la brecha de seguridad.
- El 11/06/2019 CARREFOUR presenta a la Policía Nacional un informe como contestación al requerimiento de información realizado por esa Fuerza de Seguridad.

MEDIDAS PREEXISTENTES:

CARREFOUR ha aportado copia del Registro de Actividades de Tratamiento (RAT) en el que figuran los tratamientos comprometidos.

CARREFOUR ha aportado también copia de las Evaluaciones de Impacto de Protección de Datos (EIPD) efectuadas con anterioridad a la ocurrencia de la brecha,

Como medidas de seguridad aplicadas con anterioridad a la brecha, se encuentran:

- Cortafuegos de aplicaciones web que supervisa, filtra y bloquea en su caso el tráfico a las aplicaciones web y protege frente a ataques de diferentes tipos.
- Autenticación en nube del proveedor GIGYA-SAP (GIGYA está certificado ISO 27001 y ISO 27018:2014, y usa SSAE-16 Centros de datos certificación para hospedar sus plataformas). GIGYA-SAP coteja las credenciales y si son correctas proporciona los elementos de sesión necesarios con los cuales el cliente accede a la funcionalidad.
- HTPPS: Conexión segura (cifrada) entre navegador o aplicación del cliente y la infraestructura de CARREFOUR y el proveedor GIGYA-SAP.
- Los datos de los clientes (excluyendo las credenciales) se ubican en infraestructuras de almacenamiento y proceso propias de CARREFOUR, protegidas por diferentes medidas de seguridad que incluyen medidas de prevención de intrusiones, cortafuegos, *proxies* y bloqueo de determinadas direcciones IP.
- Se han realizado pruebas de intrusión realizadas para detectar vulnerabilidades sobre las aplicaciones que resultaron posteriormente comprometidas.

Consta realizado en octubre de 2018 un estudio de las posibles vulnerabilidades y métodos que un atacante podría utilizar para explotar la app.

Se monitorizan los accesos registrados, tanto infructuosos como satisfactorios mediante herramientas informáticas que incluyen el análisis de las tendencias del tráfico por IP de origen de la conexión.

Preguntados los representantes de CARREFOUR sobre el motivo por el cual las medidas de seguridad no pudieron evitar la brecha, indican que a su juicio no se trata de una brecha de seguridad de los sistemas de CARREFOUR, sino de un ataque en el cual se emplearon para los accesos las contraseñas de los clientes expuestas en otros sitios web, por lo que las medidas de seguridad de CARREFOUR no pudieron surtir efecto.

Como se ha indicado, CARREFOUR ha manifestado también que:

> *"se comprueba que el 100% de las cuentas de usuario utilizadas fraudulentamente en línea de cajas, con las que se ha efectuado compras y las de clientes que han puesto reclamación, se encuentran expuestas en repositorios en Internet.*

Esta afirmación consta en el informe técnico aportado por CARREFOUR sobre la brecha de seguridad ocurrida.

Sin embargo, por parte de esta Inspección de Datos se efectúan las siguientes comprobaciones en Internet:

- Se realiza una búsqueda mediante la que se puede consultar si una determinada cuenta se ha encontrado expuesta, y que contiene 773 millones de registros y 21 millones de contraseñas.
- Se realiza la búsqueda de las seis primeras direcciones de correo electrónico de las personas que han formulado reclamación ante CARREFOUR por la pérdida del saldo de su cheque ahorro, encontrándose que tres de ellas se han encontrado comprometidas y las otras tres no.

Se ha requerido a CARREFOUR para que aporte información sobre si se encontraban expuestas las contraseñas asociadas a los usuarios o solamente los códigos de usuario, así como a aportar documentación acreditativa sobre ello.

La acreditación solicitada trata de una autenticación simple (de un solo paso o un solo factor) por lo que la publicación de código de usuario y contraseña podría permitir el acceso. Sin embargo, la publicación únicamente del código de usuario haría necesario que durante el ataque se quebraran las medidas de seguridad implementadas (superación de la autenticación mediante averiguación de la contraseña). Hay que tener en cuenta que el código de usuario asignado que utiliza CARREFOUR coincide con el de otras aplicaciones de uso común, por lo que un dato que el usuario puede facilitar a terceros, al contrario que su contraseña que debe mantenerse en secreto.

