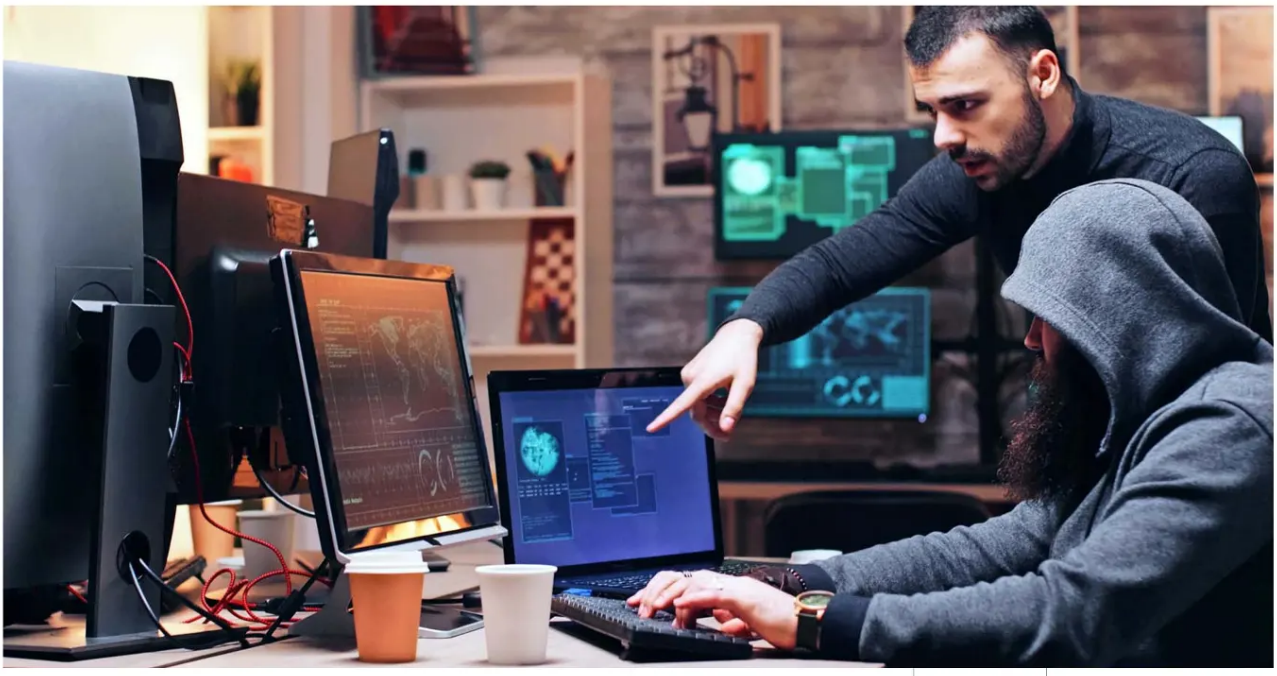
CHILETECNOLÓGICO
30/05/2025 Audiencia: 320.543 Sección: PORTADA
$11.904.291 Tirada: 126.654 Frecuencia: SEMANAL
$20.570.976 Difusión: 126.654
ada: $20.570.976 Ocupación: 57,87%

HACKERS QUE OFRECEN SUS SERVICIOS A CAMBIO DE NO VOLVERLAS A ATACAR

Consultoría criminal: La nueva técnica que amenaza la ciberseguridad de las empresas chilenas



Expertos aseguran que compañías medianas y pequeñas son las más expuestas a este nuevo tipo de ciberdelito, en parte, por la falta de cortafuegos en sus sistemas. Además, apuntan a que se debe contar con mejores lineamientos para definir el denominado "hackeo ético".

MAGDALENA ESPINOSA

Una nueva táctica criminal aterrizó en Chile en materia de ciberseguridad. Desde hace algunos meses, las empresas ya no solo se enfrentan al robo, secuestro y extorsión de información sensible, sino que las mafias virtuales sumaron otro plato al menú: el ofrecimiento de entregar informes técnicos para mejorar sus barreras de seguridad, después de amenazar a las compañías.

Parece insólito, pero es un fenómeno que comenzó hace unos años a nivel mundial y en Chile, aparecieron los primeros casos a fines de 2023. Hasta el momento, ninguno es público, porque recién a partir de este año las firmas están obligadas a reportar estos incidentes.

Herwin Cajamarca, gerente de Ingeniería de Negocios del *data center* IFX Chile, explica que lo "novedoso" es que los atacantes ofrecen consultorías posincidentes para "ayudar" a las empresas con información y consejos que les permitan evitar futuras infecciones.

"Hace un tiempo atrás escuché de un banco en Ecuador que sufrió un ataque de *ransomware* (secuestro de datos) y los mismos cibercriminales les ofrecieron que si se les contrataba como asesores, no volverían a ser atacados. En ese momento pareció un caso aislado, casi de estudio, pero hoy está siendo cada vez más común", comentó el ingeniero.

El modo de acción de los delincuentes digitales consiste en atacar las redes y solicitar un rescate mediante bitcóins. Luego, a los afectados se les da un número de *call center* para agendar la entrega del informe técnico, con el objetivo de "ayudar" mediante una consultoría.

