Los casos de fraude empresarial crecieron en el 2022, lo que obliga a invertir en prevención

El VI congreso de la Nacional Antifraude de la World Compliance detecta la necesidad de revisar los modelos de cumplimiento para dar respuesta a las amenazas nuevas de IA y ciberseguridad

El informe presentado por **César Gilmartín**, director técnico de la Asociación Española de Empresas contra el Fraude (AECF) revela que **el 68% de las empresas encuestadas confirma haber sido víctima de más casos de fraude que en el año anterior**, mientras que el resto (32%) indica que en su caso no han notado apenas diferencia respecto al ejercicio anterior o incluso han experimentado un descenso (solo un 5%).

En lo que se refiere a la cuantía de las **pérdidas ocasionadas por fraude**, el **47% de los encuestados apunta que estas han sido superiores a las del ejercicio anterior**, mientras que el 32% ha observado un descenso. El 21% restante manifiesta no haber detectado una variación significativa.

Analizando los canales a través de los cuales están llegando los ciberataques, **el 40% de las empresas siguen apuntando un año más al canal directo online** como la principal vía de entrada de la ciberestafa, seguido del prescriptor online con un 23% del peso relativo. En tercera posición de sitúa el canal telefónico (17%) seguido del prescriptor/sucursal presencial (14%).

En cuanto a la tipología de fraude, Gilmartin resaltó el **fraude de admisión en punto de venta digital** sigue la línea continuista de los últimos informes, alcanzando en esta ocasión un 42% de los casos registrados. Esta forma de fraude relacionada con las transacciones en línea, donde los **ciberdelincuentes utilizan técnicas como el robo de credenciales** o el uso de tarjetas de crédito falsas para realizar compras fraudulentas, parece ser sin duda la más complicada de combatir.

Por su parte el **fraude de admisión en punto de venta presencial** es una preocupación menos significativa, representando un 16% de los incidentes reportados.

El **fraude de cuenta en el inicio de transacción**, referido a la usurpación de cuentas legítimas para iniciar transacciones fraudulentas, representa un 21% de los incidentes detectados.

A la par se encuentra el **robo de datos o malware**, relacionado con la infiltración de sistemas informáticos por parte de software malicioso con el objetivo de robar información confidencial, como datos de tarjetas de crédito o información personal, que cuenta con un peso también del 21% de los casos analizados.

Revisión de políticas de ‘compliance’

Felipe García, socio de Circulo Legal y vocal de la Junta Directiva de la World Compiance Association indica que "**el fraude sigue creciendo de forma exponencial**, lo que hace necesario redoblar los esfuerzos de lucha contra esta lacra. 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. Tras esa venta de datos se suelen hacer ciberataques a gran o pequeña escala, si es a empresas o personas físicas"

Desde su punto de vista, en este contexto se hace cada vez más necesario "**formar a los compliance officers en estos temas para que colaboren 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 parecida que suelen tener un impacto importante cuando esa organización lo sufre".

A su juicio, "como hemos visto en algunas de las sesiones de este Congreso se ha hablado de evitar el fraude. En algunas de ellas se habla de las pérdidas económicas de las empresas por este tipo de situaciones, habida cuenta de la multitud de fraudes que hay, **no sólo por los ataques externos sino también el fraude interno**. El fraude interno es un problema y esos insider hacen operaciones ficticias, falsificación de facturas y otras parecidas. Es fundamental invertir para frenarlo".

En este contexto, García cree que "**las empresas deben invertir más en políticas de prevención del fraude**. Al final se rentabiliza porque se ayuda a detectar el fraude y cuando sucede ese problema se puede gestionar mejor su impacto. Es importante, conocido el mapa de riesgos de las organizaciones, hacer esas inversiones que ayuden a frenar la exposición de la compañía a dichos fraudes, algunos de los cuales tienen la forma de ciberataques".

Respecto a la **llegada de la Inteligencia Artificial (IA)**, "hay que darse cuenta que ya se está utilizando para suplantar identidades o realzar ataques informáticos. En esos momentos es un **problema real que tienen las empresas y los ciudadanos**, con lo cual es necesario una regulación en cuanto al uso, limitando ese uso respecto a la duplicación de caras, gestos o voz para evitar que con una videollamada se abra una cuenta de un tercero. Es una cuestión en la que la UE está trabajando en un futuro Reglamento de IA, necesario para regular su desarrollo como tecnología disruptiva que es para prevenir ese fraude".

