Cómo Responder al Tiempo de Inactividad: Cinco Estrategias Clave

Cómo responder al tiempo de inactividad: cinco estrategias clave

El espacio de la protección de datos sigue evolucionando a medida que las organizaciones se enfrentan a una "tormenta perfecta" de desafíos que golpea a sus infraestructuras de TI. Esta "tormenta" afecta la capacidad de los equipos de TI de operar con eficacia, y coloca a los responsables de la toma de decisiones económicas en un dilema a la hora de asignar los presupuestos. No es ninguna sorpresa que muchos líderes de TI se quedan despiertos por la noche con una larga lista de preocupaciones:

- Crecimiento interminable de datos estructurados y no estructurados
- Explosión de ataques de malware/ransomware
- Mayor necesidad de demostrar el cumplimiento y la propiedad de los datos
- Infraestructuras inconsistentes de protección de datos para usuarios finales más grandes
- Mayor complejidad causada por la combinación de soluciones mal integradas
- Falta de control sobre métricas clave, tales como RPO y RTO
- Erupción de la virtualización y el papel del almacenamiento basado en la nube

Para agravar estos desafíos, muchas organizaciones están poniendo la carga de administrar soluciones de TI complejas sobre los hombros de una persona con conocimientos generales de TI, que muchas veces requiere de soluciones menos complejas y de menor costo para proteger, administrar y acceder a los datos críticos. Es por esto que esas organizaciones necesitan reconsiderar cinco estrategias clave que pueden fortalecer su capacidad para responder durante el tiempo de inactividad.

1 Gestión de riesgos: la estrategia actuarial orientada a la protección de datos

Hoy, la mayoría de las organizaciones deben (o al menos, deberían) contar con planes de recuperación de desastres o disponibilidad de datos. Sin embargo, muchos de estos planes se crearon en una era informática diferente y no abordan el retorno de la inversión (ROI) y los ahorros reales de costos que necesitan los líderes empresariales de TI cuando evalúan sus inversiones actuales. Ahí es donde la estrategia actuarial se orienta a la protección de datos.

Las organizaciones de hoy deben ser capaces de acceder a los datos críticos, cuándo y dónde se necesitan. Cada vez que un líder de TI mejora la resiliencia de la infraestructura de TI, el negocio ahorra costos, reduce el riesgo y la pérdida de forma significativa, y mejora la eficiencia operativa. La razón se deriva de los aspectos económicos del backup y la recuperación, o más específicamente, del costo de la disponibilidad de las aplicaciones y los datos, que puede cuantificarse midiendo los costos directos e indirectos, tales como el impacto en la reputación, la pérdida de clientes o su incapacidad para hacer una compra, las multas cuando se producen situaciones regulatorias y la productividad de los empleados. Al adoptar un enfoque más actuarial en torno a la disponibilidad de datos y sistemas, podrá determinar:

- La expectativa de pérdida en base a la probabilidad estadística
- Cómo afectaría un desastre natural a los recursos actuales y el costo de volver a operar

- El riesgo de malware/ransomware que afecta a los sistemas críticos, y el costo y plazo de tiempo que se necesitaría para recuperar los datos, ya sea pagando o no un rescate
- Cómo la empresa podría proporcionar sus productos y/o servicios, y qué procesos son necesarios para asegurar que la productividad de los empleados o que el volumen de ventas no se vean afectados
- El efecto monetario de un punto de venta o sitio de comercio electrónico que se cae durante 5 minutos, 15 minutos o más. Dependiendo del modelo de ventas, perder la capacidad de realizar transacciones en línea durante más de unos segundos puede significar una pérdida masiva de negocios

Este enfoque actuarial, o más económico, para el backup y la recuperación, permite a una organización construir un modelo que convierte los costos por la expectativa de riesgo y pérdida incidental en números reales. A su vez, el negocio puede priorizar de manera más efectiva las áreas de debilidad más críticas y asignar sus inversiones en consecuencia.

