¿Está su Centro de Datos preparado para un desastre natural?

¿Está su centro de datos preparado para un desastre natural? La amenaza de un desastre natural se perfila en las mentes de los proveedores de centros de datos de todo el mundo. Gestionar las demandas de energía, refrigeración y seguridad de un centro de datos es bastante difícil incluso antes de tener en cuenta amenazas como huracanes, terremotos o inundaciones.

Mantener el acceso a los datos en caso de un desastre puede significar la diferencia entre el éxito o el fracaso de una empresa. Alrededor del 70% de las empresas han experimentado pérdida de datos debido a un accidente o desastre; Aún más preocupante, el 60% de esas empresas cierran en los seis meses posteriores a la pérdida de datos debido al desastre.

Es imperativo, entonces, que cada centro de datos tenga un plan integral para proteger los datos en caso de un desastre natural. Si bien se debe hacer todo lo posible para mantener el tiempo de actividad del servidor , los centros de datos deben considerar la posibilidad de que no puedan cumplir esa promesa en una situación de desastre. Después de todo, incluso el SLA más robusto no será demasiado si falla la energía y nadie puede acceder físicamente al centro de datos para que los sistemas críticos vuelvan a funcionar.

¿Qué podría salir mal?

En una palabra, todo. Estos son solo algunos ejemplos de desastres naturales que dejaron a los centros de datos tambaleándose:

- Relámpagos: Dicen que los rayos no caen en el mismo lugar dos veces, pero en 2015 uno de los centros de datos europeos de Google fue alcanzado por un rayo no una, sino cuatro veces, causando errores en el 5% de los discos responsables de Google Compute Engine (GCE) instancias. Aunque la compañía restauró muchas de las unidades, se estima que se perdió de forma irrecuperable un 0,000001% de los datos almacenados en el centro de datos. Si bien eso puede no parecer mucho, trate de decírselo a los clientes afectados por él.
- Huracanes: según National Geographic , 2017 fue la temporada de huracanes más cara en la historia de los Estados Unidos, con un costo aproximado de $ 200 mil millones. Con su combinación de fuertes vientos, mareas de tormenta y fuertes lluvias, los huracanes son uno de los centros de datos de desastres naturales más peligrosos que deben enfrentar. Las inundaciones repentinas resultantes del huracán Sandy en 2012 causaron grandes interrupciones en los centros de datos en Nueva York y Nueva Jersey. Estas fallas se agravaron aún más por el hecho de que los sistemas de respaldo se ubicaron en la misma región geográfica y fueron eliminados por el mismo evento climático.
- Tornados: un devastador tornado de 2011 arrasó varios edificios de hospitales en Joplin, Missouri, uno de los cuales era un centro de datos. Si bien ninguno de los datos perdidos fue de misión crítica, eso fue solo porque la mayoría de la información almacenada allí se había migrado a un nuevo centro de datos externo unas pocas semanas antes. Los funcionarios del hospital señalaron que si el tornado hubiera golpeado un mes antes, la pérdida de datos habría sido catastrófica y habría dejado al hospital completamente inoperable.
- Inundaciones: Las graves inundaciones en Leeds, Reino Unido, provocaron que un centro de datos de Vodafone perdiera energía temporalmente durante la Navidad de 2015. Si bien la pérdida de datos fue insignificante, el

corte de energía interrumpió el servicio de telefonía móvil temporalmente. Vodafone, por supuesto, tiene un poco de historia con las inundaciones, habiendo sufrido uno de los desastres más infames del centro de datos cuando su centro de datos de Estambul fue devastado por las inundaciones en 2009.

- Terremotos: hasta ahora, los centros de datos han tenido suerte. Los estándares arquitectónicos modernos y las precauciones adicionales (tales como gabinetes especiales y rodillos para bastidores de servidores) han recorrido un largo camino hacia la protección de los centros de datos contra terremotos, incluso en áreas de alto riesgo.
- Lo inesperado …: la planificación de desastres se trata de esperar lo inesperado. Tomemos, por ejemplo, la ardilla que desconectó el centro de datos de Santa Clara de Yahoo durante varias horas en 2010, o el camión que condujo a un transformador que alimentaba el centro de datos de Backspace en 2007.

¿Está preparado su centro de datos?

El primer paso que cualquier centro de datos debe dar para prepararse para un desastre es realizar una evaluación integral de riesgos. Esta revisión identificará la probabilidad y las consecuencias esperadas de posibles desastres. Una vez que se han identificado estos riesgos, el proveedor debe crear una lista de verificación paso a paso que detalle qué acciones deben tomarse en caso de cada desastre específico. Todo el personal relevante y el personal deben familiarizarse con estos planes y realizar simulacros regularmente para asegurarse de que todos sepan qué hacer en un escenario de desastre.

Mantener la red en funcionamiento es una consideración clave además de preservar los datos del cliente. Cada momento de inactividad conlleva costos financieros reales . Cualquier buen centro de datos ya debería tener extensas redundancias de redincorporado a su infraestructura informática, pero estos planes de respaldo deben ser aún más confiables en una situación de desastre.

Las pruebas periódicas son esenciales para garantizar que cuando se interrumpe la energía y los sistemas fallen, los datos del cliente y las operaciones críticas se mantengan en línea y seguros. Además, todo el personal relevante debe estar capacitado sobre qué hacer si el sistema de redundancia no funciona como se diseñó. Esto normalmente implica una intervención manual crítica y el personal debe estar capacitado en un entorno ‘práctico’ para obtener la experiencia y la comprensión del proceso y la reacción del sistema a las transferencias manuales.

Los centros de datos también deben considerar cómo los desastres afectarán la infraestructura que los rodea. Cuando el huracán Sandy azotó la ciudad de Nueva York, por ejemplo, muchos generadores de respaldo fallaron porque se quedaron sin combustible y no pudieron reponerse debido a las calles inundadas de la ciudad. Debido a que el acceso físico al centro de datos podría ser limitado y el acceso remoto puede no ser posible, es vital contar con sistemas de respaldo automatizados para garantizar que los datos y servicios de misión crítica de los clientes no se pierdan o interrumpan en caso de falla de energía.

Si se va a hacer una copia de seguridad de los datos en otro centro de datos, esa instalación debe ubicarse lejos del lugar afectado por un desastre natural. Los proveedores de centros de datos con instalaciones distribuidas en un área geográfica amplia están en mejores condiciones para garantizar que un desastre natural a gran escala no pueda eliminar todos sus servicios.

A medida que los desastres naturales como los huracanes y los incendios forestales se vuelven más frecuentes, los centros de datos deben tomar medidas activas para proteger sus instalaciones y, por extensión, a sus clientes. Aunque los servicios en la nube hacen que sea más fácil hacer una copia de seguridad de los activos esenciales y las técnicas modernas de construcción pueden proteger mejor el equipo contra el peligro físico, los centros de datos aún dependen de factores fuera de su control para mantenerse en funcionamiento. Solo preparándose para lidiar con una interrupción en sus operaciones diarias pueden estar verdaderamente preparados para cualquier desastre que la naturaleza decida lanzarles.

¿Está preparado su centro de datos?

Leer también: ¿Qué debe incorporar su plan de recuperación de desastres? Cloud y Colocation; Colocation (Colocación) debe ser parte de su plan de recuperación de desastres; Recuperación de desastres como servicio (DRaaS); ventajas y desventajas