Este abogado recuerda que "**nuestro país va a tener un regulador específico, AESIA, para el desarrollo de la IA** y se va a implementar un sandbox para testar esta regulación en las empresas que se alojen en este nuevo entorno desregulado. Hay que recordar que la IA no es sólo protección de datos, afecta a otros derechos fundamentales. Habrá que ver muy bien su implementación y como se coordina con el regulador existente en materia de privacidad que es la AEPD".

En esta coyuntura, Felipe García cree que las empresas "tienen que revisar sus políticas de riesgo y si ven que el fraude puede crecer más realizar las inversiones correspondientes para prevenir este tipo de comportamientos irregulares. **La inversión debe ser en tecnologías, en medios, en personas físicas que puedan liderar estos proyectos de control** donde la gestión de los datos es importante para prevenir fraudes con el de blanqueo de capitales. Ahí el papel del *Compliance Officer* es clave para orientar a cada empresa de lo que tienen que hacer".

Sobre la ley de protección al denunciante, cree que va a ayudar a detectar más bolsas de fraude. "Para ello es fundamental que se complete la normativa porque aún no existe la Autoridad Independiente, que es la que debería tener capacidad para sancionar esas conductas irregulares y revisar esas denuncias. Esa Autoridad tiene competencia de mandar la denuncia a Fiscalía, Competencia o la CNMV, dependiendo de lo que se denuncie".

El problema de la IA generativa

Para **Juan Jesús Valderas**, responsable de Disputas e Investigaciones de Álvarez & Marsal en España y ponente de este evento "no es tanto que se esté perdiendo la lucha contra el fraude como se pudiera pensar, la cuestión es que **las nuevas tecnologías abren frente todos los días** y a veces podemos tener esa impresión. Las mafias organizadas parece que van un paso por delante en este tipo de cuestiones".

Desde su punto de vista, "**la llegada de estas tecnologías obliga a revisar las políticas de *compliance***, políticas que deben revisarse con regularidad para adaptar el mapa de riesgos de cada organización al momento actual. **No se pueden fijar unos procedimientos o métodos de control de manera estática**. Hay que revisarlos de manera regular y si nuestra entidad es fruto de algún incidente, es inevitable hacerlo para saber realmente qué ha pasado y enviar otros en el futuro".

En opinión de ese abogado, "**las preocupaciones actuales de empresas y asesores legales tiene que ver con el impacto de la IA**, que tiene una vertiente positiva para este tipo de entidades desde el punto de vista de mejora de eficiencia a nivel interno y con el cliente. Sin embargo, hay que ver cómo puede afectar su uso a los métodos habituales de control y prevención establecidos por las propias compañías para detectar el fraude. Ahora mismo es complicado saber cuál será ese impacto".

A este respecto, Valderas confiesa que “con estas nuevas tecnologías siempre pasa lo mismo; **se sobrevalora el impacto a corto plazo y se subestima a largo**. Creo que con la IA va a pasar algo parecido. Habrá que ver como gestionan las empresas dichas herramientas y su adaptación al marco normativo europeo en forma de Reglamento que parece previsible que estará operativo antes de que acabe este año”.

Valderas cree que “en España existe un problema cultural importante. Las empresas **sólo se plantean invertir en prevención cuando han sufrido un problema de fraude** o lo han visto en su competencia. Al mismo tiempo, los reguladores no ejercen la función de control con el rigor y con la energía que deberían hacerlo. La CNMC está activa en prácticas contrarias a la competencia y como se nota, sin embargo, **el Banco de España ha tenido escasas actuaciones en materia de blanqueo de capitales** fuera de su intervención en el Banco de Madrid”.

A su juicio, “no es tanto el endurecimiento de sanciones como **asegurarse que se ponen los medios adecuados para identificar y sancionar todas las infracciones** que se produzcan. Si hay cien infracciones hay que tratar a todas por igual y ponerles una sanción justa. Sin embargo, por el momento se opta a elegir dos empresas para sancionarlas con fuerza, algo que es criticable realmente”.

