El caso de Air Europa muestra el problema de ciberfraudes, que cada vez afectan a más empresas en España

LINK DE LA NOTICIA

Fuente: Diario Jurídico

"Las empresas deben invertir más en políticas de prevención y control del fraude. *Al final esta inversión siempre resulta rentable, dado que se ayuda a detectar y prevenir el mismo, instaurando en las organizaciones controles eficaces para prevenir el fraude interno, y el ciber fraude. Para acometer estas inversiones, es necesario que la cúpula directiva esté sensibilizada con este problema, debiendo conocer la alta exposición a estos ataques de cualquier compañía, independientemente del sector donde esté presente la compañía, hay dos tipos de compañías, las que han sido víctimas de un ciberataque, y las que lo han sido, y todavía no lo saben"*, concluye el experto.

Ante esta problemática, **Felipe García recuerda la importancia que tienen las políticas de 'compliance' dentro de las empresas, así como la formación de la persona encargada del departamento, el llamado 'compliance officer**', para "*que puedan colaborar con los departamentos de riesgo y de esa manera puedan focalizar qué práctica les puede afectar a su cuenta de resultados, bien sea ciberataque, malware, phishing o alguna técnica parecida que suelen tener un impacto importante cuando esa organización lo sufre. A la pérdida económica, y de posibles clientes, hay que añadir el daño reputacional que entraña un ciberataque a una organización, sobre todo si esa compañía tiene datos sensibles, o es una empresa tecnológica, a la que se presupone un mayor control de su información y por ende unos controles antifraude más sólidos y punteros"*.

La importancia del 'compliance' como herramienta de prevención

En este sentido, los resultados obtenidos por el informe de la AECF son claros: **el 42% de los casos registrados fueron fraudes de admisión en punto de venta, o lo que es lo mismo, fraudes durante transacciones en línea** en los que los ciberdelincuentes utilizan técnicas de robo de credenciales o tarjetas falsas; a los que le siguieron (21%) el robo de datos o malware a través de software maliciosos de infiltración en sistemas informáticos.

"El fraude sigue creciendo de forma exponencial, lo que hace necesario redoblar los esfuerzos de lucha contra esta lacra", comenta el vocal de la Junta Directiva de la World Compliance Association, quien añade, *"hay organizaciones que acceden a nuestros datos para utilizarlos de forma fraudulenta -así ha pasado en el Ayuntamiento de Sevilla de manera reciente o el Clinic de Barcelona- y tras esa venta de datos se suelen hacer ciberataques a gran o pequeña escala, si es a empresas o personas físicas"*.

Este tipo de ataques suponen una problemática real y en auge en España, y es que, tal y como revela la Asociación Española de Empresas contra el Fraude (AECF) en su último informe, **el 68% de las empresas españolas reconoce haber sido víctima de más casos de fraude que el año anterior**, mientras que solo un 5% ha detectado un descenso. Preocupante es también que uno de cada dos afectados (47%) apunta a que la cuantía de las pérdidas ocasionadas por el fraude ha sido

superiores a las del ejercicio anterior.

"Hoy le ha tocado a Air Europa, mañana será otra gran sociedad, pero en silencio, muchas sociedades, son también víctimas del fraude*, lo que implica a los Departamentos de Compliance un esfuerzo extra para poder mitigar su impacto en la reputación y en la cuenta de resultados de las organizaciones, sin duda alguna una difícil tarea"*, afirma el experto.

El reciente ciberataque a la aerolínea Air Europa, que ha expuesto los datos bancarios (números de tarjeta, fechas de caducidad y CVV) de miles de clientes, vuelve a demostrar lo desprotegidas que siguen estando muchas empresas en España y la necesidad de invertir en prevención, según advierte Felipe García, abogado y socio del despacho Círculo Legal Madrid.