2 Disponibilidad de los sistemas: no todos los datos se crean de la misma manera

Es de común conocimiento que la mayoría, si no todas las empresas, no funcionarían sin el correo electrónico o las aplicaciones transaccionales críticas, que literalmente hacen funcionar al negocio o permiten a los clientes comprar productos y/o servicios. Tampoco se necesita un científico espacial para entender que la protección de estos sistemas y datos es clave para sobrevivir a los tiempos de inactividad no planificados. Dicho esto, hay mucho más de lo que parece, dado que estos sistemas y aplicaciones están casi siempre entrelazados, más o menos exitosamente, y tendrán diferentes niveles de criticidad.

A medida que los equipos ejecutivos revisan sus estrategias de disponibilidad actuales y a futuro, es importante tener en cuenta algunas áreas clave:

- La criticidad de las aplicaciones específicas: cuando se trata de ello, la verdadera pregunta debería ser, "¿qué tan rápido necesita acceder a los datos específicos?". Los folletos de marketing y las aplicaciones internas de uso compartido de archivos suelen soportar unas pocas horas de inactividad, mientras que los sistemas transaccionales suelen ser críticos y deben estar disponibles en cuestión de segundos. El impacto financiero en sistemas específicos puede modelarse con el enfoque de gestión de riesgos mencionado anteriormente
- Interdependencia de aplicaciones y sistemas: normalmente, la mayoría de las aplicaciones se combinan o integran en una cadena de valor o flujo de trabajo, por ejemplo órdenes EDI que alimentan toda una cadena de suministro. A esta complejidad se suma el hecho de que estas aplicaciones suelen ser monitoreadas en silos, lo que impacta en el desempeño y hace más difícil administrar toda la infraestructura. ¿Cómo impactaría la caída de un sistema en otros? Es importante entender el grado de interdependencia dentro de su organización y el impacto resultante en todo el ecosistema de TI
- Planes de mantenimiento y disponibilidad: cada aplicación tiene diferentes horarios de mantenimiento y requisitos de nivel de servicio. En base a esto, es importante determinar la rapidez con la que podría acceder a datos críticos específicos. Muchas soluciones son más o menos genéricas, requieren actualizaciones pesadas o añadir otras soluciones puntuales a medida que evolucionan las necesidades del negocio. Tenga esto en cuenta al prever futuras dependencias o cambios en su infraestructura

Al considerar estas áreas clave, podrá determinar su índice de disponibilidad de datos y cualquier posible brecha en el flujo de trabajo o la cadena de valor de las aplicaciones que hacen funcionar a su negocio, y actuar en consecuencia.

3 Complejidad: más procesos, más problemas

Los puntos anteriores sobre la disponibilidad de datos han descubierto al verdadero culpable de impedir que las organizaciones logren una continuidad del negocio eficiente: la complejidad de la infraestructura de TI y, más precisamente, de sus soluciones de protección de datos. El desafío, y el objetivo principal subyacente, es obtener un nivel de previsibilidad y consistencia de la recuperación, independientemente de lo que haya causado la interrupción que inevitablemente afectará a todas las infraestructuras. Los líderes de TI y los ejecutivos de negocios necesitan abordar este desafío desde una perspectiva de resultado neto, considerando los RPO y RTO reales, y determinando cómo hacer que el negocio se recupere en un plazo que cumpla con las exigencias. Específicamente, esto significa organizar la recuperación o el failover de sistemas críticos de una manera que produzca resultados predecibles.

Desafortunadamente, esto es casi imposible si una empresa utiliza varias soluciones o procesos separados de backup que no están bien organizados. Unificar su infraestructura de backup, recuperación y disponibilidad de datos, ya sea en forma local o con la ayuda de destinos en la nube, es la única manera de probar exitosamente sus planes y garantizar una ejecución efectiva si se produce una interrupción.
En última instancia, la menor complejidad introducida en los procesos de backup y recuperación le dará más control sobre los RPO y los RTO.

