Servidores alojados, su falta de copias de seguridad y DRP

El título puede sonar un tanto traído de los cabellos, algo forzado quizás pero mirando en el contexto noticioso reciente, tal vez no resulte tanto. Luego de lo dicho en La extinción de incendios en un centro de datos creo que todo cobra sentido. Varias empresas critican a OVHcloud por no haber realizado una copia de seguridad adecuada de su contenido.

El asunto es que la responsabilidad de la data es del usuario, del dueño de la información (que casi siempre es el dueño del servidor que se encuentra en una infraestructura de un centro de datos). El inventario de lo recuperable muestra que son responsables de no haberse suscrito a las ofertas adecuadas.

Prevenir es mejor que lamentar

Y advierten los expertos: en cualquier caso, el hecho de que OVH haya perdido determinadas copias de seguridad no le hace más responsable de la imposibilidad de restaurar los sitios web, datos o aplicaciones de empresas que no se habían tomado el cuidado de poner en marcha un auténtico Plan de Recuperación de desastres (DRP). Tanto este Disaster Recovery Plan como la implementación de copias de seguridad, son responsabilidad del director de TI del cliente y de su director general. Hacer todo lo posible para garantizar la seguridad de sus datos es una obligación regulatoria, escrita en blanco y negro en el RGPD.

Quienes no se han suscrito a una oferta de PRA (DRP) o no han instalado ellos mismos un dispositivo de este tipo, sólo pueden culparse a sí mismos. Las empresas que acusen erróneamente a OVHcloud de haber perdido sus datos probablemente no dispondrán de medios legales para reclamar una indemnización al anfitrión. Sin embargo, son principalmente los clientes de estas empresas, especialmente los de las tiendas online, los que probablemente atacan a la justicia, por haber incumplido su deber de proteger los datos

privados que operaban. Es todo un círculo vicioso.

Ninguna nube ofrece un plan de recuperación ante desastres de forma predeterminada

Algunos clientes de OVHcloud están comunicando su intención de alojar sus sitios y aplicaciones en otro lugar. ¡Pero correrán exactamente el mismo riesgo en otros lugares! Hasta que las organizaciones se suscriban explícitamente a las ofertas de redundancia, estarán en el mismo peligro de que sus datos se esfumen con el resto del centro de datos. Nunca es porque los datos están alojados en la nube, que este servicio de Cloud, de repente, asumirá la responsabilidad de hacer copias en otro lugar cuando no se le haya pedido que lo haga.

Y los competidores de esta marca tampoco es que tengan mucho en donde escudarse. Y, lamentablemente, la historia muestra que el gigante AWS, el sector de la nube número uno del mundo, tampoco es inmune a un desastre natural: en 2018, su centro de datos de Tokio desapareció entre las llamas.

Vital el DRP

Un plan de recuperación ante desastres es un proceso para garantizar que pueda volver a poner los servicios en funcionamiento después de una interrupción. El principio consiste en evaluar los escenarios de todos los posibles incidentes y establecer una solución, la mayoría de las veces con la ayuda de un proveedor de servicios. La solución no se detalla en ningún reglamento, pero generalmente consiste en implementar tres copias de seguridad: una en el sitio para reiniciar inmediatamente la actividad en caso de un incidente menor, una en otro lugar, en caso de que el sitio experimente un desastre, y otra en otro lugar en muy diferentes medios, como cintas o discos duros guardados en una caja fuerte. El

plan de recuperación ante desastres también incluye el escenario preciso de reinicio: en TI no basta con tener copias de seguridad, también es necesario saber en qué orden restaurarlas (por ejemplo, no sobrescribir el pedido).

Y pudiéramos alargarnos en torno a recalcar la importancia de entender las diferencias entre RPO y RTO y también ¿Qué debe incorporar su plan de recuperación de desastres? Cloud y Colocation.

Leer también: Elementos críticos de un centro de datos eficiente; ¿Qué es BCP (Business Continuity Plan, Plan de continuidad comercial)? ; Desastres del centro de datos: cómo prepararse para lo peor.