ITQ latam

EL MERCURIO

A CAMBIO DE UN RESCATE

RANSOMWARE: CRECE LA AMENAZA DEL SECUESTRO DE DATOS

Descubre las reflexiones de Álvaro Melo, Jefe de Ciberseguridad de ITQ Latam, en la última nota de Inteligencia Digital de El Mercurio.

Los expertos recomiendan mantener copias de seguridad almacenadas en un lugar seguro.

GYPO PHOTO

A CAMBIO DE UN RESCATE

Ransomware: crece la amenaza del secuestro de datos

Los incidentes de ciberseguridad vienen creciendo exponencialmente en los últimos años. De hecho, según la Encuesta Nacional de Ciberseguridad (ENCI) realizada por el Centro de Estudios Tecnológicos de la Información de la Universidad Católica (CetiUC), estos crecieron en promedio un 31,6% durante el año pasado en Chile. Y dentro de ellos, especial protagonismo han tenido últimamente los ataques de ransomware , tanto a empresas como a organizaciones; incluso, se estima que este tipo de malware creció alrededor de un 200% en el primer semestre de 2023, comparado con igual lapso del año pasado.

¿Qué es el ransomware ? En simple, secuestro de datos. Son tipos de programas dañinos que restringen el acceso a determinadas partes o archivos del sistema operativo infectado y piden un rescate a cambio de quitar esa restricción.

Hoy, se han sofisticado a tal punto que existen grupos que desarrollan herramientas y servicios para venderlos a terceros, bajo el modelo "Ransomware-as-a-Service" (RaaS), "lo que ha permitido el ingreso de nuevos actores de amenaza menos especializados que contratan estos recursos para llevar sus propias campañas", explica Álvaro Melo, jefe de Ciberseguridad de ITQ Latam.

> Los cibercriminales se han sofisticado a tal punto que hoy venden estos programas malignos para que puedan ser utilizados por terceros.

A ello se agrega que, muchas veces, los rápidos procesos de digitalización de las compañías no consideran la ciberseguridad como base de su estrategia: "A medida que las empresas dependen cada vez más de las tecnologías digitales, están más expuestas a los ataques de ransomware, y si no consideraron ciberseguridad desde el inicio, están más vulnerables", advierte Rodrigo Hernández, gerente del Departamento de Ciberseguridad de Entel.

Otro factor importantísimo son las personas: "Siguen siendo el punto de entrada a las empresas, y la falta de concientización en ciberseguridad a todos los niveles genera una baja inversión y una alta probabilidad de tener éxito en ataques de ingeniería social, que permiten al atacante el acceso inicial a la empresa y ejecutar los ataques de ransomware gracias a la falta de controles de seguridad", agrega Hernández.

CONSTANTE EVOLUCIÓN

Las compañías deben estar siempre alertas, porque la ciberseguridad es un campo en constante evolución, y deben "seguir adaptándose y mejorando sus medidas para mantenerse al día con las nuevas amenazas", dice Melo. "El paradigma de seguridad cambió: antes, era proteger el perímetro para que los atacantes no entraran a mi organización; hoy, es que en cualquier momento vamos a ser atacados y debemos estar preparados para responder lo más rápido posible, para minimizar el impacto adverso en el negocio", añade Hernández.

Las medidas de prevención abarcan varios aspectos. "Primero, tener presente que los temas higiénicos nunca pasan de moda (contar con un inventario actualizado de la infraestructura tecnológica, gestión de vulnerabilidades y procedimientos de instalación de parches de seguridad, utilizar estándares de configuración segura para servidores, bases de datos y computadores), capacitar a la empresa en ataques de ingeniería social y medir el comportamiento de los usuarios para determinar si son capaces de detectar ciberataques y cómo reaccionan, preparar a la compañía para responder a una cibercrisis", detalla Hernández.

Asimismo, Melo destaca que se debe implementar una estrategia de ciberseguridad integral, que incluya "medidas de seguridad de hardware , software y procesos"; mantener los sistemas operativos y programas actualizados, y establecer políticas y procedimientos de seguridad, claros y concisos, comunicados a todo el personal.

Y en cuanto a los rescates, "la recomendación siempre es no pagar el rescate, dado que, primero, va contra la ley; son ciberdelincuentes, y no existe ninguna garantía de que cumplan su palabra pospago, y la empresa podría estar financiando al terrorismo en el caso de grupos patrocinados por Estados, entre muchos otros factores", explica Hernández, de Entel.

"En algunos casos, las empresas pueden ser capaces de recuperar sus datos sin pagar, mediante la restauración de las copias de seguridad o el proceso de descifrar los datos, utilizando herramientas de terceros. Por eso la importancia de contar con copias de seguridad lo más recientes posibles y almacenadas en un lugar seguro para evitar que el contenido de dichas copias se vea comprometido", agrega Melo, de ITQ.