Recuperación y protección de datos: ¿su infraestructura crítica es realmente segura?

Las amenazas, tanto virtuales como físicas, han empeorado en los últimos meses y los riesgos siguen acechando. ¿Cómo podemos minimizar su impacto garantizando al mismo tiempo una protección más sostenible de los sistemas y los datos? El punto. Como hemos visto en los últimos meses, ningún sector de actividad se libra de la posibilidad de un ciberataque o un desastre que paralice toda la actividad.

Impacto y consecuencias

El sector bancario, la salud, la energía, los servicios públicos, la educación e incluso los medios de comunicación: todos se ven afectados, con consecuencias a menudo más graves de lo previsto y un proceso a veces laborioso de recuperación ante desastres. La amenaza es tanto virtual como física: ya se trate de ciberataques de tipo ransomware o desastres naturales o técnicos, el daño es grave y compromete la actividad de empresas e instituciones.

Los servidores están paralizados, los datos expuestos, con un impacto en la reputación y rotación de las estructuras afectadas, pero también con graves consecuencias humanas cuando las infraestructuras de sectores críticos son las víctimas. En este contexto donde los riesgos son siempre inminentes, ¿Cómo podemos minimizar el impacto de estos últimos y garantizar una protección duradera de los sistemas y los datos?

Vaya más allá del plan de respaldo

Los desastres y los ciberataques afectan a los datos más esenciales para las empresas y las instituciones públicas. En el caso de los ataques que utilizan ransomware, los delincuentes buscan cifrar los sistemas vulnerables para interrumpir las actividades y exigir el pago a cambio de una clave de descifrado. Sin la protección o la acción adecuadas, las actividades se detienen. Los equipos de TI están sometidos a una presión constante para recuperar los sistemas rápidamente y, en ocasiones, las víctimas prefieren pagar para minimizar el tiempo de inactividad.

En caso de desastres físicos, como cortes o incendios, el costo de recuperar sistemas y compensar los cierres comerciales también puede dispararse muy rápidamente. El ransomware es particularmente letal y crece a una velocidad vertiginosa. Los múltiples ciberataques que han afectado a varios hospitales en los últimos meses han demostrado que los ciberdelincuentes no se detienen ante nada, incluso a costa de graves consecuencias humanas. Este año promete ser como el anterior: seguiremos viendo cada vez más ataques contra infraestructuras críticas, y seguiremos viendo develadas las vulnerabilidades físicas e informáticas de empresas, instituciones y centros de datos.

Alternativas de solución

Para mitigar estos riesgos, es esencial contar con un sólido plan de respaldo y recuperación ante desastres. Los datos deben colocarse fuera de su alcance, en un sistema lo suficientemente fortificado para ser resistente a cualquier tipo de ataque y permitir una rápida recuperación. La estrategia clásica de respaldo es el método 3-2-1: tres copias de los datos en dos medios diferentes y una copia almacenada fuera del sitio. Para maximizar su seguridad, la copia externa debe ser inaccesible desde la red corporativa, ya que algunos

ransomware escanean específicamente en busca de archivos conectados a la red.

Para garantizar el mismo nivel de protección para todas estas copias de seguridad en diferentes ubicaciones y, al mismo tiempo, garantizar la continuidad del negocio en caso de daños, recurra a soluciones de recuperación ante desastres y protección contra ransomware que combinan ciberseguridad, protección y recuperación de datos y cobertura de seguridad para su información en línea y local. La integración de la ciberseguridad con la protección de datos es de hecho una necesidad absoluta en el contexto actual.

Sin embargo, no debemos detenernos allí: una vez que los datos están respaldados y protegidos, es crucial probar regularmente estas copias de seguridad. La calidad de un plan de recuperación depende de la calidad de su copia de seguridad más reciente. Como regla general, se recomienda que ejecute una prueba de recuperación de desastres parcial cada seis meses y una prueba completa cada año. Estas pruebas no solo identifican irregularidades o debilidades, sino que también reducen drásticamente el tiempo que lleva recuperar y proteger los sistemas durante un ciberataque, una interrupción o un desastre físico. Un procedimiento de prueba riguroso es lo que marcará la diferencia en caso de desastre y garantizará una rápida recuperación empresarial.

Continuidad empresarial y protección de datos: la anticipación es la palabra clave

El objetivo de cualquier negocio o infraestructura es limitar tanto como sea posible el tiempo de inactividad del quehacer empresarial después de un ataque o desastre. La mejor forma de hacerlo es ponerse en una lógica de anticipación, en particular creando un plan de intervención que establezca un punto de recuperación con objetivos de tiempo para cada sistema y aplicación en la red.

Dado que no es posible restaurar instantáneamente todos los sistemas en una red, es esencial construir una lista de aplicaciones y sistemas prioritarios para restaurar con anticipación con el fin de ganar eficiencia y claridad durante el proceso de recuperación, permitiendo así reducir el impacto negativo de apagar sistemas críticos. Si bien la posible pérdida de datos no es una amenaza tan inmediata para las empresas y la infraestructura como el cierre de operaciones críticas, sus implicaciones pueden ser graves.

Por lo tanto, la copia de seguridad de los datos es una prioridad alta y debe anticiparse junto con la continuidad del negocio, especialmente porque el acceso a estos datos puede

respaldar los procesos de recuperación. Por lo tanto, los datos deben almacenarse fuera y en el sitio, de acuerdo con la legislación vigente. La implementación de protocolos de ciberseguridad que incorporan protección de datos permite un proceso de recuperación mucho más fluido. El objetivo final es reducir tanto como sea posible el tiempo entre un desastre o la detección de un ataque y el inicio del proceso de recuperación para limitar el impacto en los sistemas y aplicaciones críticos.

En un contexto en el que muchos sectores de actividad han visto recortados sus presupuestos debido a la actual pandemia, este enfoque es también uno de los más rentables financieramente. La dinámica de transformación digital en la que nos encontramos ha propiciado una proliferación de datos y la digitalización de muchos procesos dentro de todos los sectores de actividad. Esta tendencia también ha ampliado enormemente el alcance del riesgo, tanto en términos de pérdidas físicas como de ciberataques.

Ciertos sectores son actualmente particularmente vulnerables y los acontecimientos recientes han demostrado la necesidad de anticiparse constantemente a estos riesgos y dotarse de medios concretos para minimizar su impacto. Los profesionales de TI, especialmente aquellos que trabajan en infraestructuras críticas, necesitan tener la mejor formación, la mejor información y las mejores herramientas posibles para comprender los riesgos y establecer un plan de acción eficaz.

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