PERIÓDICO	PÁGINA	FECHA	SECCIÓN
EXCELSIOR	10	15/12/2023	OPINIÓN

Jorge Camargo Zurita
Consultor de comunicación política
X: @jorgecamargoz
jorgecamargozurita@gmail.com

El gran pendiente de la ciberseguridad

Si bien es un avance la creación de la Comisión Intersecretarial de Tecnologías de la Información y Comunicación, y de la Seguridad de la Información a inicios de este año, no deja de llamar la atención su conformación...

En tanto legisladores y gobierno dan vueltas sobre el mismo error cometido en otros países de crear una legislación federal de ciberseguridad desde una perspectiva de seguridad nacional, descansada en las Fuerzas Armadas, con el riesgo de afectar derechos humanos y dejar fuera a compañías y ciudadanos, nuestro país se encuentra entre los cuatro que registra constantes ataques en América Latina.

Si bien es un avance la creación de la Comisión Intersecretarial de Tecnologías de la Información y Comunicación, y de la Seguridad de la Información a inicios de este año, no deja de llamar la atención su conformación, porque da carácter de invitados a representantes de la academia, investigadores y de la iniciativa privada, amén de otros órganos constitucionalmente autónomos.

Realmente no dimensionamos los miles de millones de dólares que cuesta a las compañías, a nivel global, los ataques ransomware o DoS (denial of service attack), como ya tratamos en otra entrega. De acuerdo con un reporte de la compañía global IBM, el costo promedio de una filtración de datos en Latinoamérica es de alrededor de 2.46 millones de dólares (mdd), tan sólo en este año.

En su reporte subraya que se trata de un máximo histórico e implica un aumento del 76% desde 2020, lo que dobla el costo de detección y escalamiento. No es sólo en México. La compañía Kaspersky explica que se produjeron casi 1.2 millones de ataques de malware. Y en América Latina ocurrieron 3.2 millones de ataques diarios.

El costo promedio de una filtración de datos en Latinoamérica es de alrededor de 2.46 mdd.

Brasil lleva la delantera con 1,515 ataques por minuto; México, 275; Colombia, 117; Perú, 107; Argentina, 33 y Chile, 27.

IBM subraya que los ataques de "infiltrados malintencionados" fueron los más costosos con 2.59 mdd, seguido de ataques con credenciales robadas y comprometidas, con 2.56 mdd y, en tercer lugar, por la pérdida accidental o robo de datos o dispositivos, con 2.53 mdd. Los ataques más comunes fueron el robo o compromiso de credenciales y el phishing, que representan el 16% de las infracciones estudiadas. Las ramas más afectadas fueron finanzas, con 2.99 mdd; industrial, con 2.82 mdd, y servicios, con 2.78 mdd.

En el caso de IBM, por ejemplo, ha anunciado la apertura de un nuevo Centro de Operaciones de Seguridad en São Paulo, Brasil, que brindará servicios de seguridad con inteligencia artificial a toda América Latina.

Según el Cost of a Data Breach 2023, la IA y la automatización tuvieron el mayor impacto en la rapidez para contener las filtraciones. Se contabilizaron 94 días, menos filtraciones de datos que en organizaciones que no las implementaron.

Empero, sólo el 23% de las empresas estudiadas utilizan ampliamente seguridad impulsada por IA y automatización, representando un 17% menos que el promedio mundial.

Además, se detectó que los atacantes están filtrando datos en un 43% a través de entornos como las nubes públicas y privadas, así como infraestructura local. Cuando los datos filtrados se almacenaron en múltiples entornos, también tuvieron los costos asociados más altos: 2.55 mdd y el tiempo que se tardó en identificarse y contenerse es de 339 días.

Otro hallazgo importante es que las filtraciones más prolongadas tienen mayor costo. Según el reporte, si una empresa tarda menos de 200 días en identificar y contener el incidente, el costo promedio de la filtración es de 2.13 mdd, pero si pasa de los 200 días, el costo sube a 2.79 mdd.

"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.