OFERTA ALARMANTE

Jorge Atton, exsubsecretario de Telecomunicaciones y exasesor presidencial en ciberseguridad, conoce de cerca la técnica y la califica como "alarmante". "Los delincuentes ingresan a las redes y luego amenazan con atacar o filtrar información sensible si no contratan sus 'servicios de ciberseguridad'. Esta oferta a menudo se presenta como una consultoría o una evaluación de riesgos, pero en realidad es un intento de extorsión. Lo que realmente necesitan las empresas es un informe técnico de daños y una evaluación honesta de sus vulnerabilidades, cosa que no proporcionan este tipo de 'hackers éticos', sino que buscan asegurar un beneficio económico a través del miedo y la coacción".

Andrés Corón, gerente de ciberseguridad de Entelgy Chile, coincidió con Atton y aseguró que "esta estrategia no solo busca maximizar el beneficio económico, sino también reducir la exposición directa de los atacantes, delegando la ejecución a afiliados y ampliando su alcance global".

Los ataques a entidades como bancos o *retailers* hicieron que las grandes compañías nacionales tomaran rápidamente medidas para protegerse. Sin embargo, los delincuentes centraron su atención en los eslabones más débiles de la cadena: medianas y pequeñas empresas.

Luis Porta, director ejecutivo de Accenture Chile, advirtió que "en un ecosistema digital interconectado, las brechas en ciberseguridad en empresas de menor tamaño o menor madurez tecnológica pueden representar un punto de entrada para amenazas que afecten a todo el sistema. Además, la aceleración de nuevas tecnologías como la inteligencia artificial (IA), sin procesos adecuados de evaluación de riesgos, está generando nuevas vulnerabilidades".

FACTOR SORPRESA

Luis Porta explicó que de acuerdo a un informe del Foro Económico Mundial, el 42% de los encuestados en América Latina declaró que sus países no están preparados para enfrentar incidentes graves en infraestructura crítica.

El elemento sorpresa es la principal punta de lanza de estas organizaciones, pues no existe una estrategia única para perseguirlos. De hecho, el ejecutivo de IFX Chile explicó que nunca las empresas están 100% a salvo de estos incidentes, por lo que es crucial contar con un plan multicapas, dinámico y adaptativo.

Consultoras, empresas de tecnología y el mundo académico coinciden en que la estrategia de ciberseguridad nacional debe contar con una "visión sistémica".

El ejecutivo de Accenture puso énfasis en que no basta con proteger solo los *data centers*, sino que se debe contar con una estrategia que abarque desde la educación y conciencia de los clientes, incluya la cadena de proveedores, y arme gobernanza y planes de respuesta a incidentes. "Chile tiene talento y capacidades, pero debemos cerrar brechas, especialmente en sectores más expuestos y con menos recursos", agregó.

En materia de consultoría, el debate no está exento de acaloradas discusiones. Incluso, cuando se discutió la Ley Marco de Ciberseguridad, vigente desde este año, el denominado "hacker ético" fue un punto de divergencia entre los expertos.

Uno de sus defensores es Alejandro Hevia, director del Laboratorio de Criptografía Aplicada y Ciberseguridad de la Universidad de Chile, quien explicó que el hackeo ético es un proceso hecho por un profesional de la ciberseguridad, registrado, que avisa de las fallas mediante una notificación responsable. Y agregó: "Si una persona solicita un monto de dinero, después de vulnerar las barreras de seguridad de una empresa para dar a conocer el método de cómo lo logró, es extorsión, no hackeo ético".

Bajo su mirada, un *hacker* ético comparte las fallas apenas son encontradas y no exige recompensa a cambio, pero puede ser contratado posteriormente para un análisis. "La ley chilena da luces de cómo se hace este procedimiento", añadió.

42%
DE LOS ENCUESTADOS EN AMÉRICA LATINA por el Foro Económico Mundial declaró que sus países no están preparados para enfrentar incidentes graves en infraestructura crítica.

Un *hacker* ético comparte las fallas apenas son encontradas y no exige recompensa a cambio, pero puede ser contratado posteriormente para un análisis.

El elemento sorpresa es la principal punta de lanza de estas organizaciones, pues no existe una estrategia única para perseguirlas.

PUNTO CRÍTICO

Sin embargo, el mecanismo de cómo se entrega la información es un punto crítico. Juan Pablo González, director de datos personales y ciberseguridad en HD Group, explicó que "es importante avanzar en estándares y reglas claras. Eso no ha sido discutido con profundidad. En la práctica, el fenómeno que está ocurriendo es que se detectan vulnerabilidades en las empresas y se exigen beneficios económicos. Eso empaña la labor de aquellos investigadores de 'sombrero blanco' y se entra a un terreno gris".

A su parecer, "debemos definir los espacios donde los profesionales puedan detectar fallas, como hackatones o, incluso, abrir procesos en que las compañías definan antes las recompensas en caso de detectar fallas y promover la generación de incentivos", señaló.

Pese a que la ley está vigente, González apuntó a que todavía faltan lineamientos que detallen con mayor definición el marco de acción en esta materia. "Es un tema pendiente", remató.