Por otra parte, que el código de usuario y su contraseña asociada hayan sido expuestas en una lista de Internet no implica que se haya publicado la contraseña del usuario desde el sistema de información de CARREFOUR, ya que el usuario puede definir para el acceso a los servicios de CARREFOUR una contraseña distinta. Sin embargo, es frecuente que los usuarios especifiquen contraseñas comunes a varias aplicaciones por lo que de forma indirecta es el usuario el que expone al público su

clave de acceso. Además, la contraseña creada por el usuario no tiene necesariamente que coincidir con la de otras aplicaciones que utilice.

CARREFOUR aporta trece consultas a un determinado sitio web en el que se exponen trece códigos de usuario (no se indica nada de sus contraseñas asociadas) y un listado de otros siete códigos de usuario con el estado “No expuesta”.

CARREFOUR ha aportado la política de bloqueos ante intentos infructuosos de acceso que genera un bloqueo de la cuenta por 10 minutos cuando se producen 10 intentos no satisfactorios en una hora.

Entre las medidas relacionadas con la contraseña de acceso generada por el usuario que existían con anterioridad a la brecha se encuentran:

- En el proceso de creación de la contraseña para el usuario CARREFOUR se ofrece una medida de la robustez de la clave a medida que se va introduciendo.
- Se muestra la siguiente leyenda al usuario en la pantalla de creación de la contraseña *“Seguridad: No utilices datos de carácter personal para crear tu contraseña”*
- La contraseña debe ser alfanumérica y superior a seis caracteres.
- Cada nueve meses se realiza una campaña de mailing indicando la buena práctica de cambiar la contraseña.

3.- MEDIDAS POSTERIORES A LA BRECHA :

Indican que actualmente existen, junto con la política de bloqueo de la cuenta por 10 intentos fallidos, otras configuraciones complementarias en el sistema, que incluyen los bloqueos por IP, país y activación de Captcha.

- En el primer intento de acceso, bloqueo por país (aquellos que no se encuentran en la lista de países confiables)
- En caso de producirse varios intentos de acceso no satisfactorios de la misma cuenta en 1 hora, se fuerza Captcha.
- En el caso de producirse más intentos de acceso no satisfactorios desde la misma dirección IP en 1 hora, se fuerza Captcha.
- Bloqueo de rangos IP específicos no confiables.

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

En el presente caso, no consta acreditado que el acceso indebido a las cuentas de usuario tenga su origen desde el sistema de información de que dispone Carrefour. Existen indicios razonables que el atacante consiguió, tanto el usuario como su contraseña de los clientes, de sistemas ajenos al de CARREFOUR, a través de bases de datos obrantes en Internet que recopilan fraudulentamente este tipo de datos, de tal forma que una vez obtenido el código de usuario y su contraseña el acceso malicioso por terceros es posible sin que pueda ser detectado por las medias de seguridad que hasta el momento CARREFOUR tenía implantadas.

No obstante, conocido ahora el procedimiento externo por el que el atacante obtuvo los posibles códigos y contraseñas de los clientes, CARREFOUR deberá implantar medidas adecuadas para evitar la repetición de esta misma incidencia de ciberseguridad informando a los usuarios cuando crean su propia clave de entrada que deberá ser diferente a la de otras aplicaciones de uso común y obligar a su modificación en periodos de tiempo más breves o en caso contario será cancelada, entre otras muchas posibilidades de actuación.

En consecuencia, CARREFOUR, dada la condición de gran empresa que opera en diversos sectores, incluido el financiero, deberá actualizar sus protocolos de actividad digital con sus clientes a la luz de evitar este tipo de vulnerabilidades que en principio es, en cuanto a la ahora analizada de responsabilidad ajena a CARREFOUR, pero que dada la complejidad del método indirecto usado por el atacante se ha visto afectada.

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 ***CENTROS COMERCIALES CARREFOUR, S.A. con NIF A28425270 con domicilio en CARRETERA DE BURGOS Km. 14,500 - 28108 ALCOBENDAS (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.

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