# La realidad del ransomware golpea; ¿cómo golpear de regreso?

Los ataques de ransomware se han abierto paso en los bolsillos de las empresas, que deben pagar rescates exorbitantes en respuesta a agresiones altamente selectivas de parte de sofisticadas organizaciones criminales. Con el inicio del trabajo remoto masivo, el problema sólo ha empeorado. **La extensión de los límites de la oficina a ubicaciones remotas y en línea ha expuesto graves vulnerabilidades, y los delincuentes están muy dispuestos a aprovecharlo.**

En este momento, de acuerdo con CyberSecurity Ventures, **cada 11 segundos se produce un nuevo ataque de ransomware.** Para poner esto en contexto, **cada cinco minutos habrán sido vulneradas con ransomware 27 empresas.** El mejor consejo es evitar ceder y pagar el rescate. No obstante, la mayoría de las organizaciones pagarán, aunque muchas estén bajo presión extrema para limitar el daño del tiempo de inactividad causado por el ransomware.

No es sorpresa que tantos hayan optado por pagar cuando ya están lidiando con los desafíos y las presiones de operar en el arriesgado terreno empresarial que ha creado el Covid-19. Con todo, esto simplemente alienta a los atacantes cibernéticos a seguir explotando este mercado ilegal, evidentemente lucrativo: **desde el inicio de la pandemia, los ataques han crecido 600%.**

Lo positivo es que tanto empresas como gobiernos reconocen que esto no puede continuar. **El ransomware está ahora en la agenda de todas las salas de juntas, e incluso fue tema en el G7**, así como en muchas otras conversaciones diplomáticas entre líderes mundiales. Ahora es el momento de la Protección de Datos Moderna para acabar con el ransomware.

## Pensar como un hacker

De la misma manera en que un detective tiene que pensar como delincuente para resolver un crimen, la única forma en que las empresas se protegerán con éxito de los ciberataques es pensando como los hackers informáticos. **Son implacables, hiper-conscientes y estrictos. Empleadores y empleados necesitan actuar de la misma manera para evitar que se abra la puerta hacia las vulnerabilidades.**

La buena higiene digital debe convertirse en algo natural, a diferencia de algo que se practica únicamente durante la semana posterior a la capacitación anual de seguridad cibernética, y luego se olvida hasta el siguiente año. **No aplicar parches al software debería generar la misma atención que olvidar cerrar la oficina por la noche.** No contar con un plan de recuperación ante desastres es similar a saltarse el tener un adecuado plan de alguna aseguradora. Hay que evitar pensar nada más en la seguridad en el espacio físico, pues los enemigos están operando en el digital.

Otro aspecto importante es la tasa de éxito de los hackers. En muchos casos, se pasan todo el día atacando sistemas. Dedican su tiempo a evolucionar e innovar sus ataques para superar las barreras de seguridad que los detienen. Necesitamos anticipar que eventualmente podrá tocarnos

a nosotros, incluso teniendo la mejor defensa de ciberseguridad en su sitio. Como podemos ver en la cantidad de organizaciones que pagan rescates, **un ataque puede causar suficiente daño como para empujar a los negocios a pagar en lugar de tomar rutas alternativas.**

Depende de las empresas de todos los sectores invertir en prácticas de Protección de Datos Moderna para minimizar el impacto de los ataques de ransomware. Ver los ataques como algo inevitable es el primer paso hacia la creación de una cultura más cibersegura, con empleados más educados y conscientes del ransomware. Al mismo tiempo, **las organizaciones deben contar con las protecciones adecuadas para minimizar las interrupciones, incluido el software antivirus y los firewalls, además de un respaldo y recuperación continuo para ofrecer un seguro adecuado contra los efectos paralizantes del ransomware.**

Si sucede lo peor y sus sistemas se ven comprometidos, la empresa no colapsará y el atacante no conseguirá lo que desea. El panorama de la seguridad cibernética puede parecer inestable en este momento, pero hay pasos que podemos –y debemos– tomar para protegernos mejor de los daños. **Es hora de devolver el golpe del ransomware a los hackers.**