¿Tu empresa está protegida contra el ransomware?

El **backup es la mejor opción para responder a un incidente de seguridad**, ya que permite recuperar la información de valor ante un posible ataque de ransomware y también de otro tipo de amenazas informáticas e incluso físicas.
Sin embargo, no todos le dan la importancia debida. Datos del ESET Security Report 2018 arrojaban que en México, por ejemplo, solo el **50% de las empresas contaba con una solución de backup**, y datos más recientes a nivel regional reflejan que el 37% de las compañías con perfil Enterprise no cuenta con una solución de backup.

México se encuentra entre los principales países que mayor cantidad de detecciones de ramsomware tuvo durante el año pasado. Le siegueron Colombia y Perú, mientras que a nivel global Estados Unidos y Rusia lideran el ranking.

En el caso de Latinoamérica, el 70 % de los afectados perdieron información, dinero o ambas cosas.

Perder información de valor es una de las principales consecuencias que puede sufrir una empresa o individuo al ser víctima de un ransomware. Ante ello, y en el marco del **Día mundial del Backup**, ESET destaca la importancia de realizar respaldos periódicos de información como estrategia preventiva ante un posible ataque, así como de otros posibles incidentes de seguridad.

De acuerdo con la firma de seguridad, el objetivo de los cibercriminales es dirigir las campañas de ransomware a un pequeño número de víctimas pero que sean altamente rentables, en lugar de campañas de spam maliciosas en busca de un gran volumen de víctimas, cada una generando una pequeña retribución económica.

Para conocer de primera mano las experiencias de usuarios, ESET desarrolló una encuesta a su comunidad y a ejecutivos, técnicos y gerentes de empresas de más de 15 países de la región. Entre los datos más relevantes, está que el 29% de los participantes aseguró haber sido víctima de algún tipo de ransomwarey que el 70% de ese porcentaje perdió información, dinero o ambas cosascomo consecuencia de un ataque de este tipo de malware. En este sentido, el 93% de las víctimas del ransomware dijo haber cambiado su opinión con respecto a la importancia que tiene realizar backup de la información.

Si bien los **investigadores de seguridad recomiendan nunca pagar por el rescatede la información secuestrada**, ya que alienta al mercado y no asegura que los cibercriminales realmente descifren los archivos al pagar, 1 de cada 4 de los encuestados dijo que pagaría un rescate con tal de recuperar la información del cifrado.

Por otra parte, el 60% de los encuestados dijo conocer a alguien que fue víctima del ransomwarey casi un tercio de ese porcentaje conoce a empresas que fueron afectadas por esta amenaza. En esta misma línea, el 81% de los encuestados dijo que se sentiría preocupado en caso de saber que la empresa en la cual confía su información no cuenta con una solución de backup.

ESET cuenta con unKit Anti-Ransomware, el mismo es gratuito e incluye diferentes herramientas educativas y tecnológicas que pueden ayudar a evitar las infecciones con el ransomware: https://secure.eset-la.com/kit-Antiransomware. Por otro lado, teniendo en cuenta la Ley de protección de datos, que busca garantizar la integridad de la información de los usuarios y clientes, ESET acerca una guía por país que explica los estándares y regulaciones globales, locales y las medidas de seguridad a implementar para alcanzarlas: https://www.eset-la.com/regulacion-de-datos