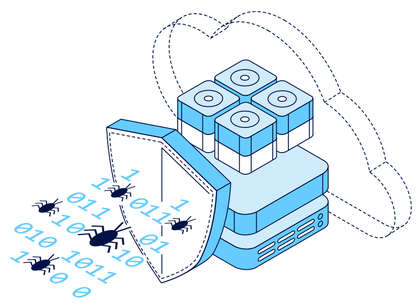
EDICIÓN EMEA

2022

Informe de tendencias de ransomware

En enero de 2022, una empresa de investigación independiente realizó llevó a cabo una encuesta a **1000** responsables imparciales de TI sobre el impacto que el ransomware había tenido en sus entornos, así como sobre los métodos de reparación y estrategias de cara al futuro. Los encuestados pertenecían a una de estas cuatro categorías: CISO, profesionales de seguridad, administradores de backup y operaciones de TI. Estas personas representaban a organizaciones de todos los tamaños de 16 países diferentes de APJ, EMEA y América, entre los que se incluían **300** afincadas en EMEA.

Penetración del ransomware



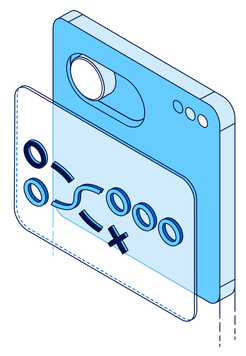
El 88 %

de los ataques de ransomware intentaron infectar los repositorios de backup, y el **75 %** de esos intentos tuvieron éxito

El 47 %

de los datos de producción fueron cifrados con éxito, y de esos solamente el **72 %** de los datos pudieron ser recuperados

Rescate ≠ reparación



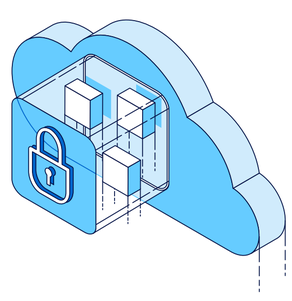
El 22 %

de las organizaciones fueron capaces de recuperar sin realizar el pago del rescate

El 29 %

de las organizaciones que pagaron el rescate todavía no han podido recuperar sus datos

Tecnologías para la supervivencia



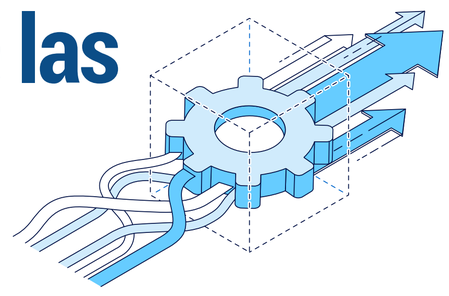
El 84 %

de las organizaciones confían en los registros de backup (logs) o legibilidad de los soportes para asegurar la capacidad de recuperación, lo que significa que solamente el **16 %** lleva a cabo pruebas rutinarias de restauración y comprobación de la funcionalidad

El 52 %

de las organizaciones primero restauraron a un entorno sandbox aislado antes de recuperar los datos tras un ataque de ransomware

Alineamiento de las organizaciones



El 49 %

de las organizaciones creen que es necesario llevar a cabo una revisión significativa o completa de lasestrategias de backup y ciberseguridad

El 33 %

de las guías contra ransomware de los equipos de ciberseguridad incluyen procesos de verificación y órdenes que garanticen la limpieza de los entornos

Un backup seguro es su última línea de defensa

El ransomware es un tipo de desastre que le cuesta a las empresas cerca de dos millones de dólares (USD) por incidente. En Veeam®, creemos que la última línea de defensa contra el ransomware es contar con un backup seguro. Nuestro software es seguro por diseño y elimina el bloqueo del hardware propietario para trabajar con su arquitectura existente, tanto localmente como en la nube, porque disponer de un backup fiable puede suponer la diferencia entre el tiempo de inactividad, la pérdida de datos y pagar un costoso rescate.

Más información: www.veeam.com/es

Descargue aquí el informe completo