SMALL BUSINESS BIG THREAT

Lo que se debe y no se debe hacer con respecto al ransomware

Qué es: el ransomware bloquea todos los archivos disponibles en su sistema informático y le hace pagar por un código para poder restaurarlos. ¡También puede dar lugar a que pierda todos sus archivos!

Quién se ve afectado: el ransomware puede afectar a cualquier empresa. Si sufre un ataque, se infiltrará en su sistema, independientemente del tamaño de su empresa. En la mayoría de los casos, afecta los sistemas Windows.

Lo que se debe hacer	¿Por qué?
Hacer las copias de seguridad de su computadora en un lugar al que no siempre tenga acceso. Cuanto mayor sea la frecuencia, mejor.	El ransomware encripta todo a lo que puede acceder, incluso las unidades de red, Box y cualquier sistema que funcione como almacenamiento externo.
Implementar un plan de recuperación ante desastres.	El ransomware puede ser un verdadero desastre. Asegúrese de planificar para estar preparado y pruebe todas las opciones.
Capacitar al personal, incluso en una empresa pequeña.	La capacitación es la mejor defensa, ya que las personas son el eslabón débil de la exposición al ransomware.
Usar un cortafuegos	Algunos ransomware atacan únicamente a través de problemas de seguridad conocidos, así que asegúrese de que no puedan pasar a través de un cortafuegos de clase empresarial.
Usar IPS/IDS	La detección de la intrusión y la prevención de la intrusión pueden detectar un ataque ni bien ingresa. También ofrecen protección para sus usuarios cuando se encuentran en el lugar incorrecto.
Usar antivirus y antimalware	Le guste o no, los antivirus salvan a las personas todo el tiempo. Las estadísticas son indiscutibles. Asegúrese de elegir una buena versión “no gratuita” de un antivirus de confianza.
Usar un sistema de protección de DNS	En ocasiones, una capa es algo que lo salvará. Considere el uso de una capa adicional de protección, como Umbrella.
Saber a quién llamar	Ya sea con respecto al ransomware o cualquier otro asunto, no confíe únicamente en las búsquedas en Internet. Busque una empresa confiable que lo ayude con lo que usted no sepa y evite formar parte de las estadísticas.

Lo que no se debe hacer	¿Por qué?
Abrir correos electrónicos de remitentes desconocidos	El ransomware encripta todo a lo que puede acceder, incluso las unidades de red, Box y cualquier sistema que funcione como almacenamiento externo.
Subestimar la amenaza	Nadie está a salvo del ransomware.
Omitir las actualizaciones y los parches de seguridad	Muchos ataques de ransomware se solucionan rápidamente en los parches. Si espera para aplicar un parche a su sistema, puede quedar vulnerable.
Mantener los datos solamente en el sitio	Recuerde que debe mantener varias copias de sus datos: 3 copias, 2 tipos de medios, 1 fuera del sitio.