Cinco beneficios de la protección de datos moderna para las empresas

Las empresas están acelerando su transición a implementaciones de nubes públicas, privadas e híbridas. Al mismo tiempo, la información digital está creciendo rápidamente y las empresas dependen cada vez más de los sistemas digitales para todos los aspectos de sus operaciones. Esto está creando un entorno en el que la protección de datos debe ser la máxima prioridad para los líderes empresariales.

Las empresas dependen de sus datos e información hoy más que nunca. Como pilar empresarial de misión crítica, el almacenamiento y la protección de datos deben formar parte de los planes estratégicos y de mitigación de riesgos de la empresa. Implementar las medidas adecuadas para administrar los datos puede ayudar a las organizaciones a proteger este valioso activo. No hacerlo podría poner en riesgo el negocio.

Ante este panorama Pure Storage destaca los cinco beneficios clave para las empresas que aprovechan la protección de datos moderna:

1. Ahorro general de costos

Los ciberataques podrían costar a la economía mundial millones de dólares y tener impacto directo en una cantidad significativa de puestos de trabajo. Las empresas afectadas sufren pérdidas debido a la pérdida de clientes, la pérdida de productividad, los costos directos de reparación y los costos que conllevan el daño a la reputación si la violación de datos se hace pública.

Las empresas afectadas por una violación de datos tienden a sufrir caídas inmediatas en el precio de sus acciones y, lo que es más preocupante, el precio de las acciones puede seguir viéndose afectado a largo plazo.

Al realizar copias de seguridad de los datos en la nube y distribuirlos entre más servidores dentro y fuera de las instalaciones, las organizaciones pueden mitigar el riesgo que representan los ataques de ransomware. Al garantizar que los datos estén protegidos por controles de seguridad adecuados, pueden minimizar las posibilidades de una violación cibernética.

Como un bono de ahorro de costos, esto también puede mejorar la escalabilidad cuando las organizaciones crecen y deben almacenar más datos, porque la facilidad de escalabilidad en sí ayuda a ahorrar costos.

2. Resiliencia operativa

Las organizaciones con múltiples servidores tanto dentro como fuera de las instalaciones para su almacenamiento de datos en la nube deben ser operativamente resistentes. Esto requiere una protección de datos sólida en todos los servidores.

La mayoría de los consultores de TI le dirían a las organizaciones que mantengan los sitios relativamente cerca unos de otros por razones de rendimiento, pero esto no siempre es así o es

tan fácil.

Un desastre que afecte a un centro de datos podría afectar fácilmente a otros cercanos, por lo que en algunos casos puede ser aconsejable elegir centros de datos geográficamente dispares.

3. Mayor capacidad para aprovechar los datos para obtener información y tomar decisiones.

Los datos mejor protegidos incluyen detener la pérdida de datos y las interrupciones en el almacenamiento de datos. Si los datos de una organización siguen siendo interrumpidos por falta de protección, esto podría conducir a un análisis de datos deficiente. La calidad de los conocimientos derivados de los datos está directamente relacionada con la calidad de los datos en sí. Por lo tanto, proteger los datos es esencial para mantener conocimientos y toma de decisiones de alta calidad.

4. Protección contra ataques de ransomware

Durante 2020, los ataques de ransomware aumentaron un 715 por ciento interanual.1 Para evitar esto, las organizaciones deben implementar una postura proactiva contra los ciberataques a través de medidas como la capacitación del personal, la búsqueda de amenazas y el monitoreo proactivo de redes y terminales.

La creación de un espacio de aire para el entorno de la copia de seguridad puede ayudar a protegerse contra los ataques de ransomware en la copia de seguridad. Estos ataques todavía ocurren y pueden paralizar una empresa. Esto se puede solucionar agregando instantáneas de SafeMode para proteger los datos de respaldo.

En caso de cualquier ataque de ransomware, las organizaciones pueden recuperar datos directamente de estas copias de seguridad protegidas. Esto también ayuda a protegerse contra administradores deshonestos.

5. Cumplimiento de las leyes de privacidad de datos

Las organizaciones deben cumplir con la Ley de privacidad y la política de violación de datos notificables. Esta ley describe cómo las organizaciones deben recopilar, mantener, usar y eliminar datos. Las organizaciones podrían enfrentar sanciones y multas si no cumplen. El cumplimiento reducirá el riesgo de que la empresa sufra una violación de datos y posicionará a la empresa como líder en el mantenimiento de la privacidad de los datos de los clientes.

La protección y el almacenamiento de datos efectivos son lo que está en juego en un mundo que depende cada vez más de los datos. Las organizaciones que adoptan un enfoque moderno y proactivo de la gobernanza de datos obtendrán importantes beneficios que las posicionarán para liderar el mercado no solo ahora, sino también en el futuro.