infoblox

ESTUDIO DE 2023 SOBRE EL ESTADO GLOBAL DE LA CIBERSEGURIDAD

MÉXICO

CRA | Business Intelligence
A CyberRisk Alliance Resource

METODOLOGÍA

Los datos y perspectivas de este informe de la CyberRisk Alliance se basan en una encuesta global online realizada en julio/agosto de 2022 a responsables de la toma de decisiones y personas influyentes en materia de TI y ciberseguridad de 13 países, incluidas 100 organizaciones mexicanas de todos los tamaños. Entre los encuestados mexicanos había desde directores ejecutivos y directores hasta analistas y consultores. Trabajaban en diversos sectores, la mayoría en la tecnología (40 %), el comercio minorista (18 %), los servicios comerciales y profesionales (11 %) y los servicios financieros (10 %).

RESUMEN EJECUTIVO

Durante años, México y Brasil se han disputado el primer puesto de la cuestionable distinción de ser el país latinoamericano que más ataques cibernéticos recibe. Según la agencia de noticias Reuters, y numerosos estudios, México ocupa el primer puesto de la lista. Aquellos que tienen la tarea de proteger las redes mexicanas deben prestar mucha atención a la creciente tendencia del ransomware y las amenazas avanzadas dirigidas a penetrar las protecciones de la red. De acuerdo con los resultados de la encuesta de inteligencia de negocios elaborada por la CRA, se encontró que los responsables de la toma de decisiones sobre seguridad cibernética todavía están intentando trabajar en una nación que es blanco de grandes ataques.

“Todos los días nos enteramos de nuevas formas en las que se roban los datos”, señaló un encuestado mexicano que siente preocupación por los ataques directos a través de los servicios en la nube.

Las organizaciones mexicanas todavía le temen mucho al ransomware; la exfiltración de datos es una de las principales preocupaciones, ya que suele ser el resultado de una falla de seguridad en los últimos 12 meses. “Una de las principales preocupaciones es el robo o destrucción de información o la cancelación de funciones del sistema, así como el robo de identidad”, afirmó un encuestado mexicano que labora en el sector educativo.

Más de 7 de 10 personas encuestadas respondieron que sufrieron uno o más ataques en los últimos 12 meses, con más frecuencia por phishing o ransomware. En la mayoría de los casos, los resultados implicaban la manipulación o el bloqueo de datos, así como la exposición de datos confidenciales y/o la interrupción o el tiempo de inactividad del sistema. En un caso, el daño causó lesiones corporales o psicológicas, incluso pérdida de la vida.

Sin embargo, la mayoría de los encuestados (79 %) dijo que preveía un aumento de los presupuestos para la seguridad cibernética en 2023 porque espera ser blanco de amenazas sofisticadas contra sus redes y bases de datos.

Los resultados del estudio de 2022 entre los encuestados mexicanos revelan las siguientes tendencias:

65 %

de las organizaciones mexicanas aceleró las transformaciones digitales para apoyar a los trabajadores en remoto

1. **Desde que comenzó la pandemia de COVID-19, muchas organizaciones mexicanas aceleraron las transformaciones digitales para apoyar a los trabajadores remotos, e incrementaron los recursos de red y base de datos, así como el soporte a los portales de clientes para proporcionar asistencia a sus empleados.** Casi dos tercios (65 %) de todos los encuestados aceleraron las transformaciones digitales para apoyar a los trabajadores remotos, y el 58 % agregó recursos a redes y bases de datos. Casi la misma cantidad (57 %) aumentó el soporte de los portales de los clientes para la interacción remota con los clientes. Otro 40 % se centró en los controles de red y seguridad en la computación perimetral (como el SASE, Secure Access Service Edge); el 34 % contrató a más personal de TI y el 29 % trasladó más aplicaciones a proveedores de nube de terceros. Además, el 13 % cerró oficinas físicas; el 11 % reasignó al personal de TI a otros puestos; el 10 % disminuyó su dependencia de proveedores de nube de terceros; y el 6 % redujo al personal de TI.

