El fraude financiero online creció un 67% en los meses de confinamiento

El fraude financiero aumentó un 67% en todo el mundo durante los meses del confinamiento por el coronavirus, llegando a registrarse tres veces más siniestros por robos financieros que entre enero y marzo en el mercado europeo.

Es una de las principales conclusiones del estudio elaborado por la aseguradora Hiscox sobre los datos de su departamento de siniestros en los mercados estadounidense, europeo y británico, entre abril y junio de 2020.

Si bien contabilizó un descenso del número de siniestros, su estudio reconoce que se dispararon las frecuencias de los ataques, sobre todo, del tipo ransomware y en los pagos por fraude financiero. El ransomware es un programa de software que infecta el ordenador y bloquea contenidos exigiendo el pago de un rescate para restablecer el funcionamiento del sistema.

El fraude por desvío de dinero fue la principal táctica empleada por los ciberdelincuentes, y según Hiscox, en este aumento ha sido clave la implantación del teletrabajo dificultando, por ejemplo, el seguimiento de los procesos y procedimientos habituales para los pagos y aprobaciones de proveedores.

Ante este escenario, la directora de Legal y Siniestros de Hiscox, Mónica Calonje, aconseja a empresas y profesionales comprender la cobertura que tienen ante incidentes ciber y agregar una cobertura adicional contra delitos de esta naturaleza, así como que ejerzan un mayor control sobre la ciberseguridad de sus proveedores, y es que en muchas ocasiones el origen del incidente se produjo en terceras compañías.

El estudio revela que los ataques de ransomware afectaron, sobre todo, a las grandes organizaciones, quienes sufrieron más incidentes de esta tipología entre enero y junio de 2020 que durante todo el año 2019, y augura además que la cifra se duplique a finales de año.

La compañía avisa de que durante el confinamiento aparecieron además nuevas cepas de ransomware, siendo el que más incidentes ha provocado el bautizado como Dhama, junto con los más habituales Snatch, Maze, LockBit y Medusa.

El responsable de riesgos ciber de Hiscox, Alan Abreu, subraya que no se trata sólo de que una empresa sufra un ataque de ransomware o fraude financiero, es importante proteger las estructuras de la cadena de suministro y asegurarse de que los proveedores externos cumplen con los protocolos.

A título de ejemplo indica que solamente en el mes de abril, el 44% de los siniestros por ransomware en Estados Unidos tuvieron su origen en un proveedor del asegurado que sufrió el ataque, lo que terminó afectándole a él.

Fuente: Expansión