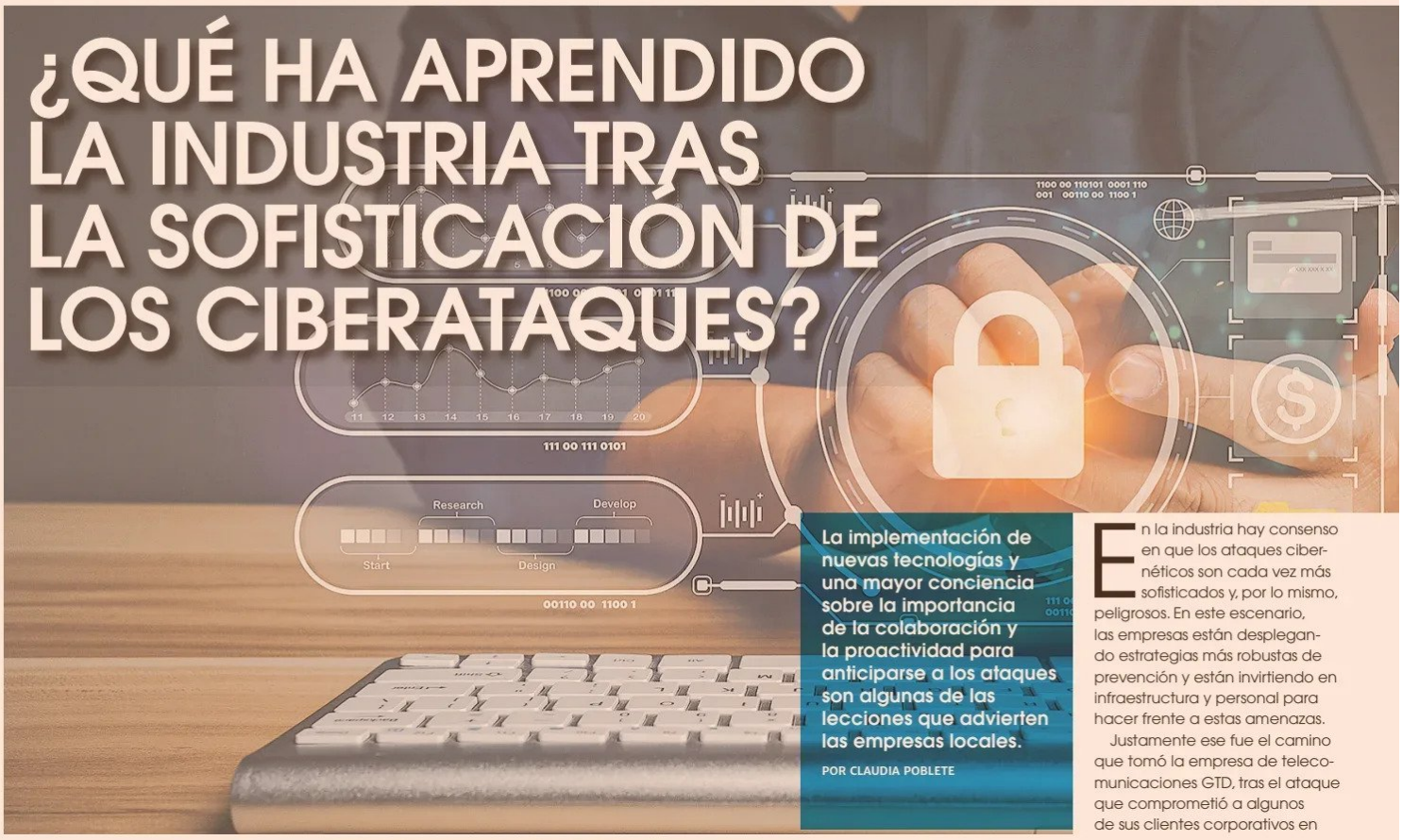
Diario Financiero

Fecha: 01/10/2024 Audiencia: 48.450 Sección: ECONOMIA
Vpe: $2.877.527 Tirada: 16.150 Frecuencia: DIARIO
Vpe pág: $7.443.240 Difusión: 16.150
Vpe portada: $7.443.240 Ocupación: 38,66%

¿QUÉ HA APRENDIDO LA INDUSTRIA TRAS LA SOFISTICACIÓN DE LOS CIBERATAQUES?



La implementación de nuevas tecnologías y una mayor conciencia sobre la importancia de la colaboración y la proactividad para anticiparse a los ataques son algunas de las lecciones que advierten las empresas locales.

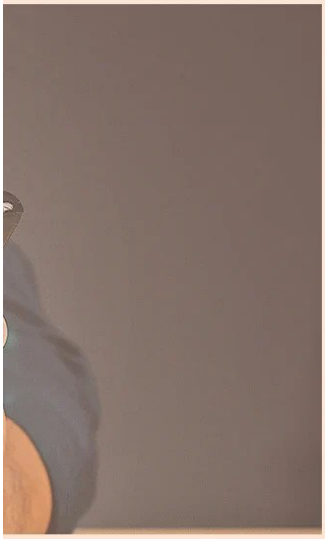
POR CLAUDIA POBLETE

En la industria hay consenso en que los ataques cibernéticos son cada vez más sofisticados y, por lo mismo, peligrosos. En este escenario, las empresas están desplegando estrategias más robustas de prevención y están invirtiendo en infraestructura y personal para hacer frente a estas amenazas.

