LITORALPRESS

Fecha: 03-07-2024
Medio: La Tercera
Supl. : La Tercera - Pulso
Tipo: Noticia general
Título: GTD contrademanda a empresa de Nicolás Luksic y la acusa de intentar "obtener un provecho ilegítimo" por ciberataque de 2023

Pág. : 8
Cm2: 740,8

Tiraje: 78.224
Lectoría: 253.149
Favorabilidad: No Definida

GTD contrademanda a empresa de Nicolás Luksic y la acusa de intentar "obtener un provecho ilegítimo" por ciberataque de 2023

La empresa de telecomunicaciones lanzó una fuerte arremetida en tribunales, presentando una contrademanda, tras sufrir un ciberataque de ransomware que paralizó sus servicios. GTD acusa a Ionix de incumplir sus obligaciones de pago y de actuar de mala fe.

LEONARDO CÁRDENAS

El 23 de octubre de 2023, GTD sufrió un ciberataque debido a un *ransomware* denominado "BabLock", que provocó la encriptación de información y la obligó a suspender temporalmente algunos servicios, incluyendo la plataforma "IaaS", para evitar la propagación.

A raíz del ataque, la empresa Ionix, propiedad del empresario Nicolás Luksic, interpuso una demanda de indemnización de perjuicios y solicitó la terminación del contrato con GTD, uno de los principales proveedores de internet en Chile y Perú.

Ante el 23° Juzgado Civil de Santiago, Ionix acusó a GTD de "incumplimiento y negligencia inexcusables" al "no haber podido evitar el ciberataque y no contar con un plan de contingencia para enfrentar la situación". Además, Ionix alegó que GTD no había logrado restablecer los servicios hasta la fecha y no había comunicado oportunamente el ataque.

El pasado 19 de junio, GTD contestó la acción en duros términos. En su escrito, la empresa fundada por el empresario José Manuel Casanueva interpuso una demanda reconvencional contra la *fintech*, insistiendo en que actuó con "la máxima diligencia frente a un evento de esta envergadura y que claramente constituye un caso fortuito o fuerza mayor".

La empresa de telecomunicaciones acusó a Ionix de no cooperar adecuadamente durante el proceso de recuperación del servicio IaaS después del ciberataque. Según GTD, Ionix no facilitó la reposición del servicio.

Además, la empresa denunció a Ionix por negarse a pagar por los servicios prestados una vez que el servicio IaaS fue restaurado. A pesar de que GTD logró recuperar la información y restablecer un ambiente seguro, Ionix decidió unilateralmente no cumplir con sus obligaciones de pago, lo cual GTD considera injustificado.

"Una vez recuperado dicho servicio, lisa y llanamente, Ionix se mantuvo en la negativa de pagar el precio del mismo a nuestra representada, sin explicación alguna." Esta negativa a pagar ha generado una disputa contractual adicional entre las partes.

GTD alegó que Ionix ha actuado de mala fe al intentar beneficiarse de la situación creada por el ciberataque. A su parecer, Ionix utilizó el incidente como excusa para terminar unilateralmente el contrato y evitar sus responsabilidades financieras.

"No es lícito que una parte, valiéndose de dicha situación, intente obtener un provecho ilegítimo a través de una acción que contiene una serie de afirmaciones que faltan manifiestamente a la verdad de lo ocurrido" consignó la demanda de GTD, patrocinada por Cristóbal Sarralde, *counsel* de Garrigues.

GTD también mencionó que, tras haber presentado la demanda de terminación de contrato, Ionix envió una carta declarando unilateralmente la terminación del contrato y negándose a pagar por los servicios a partir del 23 de octubre de 2023, lo cual GTD describe como "manifiestamente falso."

MEJORAS

Tras el ciberataque, GTD implementó una serie de mejoras en sus instalaciones para reforzar su seguridad y garantizar la continuidad de sus servicios. La empresa revisó y actualizó sus políticas de ciberseguridad, incorporando prácticas y estándares internacionales como ISO 27001 y NIST-CSF. Estas acciones incluyeron programas de capacitación en ciberseguridad para todos sus empleados.

"GTD contaba y sigue contando con las siguientes certificaciones ISO, a saber: ISO 27001: 2013 sobre Sistemas de Gestión de Seguridad de la Información", acotó.

Además, la compañía realizó una modernización de su infraestructura tecnológica, incluyendo la actualización de sus sistemas de detección y respuesta ante incidentes. La empresa instaló nuevos *firewalls* y herramientas de monitoreo de redes, capaces de identificar y mitigar amenazas en tiempo real. Se reforzaron los protocolos de respaldo de datos, asegurando que todas las copias de seguridad se realizaran automáticamente y se almacenaran en ubicaciones seguras fuera del sitio principal.

También estableció alianzas con empresas de ciberseguridad para realizar auditorías de sus sistemas y recibir asesoramiento sobre las últimas tendencias y tecnologías en seguridad informática. Estas colaboraciones le permitieron implementar "soluciones proactivas y adaptativas" para proteger sus plataformas y servicios contra futuras amenazas. Con estas medidas, mejoró su capacidad de respuesta ante ciberataques y "fortaleció su compromiso con la seguridad y la confianza de sus clientes".

El pasado viernes, Ionix presentó un escrito de réplica al tribunal en el que sostuvo que "el cúmulo de certificaciones y protocolos que esgrime GTD: un alto estándar de seguridad informática que contrasta con un actuar poco diligente".

"La vulnerabilidad que utilizó el *ransomware* que atacó los sistemas de GTD tenía una solución muy sencilla, la cual GTD tenía que adoptar preventivamente: actualizar los sistemas utilizados a una versión más nueva", añadió la compañía representada Tomás Pérez, socio de Bofill Mir Abogados.