México: número promedio de incidencias en varios vectores de ataque

65 %

de los encuestados informaron que su organización agregó VPN o firewalls y servidores DDI administrados en la nube (DNS-DHCP-IPAM), que los agregó el 50 %

2. **En el último año, una gran parte de las organizaciones mexicanas agregó dispositivos móviles remotos de propiedad corporativa, VPN, cortafuegos y servidores DDI gestionados en la nube para proteger sus redes y, al mismo tiempo, gestionar la proliferación y los riesgos de seguridad asociados de más dispositivos remotos en la red.** Casi dos tercios (65 %) de los encuestados informaron que su organización agregó dispositivos móviles remotos propiedad de la empresa, así como VPN o firewalls (58 %) y servidores DDI (DNS-DHCP-IPAM) administrados en la nube, que un 50 % agregó (en comparación con un 41 % que agregó servidores DDI administrados internamente). Además, el 44 % agregó dispositivos remotos propiedad de los empleados y quioscos inteligentes o dispositivos similares para prestar asistencia a clientes remotos (25 %).

3. **Muchos encuestados mexicanos dijeron que su organización estará más preocupada por la fuga de datos y el ransomware, así como por los ataques en la nube en los siguientes 12 meses.** La fuga de datos y el ransomware fueron los ataques más preocupantes para el 51 % de las organizaciones mexicanas, seguidos por los ataques directos a través de servicios en la nube (43 %) y los ataques a través de conexiones de trabajadores remotos (35 %). Otras preocupaciones importantes incluyeron amenazas persistentes avanzadas (APT) (27 %), ataques a través de IoT en red (21 %), amenazas internas (18 %), ataques a la cadena de suministro o de terceros (10 %) y ataques patrocinados por un estado (3 %).

4. **Los encuestados mexicanos dijeron que consideraban que su organización estaba menos preparada contra el ransomware, ataques a través de conexiones remotas de trabajadores y fugas de datos.** Los encuestados dijeron que se sentían menos preparados para defender las redes de su organización contra el ransomware (21 %), ataques a través de conexiones de trabajadores remotos (20 %), fuga de datos (18 %) y ataques directos a través de servicios en la nube (14 %). El 11 % mencionó las amenazas persistentes avanzadas (APT), seguidas de las amenazas internas (8 %), ataques patrocinados por un estado (4 %) y ataques a través de IoT en red (3 %). Al parecer, muchos no confían en la capacidad de su organización para hacer frente a las amenazas más recientes. “Los hackers están identificando nuevos métodos para robar información, y no sé si estamos preparados adecuadamente en cuanto a seguridad”, señaló un encuestado.

5. **En promedio, las organizaciones mexicanas detectaron más problemas derivados de ataques de correo electrónico/phishing que de cualquier otro tipo, incluidos los ataques a la red, a aplicaciones, a dispositivos/puntos finales, a la nube, a terceros/cadena de suministro y ransomware.** Los encuestados estimaron que su organización detectó problemas como resultado de aproximadamente 17 ataques de correo electrónico/phishing en los últimos 12 meses, así como 10 ataques a la red, 8 ataques a la nube y 7 ataques de ransomware, aplicaciones, dispositivos/punto de conexión y terceros/cadena de suministro, cada uno, en el mismo periodo.

7 de cada 10

encuestados mexicanos informaron de una o más violaciones en su organización por ciberataques

6. **Casi tres cuartas partes (71 %) de los encuestados mexicanos informaron de una o más violaciones en su organización por ciberataques, la mayoría provenientes de un punto de conexión propiedad de los empleados, la nube, puntos de acceso wifi o fuentes internas.** Una fuerza laboral remota continúa planteando problemas para el 42 % de las organizaciones de los encuestados, cuyas violaciones en los últimos 12 meses se originaron en puntos de conexión remotos propiedad de empleados (frente al 27 % para dispositivos remotos propiedad del empleador) y al 41 % de aplicaciones o infraestructura en la nube. Las violaciones también se originaron en los puntos de acceso wifi (34 %), las fuentes internas, como empleados o contratistas, (32 %), dispositivos o redes de IoT (28 %) y DNS, DHCP, IPAM u otros servidores de red (21 %). El 20 % vinculó sus violaciones a otros ataques basados en aplicaciones o a un proveedor de terceros/cadena de suministro, mientras que el 13 % mencionó el Protocolo de escritorio remoto (RDP) de Microsoft u otros programas de acceso remoto.

