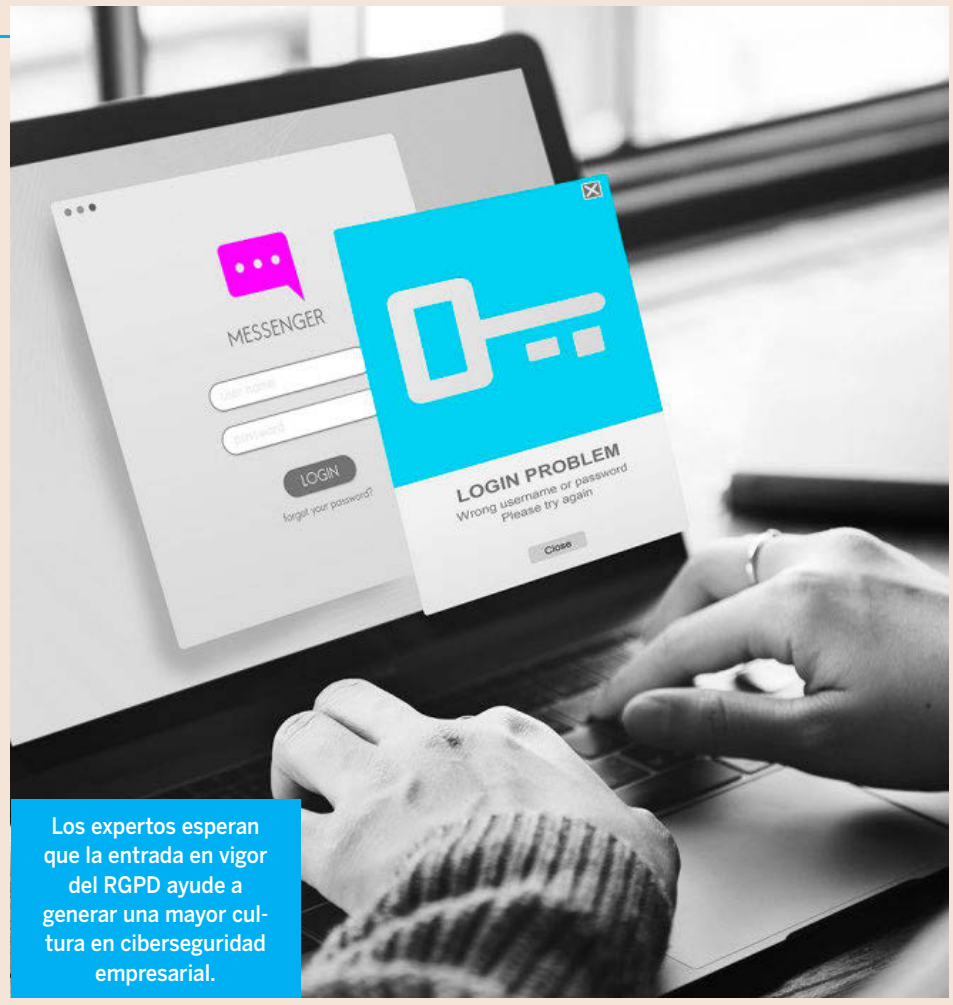
CIBERSEGURIDAD

Se acabó ocultar las brechas de seguridad

La nueva ley de protección de datos exige a las compañías comunicar las violaciones de seguridad. **Por M. Prieto**



Los expertos esperan que la entrada en vigor del RGPD ayude a generar una mayor cultura en ciberseguridad empresarial.

ENTRA EN VIGOR EN MAYO

La seguridad en la nueva ley

- **Seguridad de los datos.** La legislación exige la comunicación de las violaciones de datos o brechas de seguridad salvo que no supongan un riesgo para los intereses y libertades de los interesados.
- **Celeridad.** La comunicación a la Agencia de Protección de Datos se debe hacer en un plazo máximo de 72 horas.
- **Medidas.** Las empresas deberían implantar un protocolo que detalle cómo actuar en estos casos y minimizar así el impacto económico y reputacional de una brecha.

