¿Hacia dónde apunta la **seguridad** en la segunda mitad de año?

A medida que la pandemia y los cierres se extienden a un tercer año, las organizaciones están acelerando los proyectos de transformación digital para respaldar el trabajo remoto. Mientras tanto, los atacantes se han aprovechado de las vulnerabilidades en estos entornos, haciendo crecer el trabajo y el presupuesto para los equipos de seguridad.

Según el State of Security Report 2022, México terminó 2021 con una recesión principalmente por la escasez de la cadena de suministro y los precios más altos de envío. La contracción económica también tuvo un impacto en el panorama general de ciberseguridad del país.

En 2017, México ocupó el puesto 28 entre 182 países en términos de madurez de ciberseguridad, según el Índice de Ciberseguridad Global de la Unión Internacio nal de Telecomunicaciones de las Naciones Unidas. Para 2020, había caído al lugar **52** y vio dispararse los ataques de ransomware.

Entre los hallazgos clave en el mercado mexicano destacan:

• El aumento del trabajo remoto ha cambiado el panorama corporativo de manera significativa y permanente. El **52%** de los encuestados aceleró los proyectos de transformación digital, el **45%** aumentó el soporte del portal del cliente para la participación remota, el **30%** trasladó las aplicaciones a proveedores de nube externos y el **26%** cerró las oficinas físicas para siempre. Estos cambios dieron lugar a la incorporación de VPN y firewalls, una combinación de dispositivos corporativos y propiedad de los empleados, así como servidores DDI locales y en la nube para gestionar el tráfico de datos en la red ampliada.

• Desde 2020, muchas organizaciones mexicanas han acelerado sus transformaciones digitales para apoyar a los trabajadores remotos. El estudio muestra que el **52%** acortó los plazos para modernizar su infraestructura de TI y el **45%** agregó más recursos a las redes y bases de datos. **36%** de las empresas mexicanas también aumentaron el apoyo a los portales que permitieron la participación remota del cliente.

• La realidad de la fuerza laboral híbrida está causando mayores preocupaciones con la fuga de datos, ransomware y ataques a través de herramientas de acceso remoto y servicios en la nube. Los encuestados indican preocupaciones sobre su capacidad para contrarrestar ataques cibernéticos cada vez más sofisticados con un control limitado sobre los empleados, las tecnologías de trabajo desde el hogar y los socios vulnerables de la cadena de suministro. La sofisticación del malware patrocinado por el estado también es motivo de preocupación para muchos.

• Las organizaciones tienen buenos motivos para preocuparse: el **66%** de los encuestados experimentaron hasta cinco incidentes de seguridad que provocaron al menos una violación. El **47%** de las empresas mexicanas tenían más probabilidades de ser víctimas de ransomware y el **45%** de phishing. Los ataques tendían a originarse en puntos de acceso WiFi, terminales propiedad de los empleados o en la nube. El **70%** sufrió al menos **$1 millón** en pérdidas directas e indirectas.

• Las organizaciones están comprando herramientas de seguridad que priorizan la nube para proteger sus entornos híbridos. El **56%** de los encuestados vio presupuestos más grandes en 2021 y casi **83%** anticipa un aumento en 2022. Aquellos que anticipan un enfoque híbrido son los más aptos para adoptar VPN/control de acceso en **54%,** seguridad DNS **53%** y cifrado de datos y prevención de pérdidas 50%.

• El **83%** de las organizaciones mexicanas en general pudieron responder a una amenaza dentro de las 24 horas. Esta tasa de tiempo de respuesta, una de las más altas de todas las naciones encuestadas, fue asistida por herramientas de búsqueda de amenazas como plataforma o servicio de inteligencia de amenazas externas en **49%,** una vulnerabilidad específica del sistema en **46%** y DNS (Sistema de nombres de dominio) consultas y respuestas en **38%.**

Las compañías están creando una estrategia de defensa en profundidad utilizando de todo, desde la seguridad de la red y endpoint hasta los agentes de seguridad de acceso a la nube, seguridad de DNS y los servicios de inteligencia de amenazas para defender la superficie de ataque. **52%** utiliza DNS para determinar qué dispositivos estaban realizando solicitudes vinculadas a destinos maliciosos y **50%** para protegerse contra amenazas como la exfiltración de datos de DNS.

Fuente de información: cio.com.mx