Pruebas de recuperación ante desastres: garantizar que su plan de recuperación ante desastres funcione

Pruebas de recuperación ante desastres: garantizar que su plan de recuperación ante desastres funcione.Descubra por qué las pruebas de recuperación ante desastres son esenciales para todas las organizaciones de TI y cómo llevarlas a cabo de manera exitosa y eficiente.

La prueba de recuperación ante desastres es un simulacro de varios pasos del plan de recuperación ante desastres (DRP) de una organización diseñado para garantizar que los sistemas de tecnología de la información (TI) se restablecerán si ocurre un desastre real.

Como parte de un plan de recuperación ante desastres , las empresas suelen contratar un servicio de recuperación ante desastres .

¿Por qué son esenciales las pruebas de recuperación ante desastres?

Durante un desastre, un evento natural o provocado por el hombre interrumpe la funcionalidad normal de TI, como el procesamiento de datos, las comunicaciones, la virtualización y las operaciones de redes y centros de datos.

La investigación muestra consistentemente que la pérdida de las funciones de TI en un desastre conduce al fracaso empresarial.

Los huracanes como Katrina y Sandy, los terremotos, las

inundaciones y el tsunami son potencialmente comerciales. Los desastres provocados por el hombre pueden desconectar un negocio, incluir actos de terrorismo, vandalismo informático, sabotaje y percances involuntarios, tales como configuraciones incorrectas de hardware y archivos borrados accidentalmente.

Los desastres no ocurren con mucha frecuencia, pero cuando lo hacen, los efectos pueden ser devastadores.

El objetivo principal de DRT (Disaster Recovery Testing) es asegurarse de que, en caso de que ocurra un desastre, el plan de DR realmente funcione. El sitio de DR de una empresa se activará, los sistemas de TI volverán a estar en línea con un tiempo de inactividad mínimo. Tal vez una empresa utiliza DR basada en la nube o DRaaS ; en cualquier caso, las pruebas de DR revelan si la copia de seguridad es realmente tan infalible como debe ser.

Las pruebas continuas son una necesidad, ya que la efectividad del DRP puede verse afectada por los cambios inevitables en el personal, los niveles de habilidades y las arquitecturas de hardware y software dentro de una organización.

Escenarios de recuperación de desastres

Los planes de prueba de DR pueden ayudar a las organizaciones a prepararse para casi cualquier tipo de desastre de TI, incluidos los siguientes tipos de escenarios, que se han desarrollado en la vida real.

En un ataque de sabotaje interno, una compañía deshabilitó el acceso de un ingeniero de software justo antes de despedirlo. Sin embargo, el empleado descontento había iniciado sesión en el sistema desde su casa a principios de semana y dejó abierta su conexión remota. Después del disparo, utilizó esta conexión para eliminar varios archivos críticos

de una aplicación de fabricación. La compañía perdió cuatro horas de tiempo de fabricación antes de poder recargar los datos de respaldo y comenzar a fabricar nuevamente, dice un estudio publicado por la Universidad Carnegie Mellon (CMU).

En 2017, las empresas que incluían FedEx, Maersk, Merck y muchas otras fueron víctimas de un virus inspirado en ransomware llamado NotPetya. Después de que su negocio global de envíos se detuviera, Maersk admitió haber recibido un golpe de $ 670 millones por la limpieza de tecnología, interrupciones comerciales y pérdidas de ventas. Por su parte, FedEx perdió $ 400 millones.

En contraste, con la advertencia anticipada del huracán Katrina en 2005, la ciudad de Nueva Orleans logró mantener importantes funciones comerciales en funcionamiento sin interrupción durante y después de la tormenta mortal. La ciudad descargó sistemas críticos como la gestión financiera y los envió por adelantado a un centro de datos de ACS en California. Los sitios web de la ciudad fueron trasladados del Ayuntamiento a un centro de datos en Dallas operado por Red Carpet Host. Después de Katrina, la ciudad estableció un centro de datos de respaldo en Austin.

Recuperación ante desastres versus planificación de continuidad del negocio

La planificación y prueba de recuperación ante desastres es un término que a menudo se confunde con la planificación de continuidad del negocio (BCP). Si bien DRP y BCP están estrechamente relacionados, sin embargo, no son lo mismo.

Un plan de DR y un sistema de prueba especifica los pasos que debe seguir una organización de TI para recuperar sistemas que satisfagan las necesidades tecnológicas de la compañía después

de un desastre.

Un BCP, por otro lado, detalla lo que debe hacer una empresa para asegurarse de que sus productos y servicios permanezcan disponibles para los clientes. Un BCP se compone de un análisis de impacto empresarial, una evaluación de riesgos y una estrategia general de continuidad empresarial. Se prueba a través de una prueba de continuidad del negocio (BCT).

Algunas organizaciones tratan DRP / DRT y BCP / BCT por separado, mientras que otras incluyen DR dentro de la planificación y prueba general de continuidad del negocio.

Técnicas de prueba DR

Más allá de restaurar datos y mantener aplicaciones y servicios críticos en línea durante la emergencia, las soluciones de DR deben incluir formas de alertar al personal sobre el desastre y permitir las comunicaciones durante y después del evento si las líneas telefónicas y las redes se caen.

En el proceso de planificación y prueba, los equipos de DR también deben reconocer que, a pesar del desastre, la organización debe continuar cumpliendo con sus obligaciones de seguridad y cumplimiento normativo.

