Cuatro formas de proteger sus datos para una recuperación limpia y confiable

Los datos son vulnerables a innumerables amenazas, desde ataques cibernéticos y fallas de hardware hasta desastres naturales. Una estrategia de copia de seguridad robusta y multicapa protege sus datos, garantiza la continuidad del negocio, reduce el riesgo de pérdida de datos y fortalece su postura general de seguridad.

Estas son cuatro medidas para mejorar la postura de seguridad que ayudan a garantizar que sus datos siempre estén limpios y sean recuperables.

1. Implemente el control de acceso y la autenticación

- **Asegúrese de que solo los usuarios autorizados puedan acceder a sus datos.** Agregar una capa adicional de seguridad es esencial para la protección contra amenazas internas y externas. Habilitar la autenticación multifactor (MFA) en todas partes es un medio eficaz para protegerse contra estas amenazas, junto con el mantenimiento de sus políticas existentes de gestión de identidad y acceso.
- **Limite el acceso y los permisos según los roles de usuario.** Aplique el control de acceso basado en roles (RBAC) para proporcionar acceso y permisos limitados y granulares para los usuarios en su entorno de copia de seguridad en función de su rol específico. Esto ayuda a garantizar que cada persona tenga solo los privilegios mínimos de acceso necesarios para cumplir con sus responsabilidades.

2. Priorice la protección y la integridad de los datos

- **Implemente una bóveda de datos inmutable.** Para mantener sus datos a salvo de la manipulación, considere usar Cohesity NetBackup Flex Appliance o Cohesity FortKnox para un almacenamiento inmutable seguro y resistente a la manipulación en las instalaciones o en la nube.
- Implemente una estrategia de copia de seguridad 3-2-1 para cargas de trabajo críticas. Mantener tres copias de datos en dos medios diferentes, con al menos una copia almacenada fuera del sitio en un almacenamiento inmutable e indeleble, proporciona redundancia de datos y ayuda a garantizar que sus datos siempre sean recuperables.
- Evite la filtración de datos mediante un cifrado robusto. Proteja los datos del acceso no autorizado durante la transmisión y el almacenamiento. Para evitar el acceso no autorizado y el robo de datos, utilice un cifrado robusto para todos sus datos, ya sea que se almacenen en las instalaciones o en la nube.

Estrategia de copias de seguridad 3-2-1

3. Aproveche el monitoreo y la detección de seguridad

- Utilice la automatización para la detección inteligente de amenazas de usuarios. Nuestro motor de riesgo adaptativo monitorea continuamente el comportamiento del usuario para detectar actividades sospechosas. Al detectar anomalías u otras acciones sospechosas del usuario, la plataforma iniciará de forma autónoma acciones de seguridad, como la autenticación multifactor, para bloquear el acceso a los datos de respaldo.

- Acelere la identificación y respuesta a amenazas. Cohesity proporciona capacidades rápidas de búsqueda de amenazas que buscan proactivamente indicadores de compromiso y responden a las amenazas. También ofrecemos un análisis completo del radio de impacto de las áreas afectadas en todo el entorno, hasta un 93 % más rápido que el escaneo de malware tradicional.

4. Refuerce la configuración de su sistema

- **Cree una Digital Jump Bag.**™ Una Digital Jump Bag es un repositorio protegido y confiable que proporciona acceso rápido a las herramientas necesarias para la adquisición y el análisis remotos. Contiene las herramientas, el software, los archivos de configuración y la documentación necesarios para responder a un incidente en un almacén inmutable y resguardado, más allá del alcance de los adversarios.
- **Reduzca la exposición de la red**. Implemente controles de acceso a la red para restringir el acceso a la red a los sistemas y datos de respaldo y evitar el acceso no autorizado. Segmente fácilmente su red y cree un entorno de sala limpia para mejorar la seguridad y ayudar a minimizar el impacto de cualquier posible violación de seguridad.
- **Implemente la recuperación de datos de la sala limpia**. Cree un entorno separado y seguro para las operaciones forenses y de recuperación a fin de minimizar el riesgo de contaminación.
- **Mantenga actualizados todos los sistemas y software**. Actualice regularmente el software e instale parches de seguridad para aprovechar las nuevas características y las medidas de seguridad mejoradas.

Comparta estas pautas con su equipo y aliéntelos a implementar estos pasos cruciales para proteger los datos de su organización y fortalecer su postura de seguridad.

Para obtener planos y mejores prácticas para diseñar un entorno de copia de seguridad para su organización, lea *Topologías modernas de seguridad y gestión de datos: Una guía para líderes de TI*.

COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

9100085-001-EN 6-2025