Para este experto, “el problema de los responsables de compliance en las empresas es que **tenemos que reivindicar su papel en todas las organizaciones**. No es fácil convencer a nuestros jefes, responsables de las empresas, de que **hay que invertir más en prevención** y que nuestro papel es clave para gestionar esos modelos de compliance desde la prevención del delito. Todo lo que pedimos es necesario. Se progresa, pero de forma más lenta de lo que se esperaba a nivel de cumplimiento en las empresas”.

Sobre la ley de protección al denunciante, con cien días ya en vigor, “hay que darse cuenta de que la **utilidad de los canales de denuncia debe ayudar a una mayor denuncia del fraude** y a identificar esas malas prácticas muy recurrentes en bastantes empresas. Hay que saber gestionar bien este tipo de situaciones que ahora proliferan. A lo largo de mi carrera siempre he visto que una parte de ese fraude se localiza a nivel interno en las propias empresas y organizaciones.

No se invierte en alertas tempranas

Juan Carlos Galindo, experto en prevención de blanqueo de capitales y financiación del terrorismo, destaca que a lo largo de estos 12 años de actividad profesional se constata un repunte del fraude. “**El primer síntoma de que una economía no va bien tiene que ver con el aumento de los fraudes** y estafas en compañías de telecomunicación y seguros. Detectamos sólo un 10% o un 20% del total”.

Al mismo tiempo, advierte que “**los mecanismos para la detección y prevención temprana de ese fraude quizás no sean los adecuados**. En algunos casos se utiliza una cuenta corriente de un banco que es falsa, no hay usurpación de identidad. Esa cuenta corriente se apertura físicamente. **Estamos ante un gran problema** con algo que es básico, que es la diligencia debida, la identificación formal”.

Al mismo tiempo, revela que “las cuentas de apertura online **no disponen de los estándares adecuados para esa identificación real**. Hemos detectado que los piratas informáticos roban DNI, fotografías para luego suplantarlas y hacer los selfis de forma clara. Hay que revisar esas alertas tempranas y también es el momento de **revisar los programas de *compliance* ante lo que se avecina IA o nuevas tecnologías**”.

Desde su punto de vista, “**hay algunas empresas que prefieren pagar esas multas o rescates de los ciberataques a no invertir**. Sobre las multas que impone el SEBPLAC, son escasas. Deberían ser como las del RGPD, que supone un porcentaje entre el 4% y 6% de la facturación global de esas empresas. **Son sanciones administrativas escasas**, lo que anima a las empresas a no invertir en esos programas de prevención. Al final el daño reputacional que se genera es importante”.

Frente a la **doble victimización que sufren muchos consumidores**, a los que se les ha robado dinero de su cuenta y pese a que reclaman a sus bancos **acaban en la vía judicial para demostrar su inocencia**, Galindo señala que Europa está diciendo que los bancos tienen su responsabilidad. Igual que a nivel físico toman medidas para evitar esos robos, en la parte online tienen la misma obligación de poner esas medidas. El problema es que sólo ponen algunas. En este contexto, la tendencia cambia y ya hay bancos que devuelven al consumidor ese phishing y otras parecidas

En este contexto, **con la llegada de la IA el panorama puede ser más complejo**. “Ya se está complicando, la IA generativa es un antes y un después para todos. Con buen criterio decía **Cesar Gil** que ya en la Deep web ya se puede comprar el Crime as a services, producto ideado para hacer el mal, desde DNI, hasta un propio software para hacer phising o ransomware con apenas 600 dólares. Tenemos un problema”.

El gran problema de estos fraudes financieros a gran escala es que “normalmente, **aquel que lo comete es una organización internacional que no está en España y es difícil localizarla**. Es el caso del ciberdelito a gran escala. Estos grandes fraudes se hacen desde fuera de nuestro país y es complicado realizar la investigación y sentar a sus culpables. Ahora, con la normativa que traspone la directiva de protección al denunciante puede ayudar a detectar más el fraude interno de las empresas”.

Fuente: economistjurist.es

LINK DE LA NOTICIA