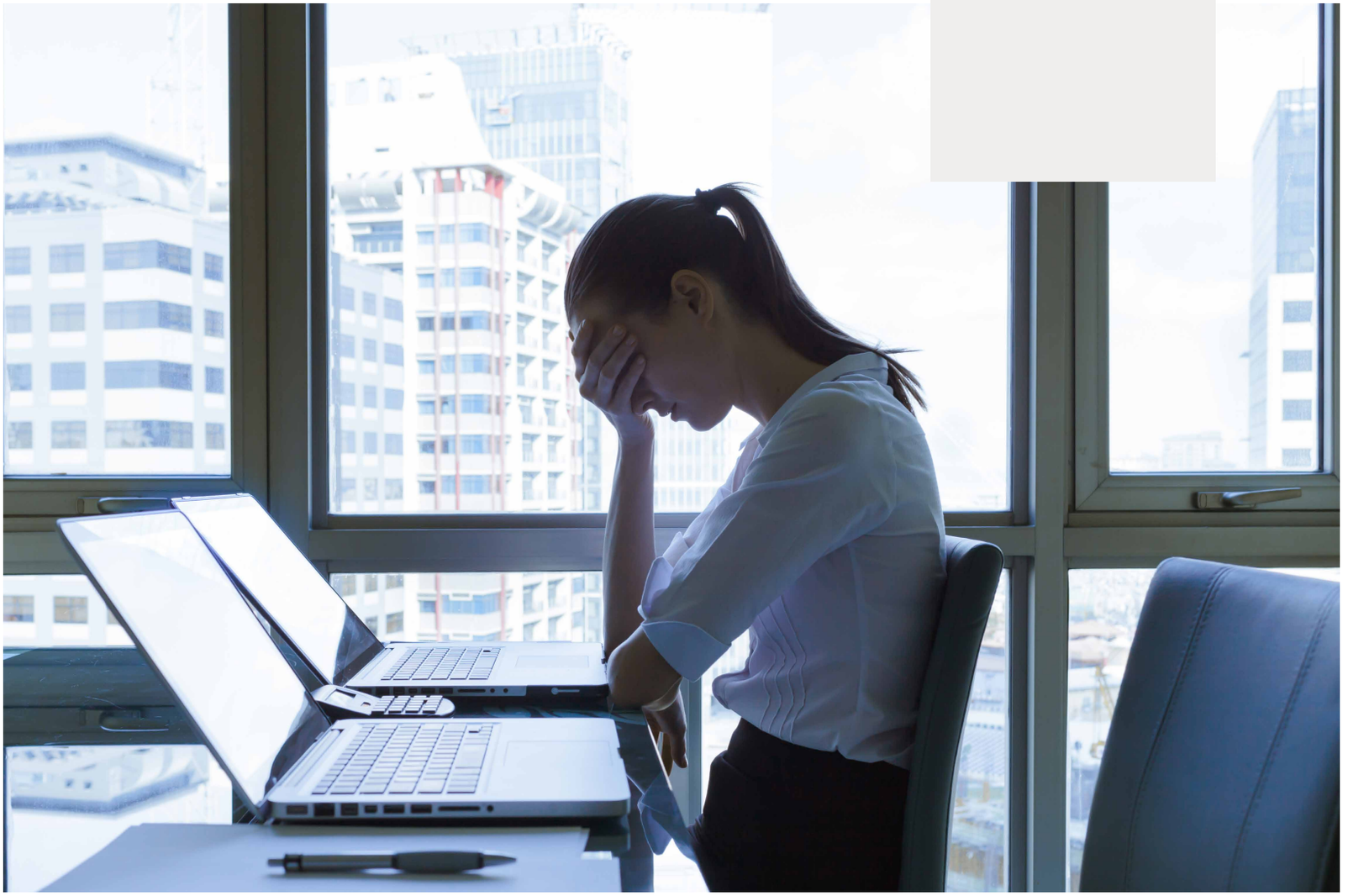
Acronis



Ransomware

La amenaza para los datos de más rápido crecimiento

El ransomware –malware que infecta sus computadoras, cifra sus datos y pide un rescate nada desdeñable a cambio de las claves de cifrado– aumenta vertiginosamente. De hecho, se espera que los daños a nivel mundial alcancen los 11 500 millones de dólares para finales de 2019, frente a los 325 millones de dólares de 2015.

Lo que desconoce es que esta amenaza puede dañarle tanto a usted como a su empresa.

EL COSTO DEL RANSOMWARE

Nadie quiere elegir entre pagar a un ciberdelincuente o resignarse a perder sus datos para siempre. Pero pagar no le protege en absoluto frente a futuros ataques, y el 20 % de la veces, la clave de descifrado no funciona. Por este motivo los expertos en seguridad recomiendan no pagar el rescate.

Además, el mayor gasto que genera el ransomware no es el rescate: son los costos de recuperación y, para las empresas, la pérdida de ingresos por el tiempo de inactividad, ya que hacen falta, de media, dos días para recuperarse de un incidente de ransomware. **Según CNNtech**, ese tiempo de inactividad cuesta a las pequeñas empresas una media de más de 100 000 dólares por ataque.

¿NO CREE QUE ESTÁ EN PELIGRO?

Los ciberdelincuentes utilizan nuevas tecnologías para crear rápidamente nuevas variantes de ransomware, mientras que los nuevos métodos de destrución han aumentado el número de ataques. Existen incluso "kits" de ransomware que se venden en Internet y que hacen posible que cualquiera pueda lanzar un ataque, incluso si no sabe escribir código. Esto hace que recibir una ataque de ransomware sea casi una certeza matemática.

FRECUENCIA DE LOS ATAQUES DE RANSOMWARE

No adoptar las medidas necesarias para proteger sus datos puede salir muy caro:

Las empresas
son atacadas cada

40 **SEGUNDOS**

Los particulares
son atacados cada

51 **SEGUNDOS**

LAS INFECCIONES SON MUY DIFÍCILES DE EVITAR

El ransomware puede introducirse en sus sistemas de muchas formas, tanto en casa como en el trabajo. Es tan simple como si alguien:

- Abre un adjunto de correo electrónico infectado
- Hace clic en un anuncio o enlace que dirige a un sitio web malicioso
- Conecta una unidad USB infectada
- Descarga software que contiene ransomware

Un solo paso en falso y un brote de propagación rápida puede bloquear portátiles, servidores, estaciones de trabajo y aplicaciones críticas

DEFIÉNDASE

Solo existe una forma infalible de detener un ataque de ransomware y recuperarse lo antes posible. La **copia de seguridad híbrida segura** combina defensas antiransomware avanzadas con copias de seguridad que se almacenan tanto in situ como en la nube.

Acronis

Para obtener más información, visite **www.acronis.com**