Los fallos en ciberseguridad de los proveedores ya acarrean multas para las empresas

Las autoridades sancionan ya a las compañías por las brechas de seguridad, Inglaterra multa con 1,4 millones a Ticketmaster por un fallo en chatbots

Los fallos de ciberseguridad de los proveedores ya acarrean multas a las empresas. Las autoridades de los países ya cuestionan la diligencia debida en lo que respecta a las medidas de ciberseguridad, así como a la responsabilidad de la empresa a la hora de gestionar el riesgo de que los ciberataques tengan su origen en las vulnerabilidades de los proveedores y otros terceros ajenos a la propia empresa, lo que se conoce como third party compliance, o control del cumplimiento normativo de terceros.

La **Autoridad de Control de Reino Unido** (ICO) ha sancionado con 1,4 millones de euros a la empresa Ticketmaster por una vulnerabilidad en un chatbot que fue explotada por un ciberdelincuente para acceder a más de 60.000 tarjetas de crédito de clientes. En este caso, la sanción a Ticketmaster se fundamenta en tres elementos principales, como son que no se evaluaron suficientemente los riesgos al instalar un chatbot en la página de pago, no se comprobaron debidamente las medidas de seguridad adoptadas por el tercero que instaló dicho chatbot y no se actuó en el tiempo debido, como lo demuestra el hecho que la empresa tardara más de nueve meses en identificar el incidente, lo que ha sido considerado por el regulador británico como un agravante a la hora de imponer su multa.

Según la **consultora Gartner**, desde el inicio de la pandemia más de la mitad de los directores de compliance de las empresas creen que la ciberseguridad y las fugas de datos son los riesgos externos que más han aumentado.

A esto hay que añadir la apresurada implantación del teletrabajo, también en el caso de los proveedores, quienes han hecho grandes esfuerzos para poder mantener su actividad inalterada. Sin embargo, la ausencia de planificación hace improbable que tales organizaciones hayan implementado prácticas adecuadas para proteger sus sistemas y, en consecuencia, las de los clientes a cuyas redes se conectan y con los que interactúan.

Los responsables de cumplimiento de las organizaciones deben incluir, dentro de sus planes, acciones para prevenir, identificar y mitigar el ciberriesgo inherente a estos terceros con los que la empresa trabaja en cada momento. Esto debe incluir la exigencia a sus proveedores de que **acrediten, por contrato, un nivel de adecuación apropiado con carácter previo** a comenzar a trabajar con ellos, explica Francisco Pérez Bes, socio de Derecho digital de Ecix y antiguo secretario general del **Instituto Nacional de Ciberseguridad de España** (Incibe).

Según los especialistas, a los efectos de garantizar la continuidad de nuestro negocio, se hace preciso llevar a cabo una **revisión exhaustiva de los contratos existentes con proveedores** de alto riesgo, para poder anticiparnos a cualquier tipo de interrupción financiera o comercial derivada de incidentes de ciberseguridad que puedan sufrir.

Este tipo de actuaciones pueden llevarse a cabo de forma remota, utilizando plataformas de third party compliance (o TPC) que permiten organizar y estructurar auditorías de proveedores y exigirles un adecuado nivel de diligencia. Esto **resulta fundamental en el caso de sufrir un ciberataque**, ya que, llegado el caso, será necesario que acreditemos qué tipo de medidas se implementaron para evitarlo. Y ese cuidado al elegir proveedores confiables puede ser clave a la hora de defendernos en un eventual procedimiento sancionador, destaca Pérez Bes.

Fuente: elEconomista.es

Los responsables de cumplimiento deben prevenir el riesgo de terceros, advierte Pérez Bes