

Robo de información: la principal amenaza para la ciberseguridad en 2022

15/10/2021
Gustavo Torres

La ciberseguridad se convirtió en una de las prioridades en muchos sectores empresariales debido al aumento de ataques en la red.

De acuerdo al informe del Panorama de amenazas en América Latina de Kaspersky, en el primer semestre de 2021 se produjeron 299 intentos de ciberataques por hora en México. La tendencia para 2022 indica que el robo de información será uno de los principales motivos para la creación de sistemas de seguridad y la alianza con medios especializados.

En entrevista para NotiPress previo a la presentación del nuevo cyber defense center de Data Warden, Jesús Navarro, CEO de Data Warden, empresa especializada en seguridad informática, comentó en exclusiva que el ransomware se convertirá en la principal amenaza para las empresas de cara a 2022. Este malware, esparcido a través de mensajes o correo electrónico, «secuestra» información y amaga con divulgarla a menos de que se pague por su liberación. «Las campañas de concientización podrían parecer suficientes, pero hay un repunte de ransomware debido a que los usuarios no están atentos al riesgo de ataques en la red. Se trata de un trabajo en conjunto entre empresas y consumidor; mientras más comunicación exista, más seguro estará su entorno», señala Navarro.

Aunque las organizaciones ya habían iniciado su migración a la nube, una red de servidores remotos, la pandemia por Covid-19 aceleró el proceso creando grietas en el tema de ciberseguridad. Ante este panorama se presentan problemas como almacenamiento mal configurado, nulo control y vulnerabilidades en la nube, fácil acceso a copias de seguridad, entre otras. Navarro explicó que las empresas no migraron de manera segura al trabajo remoto y en muchos casos no existe una estructura que permita el acceso a distancia.

De acuerdo al informe El estado del ransomware 2021 de Sophos, compañía británica de ciberseguridad, de 5mil 400 empresas encuestadas a nivel mundial, 37% fue víctima de este tipo de ciberataque. De esta cifra, el 54 por ciento sufrió robo de información por una deficiente estrategia de ciberseguridad. El estudio señala que el sector de distribución y transporte es el que tiene más capacidad para evitar el cifrado de datos, con 48 por ciento de probabilidad de ataque. Por su parte, las entidades de los gobiernos locales tienen más probabilidades de ser afectados con robo de información al tener el 69% de vulnerabilidad. Esto debido a su relevancia para el acceso a fondos públicos y su deficiente estructura de tecnología.

Es necesario la implementación de soluciones de ciberseguridad que reduzcan los puntos ciegos para hacer frente al robo de información, independientemente de quién utilice los datos o desde donde lo haga. «Es primordial educar al personal sobre cómo manejar los correos electrónicos y archivos procedentes de fuentes no reconocidas. Un solo click desde una computadora o un celular puede causar daños financieros a una empresa y, en el peor de los casos, se refleja en el cierre total de operaciones», advierte Navarro.

Otro de los puntos importantes a tratar dentro las tendencias en ciberseguridad para 2022 será la piratería de software. Esto ocasiona que los dispositivos no reciban los parches de seguridad oficiales, aumentando el riesgo de la aparición de ransomware. Además se deberá tener especial cuidado con el uso de tecnología móvil. Con las nuevas actualizaciones y su importante papel en la comunicación empresarial y personal, se convierten en uno de los principales objetivos para el robo de información.