Por qué el plan de recuperación ante desastres ya no debería considerarse una opción para su empresa

Y aquí estamos de nuevo, esta vez para desarrollar los motivos por los cuales el DRP ya no debería ser opcional para su compañía. Vamos con el tema en cuestión.

Las causas de incidentes en la infraestructura del sistema de información pueden ser diversas: fallos de hardware y software, falla de respaldo, ciberataque, error humano, desastre natural, etc. Pero hay una solución para prepararse para ello: el plan de recuperación ante desastres.

Una de cada tres empresas ya ha experimentado un incidente o falla que requirió el inicio de un plan de recuperación ante desastres (estudio Evolve IP, 2015). Como indica Evolve IP, no se trata de saber si el sistema de información de una empresa algún día se encontrará con un desastre, sino de saber cuándo ocurrirá . Y cuando lo haga, ¿estará la empresa preparada para afrontarlo?

Debido a la proliferación de redes informáticas, las empresas deben ahora establecer sus estrategias de protección de datos teniendo en cuenta también los posibles ataques y las frecuentes intrusiones en los sistemas de información (ransomware , cryptolocker, phishing, etc.). La apertura de un mercado de soluciones diseñadas para combatir los ciberataques refleja claramente este problema que se ha convertido en un tema importante para muchas empresas.

En 2021, estos ciberataques ya no deben considerarse epifenómenos en la actividad de una empresa. Sin embargo, el 54% de las organizaciones encuestadas durante el estudio de Evolve IT gastarían menos de $ 50,000 por año en implementar un plan de recuperación de desastres o de continuidad del negocio. Estadísticas que nos indican que el esfuerzo que realizan las empresas para salvaguardar su patrimonio digital, ante lo que puede costarle a una organización la pérdida total o parcial de sus datos , sigue siendo bajo.

¿Qué riesgos corre una empresa sin un plan de recuperación ante desastres ante un desastre?

El 93% de las empresas que perdieron sus datos o el acceso a ellos durante 10 días o más se declararon en quiebra dentro de un año del desastre. Estos datos informados por Continuity Central pueden dar miedo, pero indican concretamente la consecuencia a corto plazo de una interrupción de la actividad o la discontinuidad de los servicios de una empresa. Entonces, ¿cuáles son los riesgos a los que está expuesta una empresa si no ha desarrollado un plan de recuperación empresarial o no ha comenzado a reflexionar al menos en esta dirección?

Los Impactos de una pérdida en la empresa

Los efectos que se sientan serán, en primer lugar, operativos y funcionales. Si no existen medidas para restaurar los servicios, los equipos pueden verse directamente afectados en su trabajo (tiempo de inactividad de la máquina, servidor, acceso a la red, etc.), las herramientas de comunicación internas y externas pueden quedar inutilizables, etc.

Rápidamente, el pulso de la empresa se ralentiza y su actividad, al igual que su visibilidad, puede desaparecer del radar de sus proveedores, socios, clientes y prospectos. En otras palabras, cuanto más corto sea el "período de invisibilidad", menos negativo será el impacto para la empresa.

Desde un punto de vista comercial y financiero, esto puede generar pérdidas en las ventas o en la firma de contratos. Pero también es la pérdida de clientes, o incluso de cuota de mercado lo que se puede observar. Cuanto más corto sea el ciclo de ventas específico del modelo comercial de la empresa, más inmediatas serán las pérdidas desde una perspectiva comercial.

Por el contrario, con un ciclo de ventas medio a largo, es probable que la empresa experimente menos pérdidas directas. Entonces será ella quien restaure sus servicios lo antes posible. Sin embargo, esto podría tener otros impactos, como en la imagen y reputación de la empresa o en la confianza de los socios. Un mercado, un sistema de pago en línea, una plataforma de reserva de habitaciones de hotel podrían hacer que algunos usuarios se muevan hacia nuevos proveedores o se comuniquen negativamente contra el servicio que falla.

¿Cómo prepararse en previsión de un desastre en la actividad de su organización?

Si bien la respuesta tiene múltiples componentes dependiendo de los tipos de desastres, su alcance, la estructura de la organización afectada, es imperativo construir upstream un plan de recuperación del negocio, es decir, recuperación de datos y reactivación de servicios perdidos que serán probados y probados antes de su implementación el día del desastre.

Por lo tanto, el objetivo de una empresa será establecer un plan de recuperación empresarial que, idealmente, debería combinarse con un plan de continuidad empresarial.

Durante el proceso de elaboración del plan de recuperación ante desastres será obligatorio identificar las actividades de negocio consideradas críticas, entrevistar a los responsables de cada actividad, detectar el probable origen de futuros desastres, definir las necesidades humanas y materiales que apoyarán a la implementación del plan, estimar los costos relacionados con la realización y ejecución del plan de recuperación , etc.

Tantos criterios por entender, que serán numerosos y recopilados de manera precisa, promoverán el inicio y la implementación del plan de recuperación de TI por parte de todos los actores involucrados.

Leer también: RPO y RTO: Comprender las diferencias ; Desastres del centro de datos: cómo prepararse para lo peor ; Características de Veeam Cloud backup, para qué sirve, alternativas