18/02/2024

La ciberseguridad se mete en "terreno compliance"

Ahora cualquier organización, incluso aunque sea diminuta, puede ser objeto de un ciberataque. Las organizaciones cada día son más conscientes de la necesidad de combatir la ciberdelincuencia.



No es ninguna novedad afirmar que la ciberseguridad se ha convertido en una de las principales preocupaciones de los directivos. Lejos quedan aquellos tiempos donde solo unas pocas empresas eran las que sufrían ciberataques. Ahora cualquier organización, incluso aunque sea diminuta, puede ser objeto de un ciberataque. Las organizaciones cada día son más conscientes de la necesidad de combatir la ciberdelincuencia, no solo los resultados del ejercicio están en

Durante el año 2023, la mayor parte de los ataques han sido originados por Cl0p, a través de campañas como la de MOVEit, (Shell, BBC y el Departamento de Energía de Estados Unidos, entre otros afectados), otros, como Black Cat, (MGM Resorts), también han tenido gran impacto.

Akira, Royal, Lockbit, y Black Basta también han tenido, por desgracia, una □□□□□A recaudación por los ciberdelincuentes, el mejor dato que hemos tenido, es que solo un 29% de las organizaciones pagan las extorsiones de los hackers, lo que deja la cifra en el porcentaje más bajo de los últimos años, un dato que arroja cierto optimismo entre los directivos.

La ciberseguridad se ha vuelto en el cuerpo directivo cada vez más crítico y ocupa un papel clave en los planes estratégicos de las organizaciones, sobre todo en las empresas con componente tecnológico. De la misma manera, la Unión Europea, ha puesto en la ciberseguridad, un pilar clave donde pretende fortalecer la seguridad en las organizaciones públicas y privadas, sabedora de que, sus ciudadanos, estarán a salvo, no solo ante el robo y filtración de datos, sino incluso ante actos de ciberguerra, cada vez más frecuentes y lesivos.

Hasta hace poco tiempo, la tarea de ciberseguridad solo impactaba sobre los departamentos de seguridad de la información, pero cada vez es más frecuente, ver cómo las organizaciones enclavan el control y monitorización de su ciberseguridad en los departamentos de compliance, ya que muchos empresarios están entendiendo que debe ser esta figura la que pilote los controles y procedimientos establecidos en las organizaciones, cuyo objetivo principal, es mantener los sistemas informáticos indemnes ante los accesos de los hackers.

La ciberseguridad ha quedado en los últimos meses relegada por la IA, que ha impactado en las organizaciones y en la economía global como una forma de generar riqueza, y optimizar los procesos de trabajo. Pero, no es menos cierto, que la IA, de momento, al menos en las pymes, no ha penetrado en los departamentos de compliance incrementando su trabajo, salvo para instaurar los típicos procedimientos de uso de la inteligencia artificial para trabajadores y directivos. Sin embargo, el papel del compliance officer, en materia de ciberseguridad, va creciendo paulatinamente, y en muchas organizaciones, los departamentos de seguridad de la información, están reportando sobre su trabajo e incidencias al compliance officer.

Este hecho da buena cuenta de que los departamentos de compliance, son verdaderos repositorios de funciones y tareas de control, sin olvidar, por supuesto, de la importante labor técnica de los departamentos de seguridad de la información, quienes son la primera línea de protección para una organización. Sin duda, los departamentos de seguridad de la información, tienen el gran reto de comprender y conocer todos los riesgos de su organización, como un todo, y solo con ese conocimiento y el trabajo en equipo con los departamentos de compliance, se consiguen los objetivos.

Estas decisiones empresariales vienen motivadas, en parte, por dos razones. La primera es porque el compliance officer va tomando posición cerca del cuerpo directivo de las organizaciones, y segundo, y factor clave, es que desde Bruselas, se está preparando un "paquete" legislativo absolutamente abrumador que va a sobrecargar más, si cabe, a las organizaciones.

Véase por ejemplo, en materia de seguridad de las redes y sistemas de información, la segunda directiva (NIS2), la de resiliencia de las entidades críticas, normas que van a convivir con el Reglamento Dora, y con la futura ley de ciberresiliencia y cibersolidaridad, sin olvidarnos del Reglamento de inteligencia artificial o de los criptoactivos, entre otras muchas, sin duda alguna, esta campa obligacional que viene desde la Unión Europea, no hace más que reforzar el papel del compliance officer en las organizaciones, quien, de forma natural, absorberá parte de la función de control y supervisión del cumplimiento de esta normativa.

Sin duda alguna, las empresas deberán gestionar y medir cada día más los riesgos de ciberseguridad, porque la norma se lo va a exigir, de forma directa o indirecta, y, esto impactará en el análisis de riesgos de la sociedad, la regulación, exigirá en las grandes empresas una monitorización a tiempo real de las ciberamenazas, y se deberá acometer un abordaje de la gestión del riesgo con mecanismos tecnológicos, muchas empresas, ya están trabajando sobre la implementación de estas herramientas, estableciendo previamente medidas preventivas y reactivas frente a las amenazas.

Sin duda, la IA, tendrá también campo para poder ayudar a las organizaciones ante ataques de ciberseguridad, aprendiendo de ataques parecidos previos, aunque la IA, como todos sabemos, mal utilizada, podrá también comprometer los sistemas, veremos si es más beneficiosa o perjudicial para la seguridad de la información.

Sin duda, la toma de decisiones correctas de los cuerpos directivos, en cuanto a estrategia, inversión y concienciación en materia de ciberseguridad, minimizan los ataques y efectos, pero queda un largo camino, porque los □□□□□A no descansan, todo lo contrario, se perfeccionan con nuevas tecnologías y formas de acceso, y en número, son cada día más. Habrá, pues, que extremar las precauciones en las organizaciones, y secundar las normas comunitarias y nacionales, todo ello, auspiciado por un trabajo en equipo entre los departamentos de compliance y de seguridad de la información, o viceversa. No se trata de una guerra de poder interdepartamental por el control de un área crítica, sino de una guerra contra los hackers.

__Felipe García Hernández__, *abogado, socio de Círculo Legal, y miembro de la junta directiva de la World Compliance Association.*

Fuente

Link de la noticia