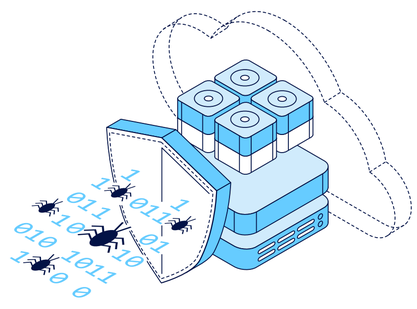
EDICIÓN PARA AMÉRICA

2022

Informe sobre tendencias de ransomware

En enero de 2022, una firma de investigaciones independiente completó una encuesta a **1,000** líderes de TI imparciales sobre el impacto que el ransomware tuvo sobre sus entornos, además de hablar sobre sus métodos de remediación y sus estrategias de cara al futuro. Los participantes pertenecían a uno de los siguientes puestos: CISO, profesionales de seguridad, administradores de backup y operaciones de las TI. Estos puestos representaron a organizaciones de todos los tamaños en 16 países de APJ, EMEA y América, de los cuales **500** son del Continente Americano.

Omnipresencia del ransomware



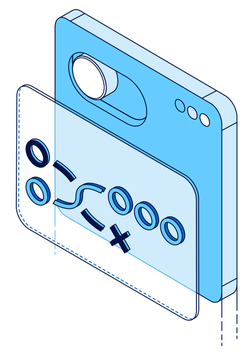
95 %

de los ataques de ransomware intentaron infectar los repositorios de backup y **71 %** de esos intentos fueron exitosos

44 %

de los datos de producción fueron cifrados, y de ese porcentaje, **67 %** de los daos pudieron recuperarse

Rescate ≠ remediación



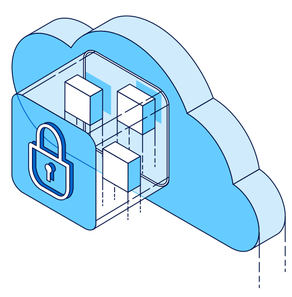
19 %

de las organizaciones pudieron recuperar los datos sin pagar el rescate

31 %

de las organizaciones que pagaron el rescate no recuperaron sus datos de todos modos

Tecnología para sobrevivir



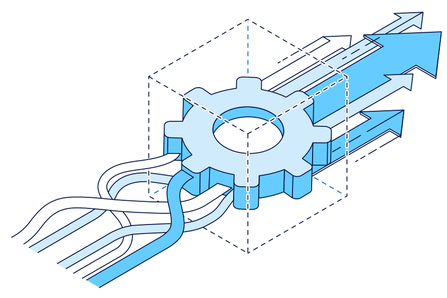
84 %

de las organizaciones dependen de registros de backups o de la capacidad de lectura de medios para garantizar la capacidad de recuperación, lo que quiere decir que solo **16 %** realizan pruebas rutinarias de restauración y pruebas de funcionalidad

43 %

de las organizaciones restauraron primero a un sandbox aislado antes de recuperar sus datos luego de un ataque de ransomware

Alineación organizativa



53 %

de las organizaciones creen que es necesaria una reforma significativa o completa entre el backup y la ciberseguridad

38 %

de los métodos contra el ransomware de los ciberequipos incluyen verificaciones o reglas para la comprobación de la limpieza de los datos

Un backup seguro es su última línea de defensa

El ransomware es un desastre que cuesta a las empresas casi dos millones de dólares (estadounidenses) por incidente. En Veeam®, creemos que un backup seguro es su última línea de defensa contra el ransomware. Nuestro software cuenta con un diseño seguro. Elimina la dependencia del hardware propietario para trabajar con su arquitectura ya existente, tanto en las instalaciones locales como en la nube, ya que contar con un backup confiable puede ser lo único que lo salve del tiempo de inactividad, la pérdida de datos y el pago de un rescate elevado.

Más información: www.veeam.com/es-lat

Descargue el informe completo de la investigación aquí