Así se roban los datos hoy: cómo ingresan los atacantes y qué consecuencias tiene

01/07/2025

Las amenazas digitales actuales ya no hacen ruido cuando entran. En muchos casos se infiltran en silencio, aprovechando una distracción, una falla técnica o un error humano. Lejos de ser incidentes aislados, los robos de datos son parte de campañas cuidadosamente planificadas, lideradas por actores maliciosos que conocen a fondo las vulnerabilidades de las organizaciones. La seguridad hoy no depende solo de lo que hace una empresa internamente, sino también de sus políticas de acceso, los parches que omite y los comportamientos que normaliza.

Uno de los vectores de ataque más comunes sigue siendo el email. Técnicas como phishing o spear-phishing son el origen del 91% de las brechas, según el Data Breach Investigations Report de Verizon. Enlaces fraudulentos, archivos adjuntos con scripts o malware oculto permiten a los atacantes ingresar a redes corporativas con eficacia.

Otra vía crítica son las vulnerabilidades sin parchear. En Argentina, el 68% de las PyMEs admite no tener una política de actualización de sistemas completa, según ISACA. Solo en 2023, más del 35% de los accesos no autorizados en América Latina se

originaron en software de acceso remoto como RDP o VPN, según Cisco.

La cadena de suministro (proveedores, socios o terceros con los que se comparten accesos y operaciones) también implica un riesgo alto. En abril de 2023, un proveedor regional de TI en Uruguay fue atacado mediante un exploit. Se robaron credenciales y se comprometieron tres entidades bancarias en Uruguay y Paraguay, con pérdidas por más de 800.000 dólares.

El factor humano no se queda atrás. El 22% de los incidentes en empresas de entre 250 y 1.200 empleados involucró a un colaborador, de acuerdo con Cybersecurity Insiders. Ya sea por negligencia o acción voluntaria, las configuraciones débiles y la falta de control interno amplifican el riesgo.

En entornos en la nube, los errores de configuración también generan consecuencias graves. Bases de datos en AWS, Azure o Google Cloud pueden quedar expuestas si los buckets de almacenamiento no se configuran adecuadamente. En 2023, una de cada cuatro empresas del sector salud en Uruguay reportó incidentes vinculados a esta causa, según Forbes LatAm.

Los casos recientes dan cuenta de estas fallas. En junio de 2023, el Hospital de Clínicas de Montevideo fue víctima de ransomware: más de 200.000 historiales clínicos cifrados, un pedido de rescate de 100.000 dólares y un costo total de recuperación que superó los 350.000. Aunque tenía firewalls y antimalware, la falta de monitoreo y de un plan de respuesta lo dejó vulnerable.

En noviembre de 2022, Sancor Seguros en Argentina sufrió la filtración de datos de más de 300.000 clientes tras una campaña de spear-phishing. Un archivo malicioso descargado por un empleado dio acceso persistente a la red. Se filtraron datos personales, pólizas e información financiera. La empresa tuvo que activar un plan de contingencia y notificó a las autoridades.

En marzo de 2024, DKV Seguros en España confirmó un ataque de ransomware que afectó a 120.000 clientes. La brecha, iniciada por un servidor VPN sin parches, permitió acceder a historiales médicos. Las pérdidas superaron los 2 millones de euros.

Estos episodios muestran que el robo de datos no distingue sector ni país. **Lo que se repite es una falsa sensación de seguridad basada en controles básicos o soluciones aisladas. Sin una gestión profesional y sostenida, el riesgo no solo persiste: escala.**

Las consecuencias de una brecha exceden la pérdida de datos. Según Gartner, el 78% de las organizaciones atacadas enfrenta interrupciones críticas de más de 48 horas. Para una empresa mediana, eso puede representar pérdidas de hasta 100.000 dólares diarios. A esto se suma el daño reputacional: el 56% de los clientes abandona un servicio tras una filtración. En salud, la pérdida de confianza llega al 70%, según estudios de PwC y Accenture.

Desde el plano legal, las sanciones también pesan. En España, el incumplimiento del RGPD puede implicar multas de hasta el 4% de la facturación anual. En Uruguay, la Ley 19.529 contempla sanciones de hasta 100.000 dólares. En Argentina, la Ley 25.326 exige notificar filtraciones sensibles en menos de 24 horas.

El costo promedio de contención de un incidente es de 1,2 millones de dólares, según el Cost of a Data Breach Report de IBM. A ello se suman campañas de comunicación, asistencia legal y, en algunos casos, demandas colectivas. Más preocupante aún: el 43% de las medianas empresas que sufrieron un ciberataque no lograron recuperarse financieramente en el primer año, y un 13% cierra definitivamente, según IDC y el Ponemon Institute.

La única salida sostenible es adoptar un enfoque integral de

ciberseguridad. Esto implica gestionar todo el ciclo de protección: identificación de activos, análisis de riesgos, tecnologías de defensa (firewalls, EDR, MFA, SIEM) y planes de respuesta post-incidente. No basta con sumar herramientas: se trata de integrar capacidades, procesos y cultura organizacional.

El riesgo no desaparece, pero puede ser gestionado con estrategia y conocimiento. La resiliencia nace de la visibilidad y la preparación. Y la ciberseguridad ya no es una cuestión exclusiva del área de IT: es un pilar esencial para la continuidad de cualquier negocio.

Fuente: Ámbito Financiero