Plan de recuperación de OVH luego del incendio de su data center en Francia

En La extinción de incendios en un centro de datos señalamos a grosso modo lo que sucedió con OVH y el incendio en su data center en Francia. Ahora queremos ahondar en lo que vienen a continuación y lo que nos enseña este tipo de siniestros a todos los demás centros de datos del mundo. Pero vamos por pasos.

Paso 1

Después del incendio que destruyó uno de los cuatro centros de datos en su campus de Estrasburgo, OVHCloud cerró todo el sitio por razones de seguridad. El grupo tiene la intención de relanzar gradualmente los servidores. Tras el incendio que estalló la noche del 9 de marzo en el sitio de OVHCloud en Estrasburgo, uno de los cuatro centros de datos del campus (SBG2) quedó completamente devastado por las llamas. Un segundo (SBG1) está parcialmente dañado: cuatro de sus doce salas de servidores han sido destruidas.

Como medida de precaución, se había cortado la electricidad en toda la instalación, impactando por rebote los dos centros de datos restantes (SBG3 y SBG4). OVHCloud está relanzando gradualmente las infraestructuras y servidores que aún funcionan. El suministro eléctrico se reinició el 16 de marzo y la restauración de la red está casi completa. OVH tiene previsto ahora reiniciar gradualmente los servidores desde el 22 marzo. El grupo tiene la intención de verificar el estado de cada servidor antes de que vuelva a funcionar.

Paso 2

Los clientes se beneficiarán de tres meses gratis en caso de que se produzca un corte en servicio y seis meses gratis en caso de pérdida de datos ”.

Las lecciones, la enseñanza

Finalmente, el director general (Octave Klaba)pretende sacar todas las lecciones del desastre en relación con la gestión de copias de seguridad, que resultaron ser defectuosas.

El grupo ha elaborado un inventario de copias de seguridad de datos no recuperables o datos en investigación según el centro de datos utilizado y el servicio suscrito, información crucial para permitir a sus clientes restaurar su sitio web y otras aplicaciones en la nube sin demora.

¿Copias de seguridad en la misma sala?

Sorpresa principal: dentro de SBG1, la oferta de nube privada de OVH (Private Cloud) se alojó en una sala y su copia de seguridad en otra sala del mismo centro de datos. Ambos fueron destruidos por el fuego. A menos que haya tomado la precaución de implementar una segunda copia de seguridad con otro proveedor (O un sólido plan de Recuperación de desastres), los datos se perderán. Recuerde que la solución de nube privada se ha posicionado históricamente en la gama alta.

Por otro lado, el 20% de las copias de seguridad de VPS / PCI basadas en la infraestructura alsaciana de OVH también se esfumó. Los clientes cuyas copias de seguridad forman parte de su 20% solo pueden esperar que sus servidores privados virtuales se hayan salvado.

También se suspendió la facturación en la fecha del incendio

para todos los clientes que utilizan los servicios en los centros de datos de OVH en Estrasburgo. A la espera de su regreso al servicio, se les ofrecen infraestructuras alternativas de forma gratuita (servidor bare metal, Hosted Private Cloud y Public Cloud) en los centros de datos del grupo en Roubaix y Gravelines. OVH también ha puesto a disposición de sus clientes un sistema de preguntas y respuestas para ayudarles a afrontar la situación.

Algunos hechos puntuales

El incendio se inició en el centro de datos SBG2, que quedó completamente destruido. Las alertas de incendio funcionaron bien. Pero el fuego se extendió demasiado rápido para permitir la intervención de agentes en el lugar. Tras el incendio que estalló la noche del 9 al 10 de marzo en el sitio de OVHCloud en Estrasburgo, se encuentran sin conexión 3,6 millones de servidores HTTP que representan 464.000 nombres de dominio. OVHCloud menciona entre 12.000 y 16.000 clientes afectados.

Consecuencias que demuestran la importancia de suscribirse a un servicio de respaldo en un centro de datos ubicado en otra geografía, o incluso en otro proveedor para compensar fallas que podrían afectar a todos los centros de datos del proveedor, como un desplome de la red que repercute en todos los servicios.

Recuerde que en HostDime, tenemos no solo un gran equipo humano altamente calificado para resolver sus inconvenientes sino que dispone de un DRP con esteroides, que ayudará a prevenir y a mitigar sorpresas innecesarias con su valiosa información.

Leer también: La extinción de incendios en un centro de datos; Centros de datos que enfrentan riesgos: amenazas controladas; Por qué el plan de recuperación ante desastres ya no debería considerarse una opción para su empresa