G A _ P

Gómez-Acebo & Pombo

Las lecciones que nos deja una fuga de información cuando se notifica al regulador

Francisco Pérez Bes

Of counsel

Director del Área de Derecho y Economía Digital de Gómez-Acebo & Pombo

La notificación al regulador por parte del afectado por un incidente de seguridad es uno de los aspectos que más preocupan a las empresas desde la aplicación del Reglamento General de Protección de Datos y, más recientemente, de la Directiva NIS[1]. En estas normas se regulan, en el primer caso, la notificación de la fuga de datos ante la Agencia Española de Protección de Datos y, en el segundo, la notificación de la brecha de seguridad al correspondiente equipo de respuesta para emergencias informáticas (CERT[2]), además de al regulador competente para ello cuando proceda. En el caso que ahora analizamos, la agencia se pronuncia en relación con la adecuación de las medidas reactivas implantadas por la empresa afectada que ha notificado un incidente. Gracias a ello, la agencia declara el archivo de las actuaciones, y de su resolución podemos identificar algunas pautas que son consideradas positivamente por este organismo a la hora de resolver una notificación de esta naturaleza.

En el caso que ahora nos ocupa, una empresa tiene conocimiento, por medio de las afirmaciones de un periodista, de que en la conocida como *internet oscura («dark net»)* se habían puesto a la venta datos relacionados con el servicio de la empresa afectada. Tal situación

[1] Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio del 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

[2] CERT: sigla inglesa de *computer emergency response team*.

N. de la C.: En las citas literales se ha rectificado en lo posible —sin afectar al sentido— la grafía de ciertos elementos (acentos, mayúsculas, símbolos, abreviaturas, cursivas...) para adecuarlos a las normas tipográficas utilizadas en el resto del texto.

se produjo como consecuencia de un ataque informático que supuestamente había tenido lugar hacía casi dos años y que provocó una brecha de seguridad que comportó una fuga de datos personales, entre los que se encontraban nombres, direcciones de correo electrónico y nombres de usuarios en redes sociales.

De esta primera situación podemos extraer dos conclusiones: la primera, que la noticia de una fuga de datos suele venir del exterior (en ocasiones, por la prensa), por lo que debemos estar en condiciones de poder gestionar la recepción de esa noticia dentro de la organización cuando se produzca, porque previsiblemente será de manera inesperada. En este caso, cobra especial importancia la conveniencia de contar con un servicio de monitorización con capacidad para detectar —incluso en la internet oscura— este tipo de situaciones que afectan a una organización, pues ello nos permitirá actuar con prontitud.

La segunda conclusión tiene que ver con el origen de la incidencia. Es habitual que los incidentes de seguridad no sean detectados de manera inmediata, sino que haya transcurrido cierto tiempo hasta que se tiene conocimiento de ellos, bien porque se trata de una de las amenazas conocidas como APT *(advanced persistant threat)* —que se ocultan en los sistemas afectados durante el máximo tiempo posible—, bien porque la organización carece de las herramientas técnicas adecuadas para poder detectar un incidente de esta naturaleza de manera inmediata.

Ante la situación descrita y sin perjuicio de la posible concurrencia de un delito, la empresa afectada llevó a cabo una exhaustiva investigación interna antes de notificar a la Agencia Española de Protección de Datos una brecha de seguridad provocada por el acceso inconsentido de un tercero a los servidores de la empresa anterior al robo de esa información. Y, aunque no se pudo determinar la causa que provocó la citada brecha ni la forma en que el supuesto cibercriminal accedió a los sistemas de la empresa y tampoco se pudo acceder a la supuesta web donde se había puesto a la venta la información robada, se decidió notificar al regulador.

En este caso hay que añadir un elemento adicional, como es que el paso del tiempo desde la presunta brecha (octubre del 2017) hasta el conocimiento de ésta por parte de la empresa afectada (febrero del 2019) impide confirmar de manera concluyente que los datos supuestamente vendidos en la internet oscura proviniesen de los servidores de la ahora denunciante. Y de ese mismo modo tampoco se pueden obtener datos forenses que permitan determinar el origen de la fuga.

¿Qué acciones pudo acreditar la empresa afectada ante la Agencia Española de Protección de Datos para resolver favorablemente este incidente de seguridad?

La importancia de esta fase es de gran relevancia, puesto que del nivel de diligencia mostrado puede depender que se archiven las actuaciones —como finalmente ocurrió en este caso— o que se abra un procedimiento sancionador contra la empresa víctima del ciberataque.

Tal y como se aporta ante la inspección, una vez tuvo ésta conocimiento del incidente, la empresa activó de inmediato su procedimiento interno de respuesta a brechas de seguridad, además de constituir un equipo interno de investigación para evaluar el potencial daño que dicha fuga pudiera producir a los afectados y de diseñar un plan de acción a corto y a largo plazo.

Sin perjuicio del cambio de contraseñas, revocación de claves de acceso y de activar la autenticación multifactor, se actualizó la política de seguridad en vigor para incluir nuevas exigencias y se añadieron nuevos requisitos técnicos adicionales a los ya existentes.

Desde el punto de vista organizativo, se informó a la plantilla de la empresa de la existencia de la brecha de seguridad y se celebró una acción formativa para los empleados. Adicionalmente, se reabrió un programa de recompensas *(bug bounty)* mediante el cual veinticinco investigadores de seguridad *(hackers)* pudieran encontrar vulnerabilidades dentro de los sistemas de la compañía. Toda esta información se puso a disposición de la inspección, además de otra información de control interno, entre la que se pueden destacar la evaluación de impacto, el análisis de riesgos o la copia del registro de actividad.

En este caso, la actuación diligente de la empresa, demostrada tanto en las actuaciones técnicas de investigación y refuerzo de equipos como en otras actuaciones procedimentales e informativas entre sus empleados y en la ausencia de denuncias de terceros, permitió a la Agencia Española de Protección de Datos sostener que había quedado acreditado que la actuación reactiva de la empresa afectada había sido acorde con la normativa sobre protección de datos, lo que llevó a tal organismo a acordar el archivo de las actuaciones.

A la vista de lo anterior, podemos afirmar que, ante un incidente como el descrito en este caso, resulta fundamental contar con los procedimientos y medidas adecuadas tanto de naturaleza técnica como organizativa. Cabe destacar que, en lo que a la ciberseguridad respecta, tan importante es implantar y reforzar continuamente las acciones preventivas como disponer de medidas reactivas eficaces y suficientes para el supuesto de que, a pesar de todo, el incidente haya tenido lugar.

En este caso, y a los efectos de gestionar la responsabilidad de la empresa afectada, así como la de sus administradores y directivos, resulta fundamental contar con el diseño de una política global y eficiente en la que se incluyan acciones preventivas (de concienciación, sensibilización y formativas) y reactivas (investigación, forense, **ciberseguros**, *bug bounty*) conformadas por medidas de naturaleza técnica y organizativa adecuadas y efectivas que permitan acreditar la diligencia debida.