7. **El phishing fue el método de ataque más común contra las organizaciones que sufrieron violaciones.** Representó el 59 % de los métodos de ataque en el último año, seguidos de ransomware (54 %) y las amenazas persistentes avanzadas (APT) (46 %). Los objetivos de estos ataques que se informaron incluyeron exfiltración de datos (69 %), secuestro de credenciales (59 %), escalada de privilegios (28 %) y comunicaciones de mando y control (27 %) contra la organización.

$2.6 mil

el valor promedio estimado de las pérdidas organizacionales mexicanas

8. **En conjunto, el valor promedio estimado de las pérdidas organizativas mexicanas (incluidas las pérdidas financieras directas e indirectas, así como el daño a la reputación y los gastos de reparación) derivadas de las violaciones del año pasado era de aproximadamente 2.6 millones de dólares.** Las organizaciones que fueron víctimas de dichas violaciones experimentaron principalmente manipulación de datos (63 %), bloqueos de datos debido a ransomware (51 %), exposición o exfiltración de datos confidenciales, (44 %) o interrupciones del sistema o tiempo de inactividad (42 %). Un encuestado mencionó que la violación había provocado lesiones corporales y daño psicológico, y otro, dijo que la muerte.

9. **Las organizaciones mexicanas utilizaron diversos controles para proteger sus activos en red en entornos locales, basados en la nube e híbridos (locales y basados en la nube).** Entre los diversos controles utilizados, los más frecuentes son la seguridad DNS (31 %) para entornos locales; los corredores de seguridad de acceso a la nube (37 %) para entornos basados en la nube; y el cifrado de datos, la prevención de pérdida de datos y las herramientas de seguridad de red (firewalls e IPS, etc.), cada uno utilizado por el 50 % de las organizaciones para proteger entornos híbridos.

> “Los ataques de ransomware y phishing nos han costado mucho, y creo que seguirán afectándonos”.
>
> Director de seguridad cibernética de empresa minorista mexicana

79 %

de las organizaciones tardan hasta 24 horas en investigar una amenaza

10. **En promedio, la mayoría de las organizaciones (79 %) tarda hasta 24 horas en investigar una amenaza, y muchas dependen de búsquedas y respuestas de DNS e información de vulnerabilidad específica del sistema.** Para ayudar a sus investigaciones o búsquedas de amenazas, los equipos de seguridad se basan principalmente en búsquedas y respuestas de DNS (48 %), información de vulnerabilidad (47 %), datos de flujo de red (43 %), plataformas o servicios de inteligencia de amenazas de terceros (41 %) o alertas CERT (37 %).

11. **El Domain Name System (DNS) proporciona varias medidas de seguridad para proteger a las organizaciones y es un componente clave en prácticamente todas las estrategias de seguridad de las organizaciones.** Muchos de los encuestados (59 %) indicaron que su organización suele utilizar DNS en su estrategia para ayudar con lo siguiente: bloquear solicitudes de destinos maliciosos conocidos para reducir la carga de las defensas perimetrales; informarles de dispositivos que realizan solicitudes para conectarse a destinos maliciosos; y proporcionar protecciones específicas asociadas con la exfiltración de datos/túneles DNS, algoritmos generados por dominios, dominios similares y otras cosas que las herramientas de seguridad pueden pasar por alto. Otro 36 % dijo que utiliza DNS para ayudar a detectar malware antes en la cadena de eliminación.

12. **Los principales desafíos previstos en la protección contra los ataques están relacionados con la capacidad de supervisar el acceso remoto de los trabajadores, la escasez de personal de seguridad de TI y la resiliencia cibernética.** El 40 % de los encuestados mexicanos informó que su organización tenía dificultades para monitorear el acceso remoto de los trabajadores, escasez de habilidades de seguridad de TI (29 %), falta de resiliencia o preparación para responder a un ataque cibernético (27 %) y falta de presupuesto (24 %). Otros desafíos principales incluyen el volumen de incidentes (21 %), la falta de visibilidad de dispositivos o redes (19 %), protecciones de firewall inadecuadas u obsoletas (18 %), demasiadas herramientas de seguridad aisladas (17 %), demasiadas alertas para analizar y responder (16 %), falta de soporte de los líderes empresariales (14 %) y falta de visibilidad del acceso y uso de la nube (13 %).

