Comunicados

El costo promedio de una filtración de datos en Latinoamérica alcanzó USD 2,46 millones en 2023

- En la región, las organizaciones con un uso extensivo de seguridad impulsada por inteligencia artificial y automatización pudieron reducir los costos de las filtraciones de datos en USD 1,04 millones y los ciclos de vida de las filtraciones en 94 días.

- IBM Consulting abre un nuevo Centro de Operaciones de Seguridad en Brasil, ampliando su capacidad para proporcionar servicios de inteligencia en ciberseguridad impulsados por IA y Automatización en América Latina.

Buenos Aires, 23 de Agosto, 2023 -- IBM (NYSE: IBM) Security publicó su reporte anual Cost of a Data Breach[1], mostrando que el costo de una filtración de datos en Latinoamérica alcanzó los USD 2,46 millones en 2023, un máximo histórico en el reporte y un aumento del 76 % desde 2020. Los costos de detección y escalamiento se duplicaron durante este mismo período de tiempo, representando la porción más alta de los costos en las filtraciones e indicando un cambio hacia investigaciones más complejas. Considerando el creciente impacto financiero de las filtraciones de datos, hoy IBM Consulting anunció la apertura oficial de un nuevo Centro de Operaciones de Seguridad (SOC) en la ciudad de São Paulo, Brasil, que brindará servicios de seguridad en toda América Latina.

De acuerdo con el reporte de IBM en 2023, en América Latina, los ataques de infiltrados malintesionados (*malicious insider*) fueron los más costosos por USD 2,59 milliones, seguido de ataques con credenciales robadas y comprometidas por USD 2,56 millones y en tercer lugar, por la pérdida accidental o robo de datos o dispositivos, por aproximadamente USD 2,53 millones. Los vectores de ataque iniciales más comunes en la región fueron el robo o compromiso de credenciales y el phishing, que representan el 16 % de las infracciones estudiadas. Desde la perspectiva de la industria, Finanzas (USD 2,99 millones), Industrial (USD 2,82 millones) y Servicios (USD 2,78 millones) fueron los sectores con los costos promedio de filtraciones de datos más altos en la región.

El reporte Cost of a Data Breach 2023, analizado por IBM Security y conducido por el Ponemon Institute, se basa en un análisis a profundidad de filtraciones de datos reales experimentadas por organizaciones a nivel mundial entre marzo de 2022 a 2023. Algunos hallazgos adicionales en Latinoamérica incluyen:

- **La IA y la automatización aumentan la velocidad.** La IA y la automatización tuvieron el mayor impacto en la velocidad de identificación y contención de las filtraciones para las organizaciones estudiadas. En América Latina, las

organizaciones con un uso extensivo de IA y automatización experimentaron un ciclo de vida 94 días más corto en las filtraciones datos que las organizaciones que no implementaron estas tecnologías, y vieron, en promedio, USD 1,04 millones menos en costos de filtración de datos. Sin embargo, solo el 23 % de las empresas estudiadas en América Latina utilizan ampliamente seguridad impulsada por inteligencia artificial y automatización, representando un 17 % menos que el promedio mundial.

- **Los atacantes están filtrando datos a través de los entornos.** En Latinoamérica, 43 % de las filtraciones de datos estudiadas resultaron en la pérdida de datos en múltiples tipos de entornos (como nube pública, nube privada, infraestructura local), indicando que los atacantes pudieron comprometer múltiples entornos y evitar la detección. Cuando los datos filtrados se almacenaron en múltiples entornos, también tuvieron los costos asociados más altos (USD 2,55 millones) y tardaron más en identificarse y contenerse (339 días).
- **Las filtraciones más largas cuestan más.** El tiempo necesario para identificar y contener una filtración de datos afecta el costo total de la filtración. Según el reporte, en América Latina, si una empresa tarda menos de 200 días en identificar y contener el incidente, el costo promedio de la filtración es de USD 2,13 millones, pero si pasa los 200 días, el costo sube a USD 2,79 millones.

IBM Inaugura Nuevo Centro de Operaciones de Seguridad en América Latina

Con los costos de las filtraciones de datos aumentando en la región, hoy IBM Consulting anunció la apertura oficial de su segundo Centro de Operaciones de Seguridad (SOC) en Brasil. Este nuevo SOC aprovechará las capacidades de gestión de amenazas globales de IBM para proporcionar servicios proactivos de detección de amenazas las 24 horas del día, los 7 días de la semana. El modelo SOC de IBM aprovecha la inteligencia artificial, el aprendizaje automático y la automatización para ayudar a los clientes a identificar y contener las infracciones de manera más rápida y eficiente.

"Al enfrentarse a los crecientes costos de detección, particularmente para filtraciones prolongadas, el énfasis en la velocidad y la eficiencia en los programas de gestión de amenazas nunca ha sido más crítico", dijo Nicolas Mucci, Líder de IBM Security Services en Latinoamérica. "Este nuevo SOC ofrece IA, automatización, y servicios de gestión de amenazas basados en datos para ayudar a las empresas de en la región a responder rápida y estratégicamente a las ciberamenazas”.

El nuevo SOC es parte de la vasta red global de IBM, que atiende a más de 3000 clientes en todo el mundo, administrando más de 2 millones de *endpoints* y 180 mil millones de eventos de seguridad potenciales por día. La red global de IBM ahora incluye SOCs en 16 ubicaciones, como Atlanta (USA), Australia, Costa Rica, Japón, Polonia, Arabia Saudita y más. Ofrece expertos en investigación de Servicios de Seguridad Gestionados (MSS) para asistir en la respuesta en el lugar, expertos en seguridad dedicados con una sólida experiencia vertical, servicios de asesoramiento personalizados combinados con un enfoque holístico para proteger los entornos de nube híbrida.

Sobre IBM Security

IBM Security ayuda a proteger a las empresas y los gobiernos más grandes del mundo con un portafolio integrado de productos y servicios de seguridad, impulsados con capacidades de IA dinámica y recursos de automatización. El portafolio, respaldado por la investigación de renombre mundial de IBM Security X-Force®, permite a las organizaciones prever las amenazas, proteger los datos a medida que se mueven, y responder con rapidez y precisión sin frenar la innovación empresarial. Miles de organizaciones confían en IBM como su socio para evaluar, diseñar estrategias, implementar y gestionar transformaciones de seguridad. IBM opera una de las organizaciones de investigación, desarrollo y entrega de seguridad más amplias del mundo, monitorea más de 180 mil millones de eventos de seguridad por día en más de 130 países y ha recibido más de 10.000 patentes de seguridad en todo el mundo.

[1] This report considers Argentina, Brazil, Chile, Colombia, and Mexico as Latin America.