1 http://finance.yahoo.com/news/victims-paid-more-24-million-222700088.html

2 https://www.justice.gov/criminal-ccips/file/872771/download

4 Ransomware: no es un problema de seguridad, es un problema de recuperación de datos

El Internet Crime Complaint Center informó que, sólo el año pasado, los eventos de ransomware costaron USD 24 millones a las organizaciones estadounidenses[1], y según el Departamento de Justicia, los ataques de ransomware han aumentado un 300% hacia 20162. Estas estadísticas subrayan un creciente problema que afecta a negocios de todos los tamaños, uno que los ejecutivos de la compañía no pueden ignorar, y que inevitablemente recaerá en TI para su resolución.
A diferencia de otros eventos lógicos de interrupción de datos, el ransomware también puede provocar un impacto muy alto en la reputación. Una mirada al reciente incidente que involucró a Delta Air Lines ilustra no sólo el alto costo del rescate, sino el impacto en la confianza del cliente, que a menudo es el resultado más perjudicial.

La mejor estrategia para mitigar el daño de un evento de ransomware es ser proactivo, en lugar de reactivo. Al dar espacio a su organización para que tome sus propias decisiones, eliminará la necesidad de negociar con los hackers la posibilidad de que el ransomware se propage e infecte los datos críticos del negocio.
Una manera extremadamente eficaz de lograr esto es mediante la implementación y las pruebas periódicas de una solución de recuperación robusta con opciones tradicionales y en la nube que le permitan “volver atrás el reloj” y restaurar datos sensibles para la empresa, sin necesidad de un rescate.

La mayoría de las veces, el ataque del ransomware es la mayor amenaza para las organizaciones; sin embargo, ofrece a las empresas la oportunidad de reevaluar las estrategias de continuidad del negocio y recuperación de desastres para garantizar que no se haya pasado por alto ningún área. Al combinar una sólida solución de detección de amenazas y erradicación de malware con un sólido plan de disponibilidad de datos, las organizaciones están bien posicionadas para superar un evento de ransomware y la multitud de daños que puede causar.

5 Confiando en la nube: cómo y cuándo tiene sentido para su infraestructura

Mucho se ha escrito sobre el uso de servicios en la nube para complementar o, incluso, reemplazar las infraestructuras tradicionales de backup y recuperación. Sin embargo, hay muchas cosas a tener en cuenta a la hora de evaluar cómo y cuándo introducir un componente de nube. Entre estas, los líderes de TI y de negocio deben considerar:

- El tipo real de servicio, ya sea backup como un servicio (BaaS), recuperación de desastres como un servicio (DRaaS) o hosting de datos/flujos de trabajo
- Cómo pasar de una solución de continuidad del negocio/recuperación de desastres a una infraestructura más híbrida, que incluya el tipo de almacenamiento en la nube (disco, cinta o una combinación de ambos), la necesidad de archivado, el mecanismo de obtención y recuperación de datos (cómo llevar sus datos a la nube y viceversa), y la flexibilidad de los costos

Más importante aún, estas consideraciones deben abordarse en el contexto de los requisitos originales de RPO y RTO. Otras áreas de discusión incluyen las instalaciones y ubicaciones del proveedor, las cuales deben considerarse cuidadosamente tanto desde el punto de vista del cumplimiento como del de una zona potencial de impacto de desastres (por ejemplo, tener datos y sistemas de failover “en otra región” es una práctica recomendada).

Conclusión

La mayoría de las organizaciones entienden la urgencia de mantener la resiliencia del sistema y garantizar la disponibilidad de datos frente a amenazas que están en constante evolución. Fundamentalmente, se trata de resolver una ecuación compleja: ¿qué niveles de servicio necesito desde una perspectiva de RPO y RTO, y qué inversiones debo hacer para obtener esos resultados y maximizar el retorno de la inversión?

Las organizaciones que confían en las estrategias de mitigación de riesgos, las respuestas proactivas ante el ransomware, la disponibilidad de datos para ecosistemas de sistemas, la simplificación de procesos y el papel de la nube, estarán bien posicionadas para satisfacer cualquier demanda del negocio.

Así, mientras que la “tormenta perfecta” que está golpeando a muchas infraestructuras de TI es, sin duda, una causa de preocupación, también representa una oportunidad para que la continuidad del negocio y la recuperación de desastres formen parte de la conversación a nivel ejecutivo. Así, la pérdida de datos dejará de ser solamente una preocupación de TI para pasar a ser una preocupación del negocio.

Para obtener más información sobre Arcserve, visite arcserve.com/la