Se utilizan estos tipos de DRT para probar soluciones de recuperación ante desastres:

1. Prueba en papel: en una prueba en papel, los miembros del equipo de DR leen y anotan documentos del plan de recuperación, como las políticas, los procedimientos, los plazos, los puntos de referencia y las listas de verificación de DR. Una copia impresa de los documentos debe almacenarse en un entorno seguro fuera de línea y una copia digital en la nube.
2. Prueba de recorrido: Una prueba de recorrido es un

recorrido grupal del DRP para identificar cualquier problema que deba abordarse y cualquier modificación que deba realizarse en el entorno de recuperación ante desastres.

3. Simulación: en un procedimiento similar a un simulacro de incendio, los equipos practican el DRP en la vida real para asegurarse de que sea suficiente para la recuperación de desastres de TI.
4. Prueba paralela: en una prueba paralela, los sistemas de recuperación de conmutación por error se prueban para asegurarse de que, en caso de desastre, puedan realizar transacciones comerciales reales que admitan procesos y aplicaciones clave. Mientras tanto, los sistemas primarios continúan ejecutando la carga de trabajo de producción completa.
5. Prueba de corte: una prueba de corte va más allá para probar los sistemas de recuperación de failover creados para hacerse cargo de la carga de trabajo de producción completa en caso de desastre. Los sistemas primarios se desconectan durante la prueba.

Seis niveles de prueba de recuperación ante desastres

En pruebas paralelas y de transición, los sistemas de TI se pueden probar en diferentes niveles de exhaustividad. Las organizaciones de TI varían en cuanto a los niveles de pruebas realizadas, al igual que los proveedores de servicios de DR.

1. Verificación de datos

Este nivel de prueba comprueba que los bloques / archivos son buenos después de haber sido respaldados, pero no garantiza que las aplicaciones puedan recuperarse funcionalmente.

2. Montaje de base de datos

El montaje de la base de datos verifica que una base de datos tenga una funcionalidad básica dentro de las copias de seguridad.

3. Verificación de arranque de máquina individual

La verificación de arranque de una sola máquina verifica que un solo servidor se pueda reiniciar después de que se haya apagado.

4. Arranque de máquina individual con verificación de captura de pantalla

Esta prueba envía una imagen del sistema operativo a los administradores como prueba de que se puede reiniciar un servidor. Sin embargo, no prueba que el servidor seguirá siendo funcional para el negocio.

5. DR Runbook Testing

Involucrando múltiples servidores, las pruebas de runbook DR se usan principalmente con múltiples máquinas que brindan un servicio comercial en conjunto, como bases de datos agrupadas o sistemas de planificación de recursos empresariales (ERP).

6. Aseguramiento de recuperación

El nivel más alto de pruebas, la garantía de recuperación abarca múltiples máquinas, pruebas de aplicaciones profundas, evaluación de acuerdo de nivel de servicio (SLA) y análisis de la razón por la cual falló cualquier recuperación a la recuperación del sistema. Algunos pero no todos los proveedores de DRaaS ofrecen pruebas de garantía de recuperación.

Mejores prácticas de prueba de recuperación ante desastres

Prueba regularmente y a fondo

Algunas organizaciones grandes realizan pruebas de DR trimestralmente. Sin embargo, a pesar de la publicidad sobre las lecciones aprendidas de recuperación de desastres, el 23 por ciento de las empresas nunca prueba la recuperación de desastres, mientras que aproximadamente el 33 por ciento lo hace una o dos veces al año. Además, de las compañías que sí prueban sus DRP, alrededor del 65 por ciento falla sus propios DRT, según una encuesta.

Si bien la frecuencia de las pruebas dependerá de su negocio y su preparación para la recuperación ante desastres, los expertos recomiendan encarecidamente realizar una prueba completa al menos una vez al año.

Establecer puntos de referencia medibles

Para aplicaciones críticas, establezca RPO y RTO (objetivos de tiempo de recuperación y objetivos de punto de recuperación), que se pueden medir a escala. Los propósitos de estos puntos de referencia son asegurarse de que está alcanzando sus objetivos y al mismo tiempo detallar los procesos que explican el éxito.

Algunas industrias, incluida la atención médica, requieren que las organizaciones conozcan y documenten sus RTO. Independientemente de la industria en la que se encuentre, al usar puntos de referencia que se miden en una escala, en lugar de solo pasar / fallar, está mejor equipado para identificar los procedimientos de DR que necesitan mejoras.

Mantenga a los miembros del equipo DR alerta

Defina claramente a todas las personas responsables de investigar, desarrollar, implementar y probar el DRP. Asigne una persona de respaldo para cada función en un ejercicio de DR en caso de que la persona designada esté fuera de la oficina. Comparta el DRP y el DRT con todos los miembros del equipo.

Si los miembros del equipo abandonan la empresa, asegúrese de que sus reemplazos estén capacitados en las políticas y procedimientos de DRP y DRT. Luego, organice una ejecución grupal del DRT para suavizar los procesos de recuperación ante desastres.

Trabaje con un socio de DR si necesita uno

Si bien las grandes organizaciones tienen la experiencia interna disponible para realizar DRT por sí mismas, muchas empresas más pequeñas recurren a las empresas de DR para obtener ayuda.

Más allá de la DRaaS multifacética, los proveedores de servicios de recuperación ante desastres ofrecen servicios especializados como pruebas continuas y monitoreo del desempeño 24/7 de las soluciones DR de los clientes.

Leer también: ¿Qué debe incorporar su plan de recuperación de desastres? Cloud y Colocation; Backup remoto, qué es y por qué es importante