Justamente ese fue el camino que tomó la empresa de telecomunicaciones GTD, tras el ataque que comprometió a algunos de sus clientes corporativos en

Diario Financiero

Fecha: 01/10/2024 Audiencia: 48.450 Sección: ECONOMIA
Vpe: $2.943.061 Tirada: 16.150 Frecuencia: DIARIO
Vpe pág: $7.443.240 Difusión: 16.150
Vpe portada: $7.443.240 Ocupación: 39,54%



octubre del año pasado, quienes vieron afectados sus servicios por el secuestro de datos provocado por un malware tipo ransomware. Casi un año ha pasado, y desde ese momento, la compañía se ha propuesto robustecer sus sistemas de seguridad, según cuentan, además de generar conciencia sobre los riesgos y compartir su experiencia con la industria: "Aprendimos que es crucial aunar esfuerzos y trabajar colaborativamente para hacer frente a un enemigo común: los ciberdelincuentes", aseguran fuentes de la firma. Una acción concreta, detallan, vino con lo aprendido a raíz de la constante comunicación que tuvieron con sus clientes en ese complejo momento: crearon una unidad de respuesta ante este tipo de incidentes para operar en toda Latinoamérica, y así mejorar su capacidad de responder si algo así vuelve a ocurrir. "Estamos trabajando para ofrecer arquitecturas acordes a la realidad de cada empresa", aseguran.

Datos de FortiGuard Labs indican que en América Latina y el Caribe se produjeron 200 mil millones de intentos de ataque en 2023, mientras que el Reporte de Ciberseguridad 2024 de Entel Digital da cuenta de que Chile registró en 2023 tres veces más vulneraciones que el año anterior.

Y no solo se producen más ataques, sino que las formas y estrategias de perpetrarlos también evolucionan. Marcelo Castiglione, vicepresidente de la Asociación Chilena de Empresas de Tecnología de Información (ACTI), considera que este fenómeno es consecuencia de un mayor nivel de preparación de parte de las empresas.

"La utilización de nuevas tecnologías, ya con componentes de inteligencia artificial, para defender los activos tecnológicos junto con una mayor conciencia de la relevancia de tomar mayores resguardos para proteger la información y la continuidad de las operaciones obliga al cibercrimen a un mayor nivel de sofisticación y volumetría de sus ataques", comenta Castiglione, aunque aclara que esta mayor preparación empresarial, lamentablemente, no es un proceso homogéneo, ya que "tradicionalmente los sectores regulados o los que son foco del cibercrimen desarrollan una mayor preparación más temprano que el resto", indica.

11,7%

DE LAS EMPRESAS EN CHILE CALIFICAN LA CIBERSEGURIDAD COMO EL SEGUNDO RIESGO MÁS CRÍTICO PARA SUS OPERACIONES, SEGÚN EL ESTUDIO PERCEPCIÓN DE RIESGOS EMPRESARIALES 2024.

Más que sobrevivir a amenazas

Aún así, hay avances y lecciones. Luis Porta, director ejecutivo de Accenture Chile, explica que desde la implementación de la Ley Marco de Ciberseguridad en abril de 2024, que establece un marco robusto para proteger la información y la infraestructura crítica, el país ha escalado al puesto 25 en el Índice Nacional de Seguridad Cibernética, posicionándose como el segundo más seguro de la región.

"Las compañías, especialmente las del sector financiero, tienen la oportunidad de reevaluar y reforzar sus sistemas de seguridad para los siguientes años, viendo la ciberseguridad como una inversión estratégica que no solo protege, sino que también potencia su crecimiento y adaptación en un entorno digital en constante evolución. Con un enfoque proactivo y colaborativo, las organizaciones no solo pueden sobrevivir a las amenazas cibernéticas, sino prosperar en un mundo digital cada vez más complejo", expresa.

Karin Quiroga, directora nacional de Escuelas AIEP y experta en ciberseguridad, pone en relieve algunos de los principales avances de las empresas en la materia, entre los que destaca la habilitación de centros de operaciones de seguridad, sistemas de detección y respuesta ante amenazas, sistemas de IA y aprendizaje automático, para analizar grandes volúmenes de datos y detectar patrones que permitan identificar posibles ataques; y la implementación de programas de capacitación a colaboradores.

"La preparación de los profesionales responde a una combinación de distintos mecanismos, tales como educación formal, capacitación, certificaciones específicas y experiencia práctica-laboral para fortalecer sus competencias en esta materia", aclara Quiroga, quien también es cofundadora de la Alianza Chilena de Ciberseguridad. Agrega que ante la evolución de los ataques y el contexto actual corporativo, los profesionales requieren un conjunto de habilidades técnicas y blandas que les permitan no solo gestionar y prevenir ataques de ciberseguridad, sino también liderar equipos y comunicarse efectivamente con otros departamentos y con la alta dirección.