13. **La mayoría (69 %) de las organizaciones mexicanas indicó que sus presupuestos de seguridad informática aumentaron en 2022, y el 74 % dijo que esperaba mayores presupuestos de seguridad en 2023 para combatir las amenazas conocidas y nuevas.** El otro 12 % no espera ningún cambio en sus presupuestos, mientras que el 26 % espera que sus presupuestos se reduzcan el próximo año. Muchas de las amenazas percibidas se centraron en la exfiltración de datos y las amenazas de red. "Las más grandes amenazas están evolucionando constantemente, y actualmente encontramos nuevos ataques de IoT que son difíciles de contrarrestar", dijo el director de seguridad y cumplimiento normativo de una empresa minorista mexicana.

69 %

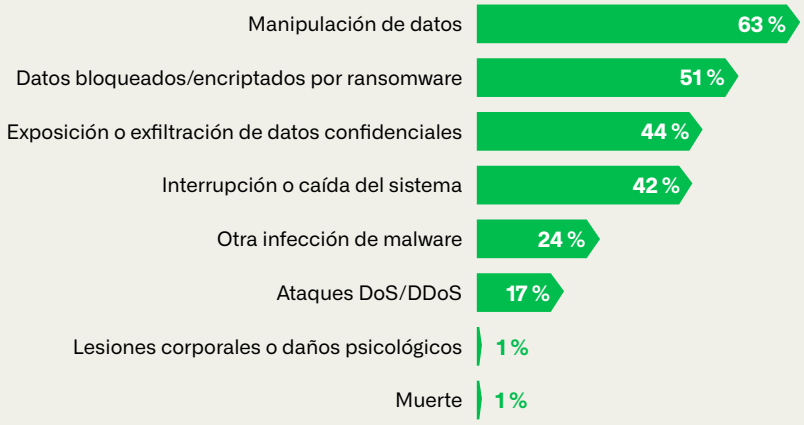
de las organizaciones mexicanas indicó que sus presupuestos de seguridad informática aumentaron en 2022

14. **Las compras tecnológicas previstas más populares incluyen el aprovisionamiento seguro y la prevención de pérdida de datos y aprovisionamiento y desaprovisionamiento seguros (22 % cada uno) y seguridad de red (firewalls/IPS, etc.) (21 %) para la protección de entornos locales; puntos de aplicación de seguridad de acceso a la nube (CASB) (39 %) y VPN/controles de acceso (28 %) para sistemas basados en la nube; y seguridad de red (58 %) y cifrado de datos, prevención de pérdida de datos y seguridad DNS (57 % cada uno) para entornos híbridos.** Las prioridades más altas para mejorar la protección de la red generalmente están relacionadas con la prevención de la exfiltración de datos, la aplicación de más protecciones en torno al uso de la nube y una mejor capacitación para los empleados para ayudar a combatir el phishing.

15. **Para administrar sus redes remotas distribuidas y optimizar sus servicios basados en la nube en 2022, la mitad de los encuestados en México indicó que su organización había agregado recientemente servidores DDI administrados en la nube, que representó un aumento en comparación con 2021 cuando solo un tercio mencionó la implementación de soluciones DDI de administración de red.** Los ataques a la nube aumentaron para las organizaciones mexicanas en 2022, ya que el 41 % de las víctimas de violaciones indicó que su entorno en la nube fue el vector de ataque, en comparación con el 30 % en 2021. Después de la filtración de datos y las amenazas de ransomware, la preocupación por los ataques a la nube es cada vez mayor en las organizaciones mexicanas en 2022, con un 43 % que menciona esta amenaza entre sus principales preocupaciones en comparación con el 38 % en 2021.

¿Cuáles fueron las repercusiones de las violaciones que experimentó su organización en los últimos 12 meses?

Seleccione todas las que correspondan.



OBTENGA UNA COMPRENSIÓN MÁS COMPLETA

Este informe se basa en datos nacionales de una encuesta global online realizada entre julio y agosto de 2022. En Infoblox, encontrará un informe global más detallado que proporciona información adicional sobre los resultados de la encuesta y una perspectiva global invaluable del panorama de amenazas que todos enfrentamos , así como las opiniones de tecnología y seguridad de otros líderes de seguridad en todo el mundo.

Sede corporativa
2390 Mission College Boulevard,
Ste. 501, Santa Clara, CA 95054

+1.408.986.4000
info@infoblox.com
www.infoblox.com