No se sorprenda si, a partir de mayo, lee con frecuencia noticias sobre brechas de seguridad producidas tras ciberataques a empresas europeas, incluidas españolas. No es que, de un día para otro, los *hackers* hayan redoblado los ataques hasta el punto de quebrar sistemáticamente la seguridad de las organizaciones. Sencillamente, es que hasta ahora no hemos sido conscientes de la existencia de estas brechas porque la legislación no obligaba a las empresas a comunicarlas. Una situación que va a cambiar con la entrada en vigor en mayo de la nueva Ley General de Protección de Datos, una legislación que incrementa las exigencias para las empresas e instituciones que manejen datos de consumidores europeos.

El articulado afecta directamente a la política de ciberseguridad de las empresas. Así, establece la obligación de comunicar las violaciones de seguridad a la Agencia Española de Protección de Datos en un plazo de 72 horas desde que la organización tiene conocimiento de la misma, salvo que no suponga un riesgo para los derechos y libertades de los interesados. Si esta violación supone un alto riesgo para los afectados, además debe comunicarlo a éstos directamente y sin dilación. La ley entiende como violación de la seguridad la que ocasione "la destrucción, pérdida o alteración accidental o ilícita de datos personales (...) o la comunicación o acceso no autorizados a dichos datos". Si no hay notificación, la empresa se expone a multas que pueden ascender a 20 millones de euros o el 4% de su facturación anual.

Finalidad

Según apunta Jesús Yañez, socio de Ecija, esta novedad en el ámbito de la comunicación de las violaciones de la seguridad tiene tres finalidades: ayudar a la coordinación de respuesta ante incidencias por parte de las autoridades, lograr mayor transparencia de cara a los particulares y aumentar la concienciación entre las empresas para implementar las medidas de seguridad necesarias.

"Vamos a asistir a una oleada de informaciones sobre brechas de seguridad en empresas europeas", opina Luis Corrons, director técnico del laboratorio de la empresa española de ciberseguridad Panda.

Noticias que, hasta ahora, han protagonizado fundamentalmente empresas estadounidenses, que están obligadas legalmente a comunicar estos ciberataques, como ha ocurrido con los robos masivos de datos de clientes que han sufrido compañías como el servicio de Internet Yahoo!, el banco JPMorgan, la cibertienda eBay, la firma de solvencia crediticia Equifax, o la aseguradora Anthem.

EL DATO

20

millones de euros

La no notificación a las autoridades de una brecha de seguridad que afecte a datos personales puede acarrear sanciones de 20 millones de euros o el 4% de la facturación anual.

Efecto positivo

Corrons apunta un efecto positivo de la nueva legislación al ayudar a generar una mayor cultura de seguridad. "Va a favorecer una mayor preocupación por la ciberseguridad por parte de empresas e instituciones. Es cierto que nadie está libre de ser víctima de un ciberataque, pero cuando no hay obligación de comunicarlo a los clientes afectados y a las autoridades, la preocupación puede ser menor ", opina este experto, quien considera que debido a la nueva normativa, las empresas destinarán "más recursos, presupuestos y atención a la ciberseguridad".

En esta línea, Daniel González, *senior account manager* de la empresa de soluciones de movilidad MobileIron, también considera que el nuevo reglamento se traducirá en un aumento de los recursos destinados a seguridad. "Ya estamos constatando que las empresas están dedicando más presupuesto a implementar herramientas que les ayudan con la gestión y la securización de todo tipo de dispositivos. El GDPR ayudará a que adopten soluciones de ciberseguridad de nueva generación para plataformas de movilidad y para detección de *malware*", opina González.

"Vamos a ver una oleada de noticias sobre brechas de seguridad", opina Corrons, de Panda

Los expertos aconsejan a las empresas establecer un protocolo para notificar brechas

Se espera que las empresas implanten herramientas de protección más avanzadas

Protocolo

Además de nuevas herramientas, las empresas deberían implantar un protocolo para manejar estos supuestos, puesto que la ley impone un marco temporal muy corto para comunicar las brechas y, además, puede ocurrir que éstas ocurran en los sistemas de los proveedores tecnológicos de una empresa. "Una regulación interna procedimentada es necesaria para cumplir plazos y, sobre todo, realizar una notificación coordinada que aminore riesgos económicos y reputacionales", apunta Yañez.