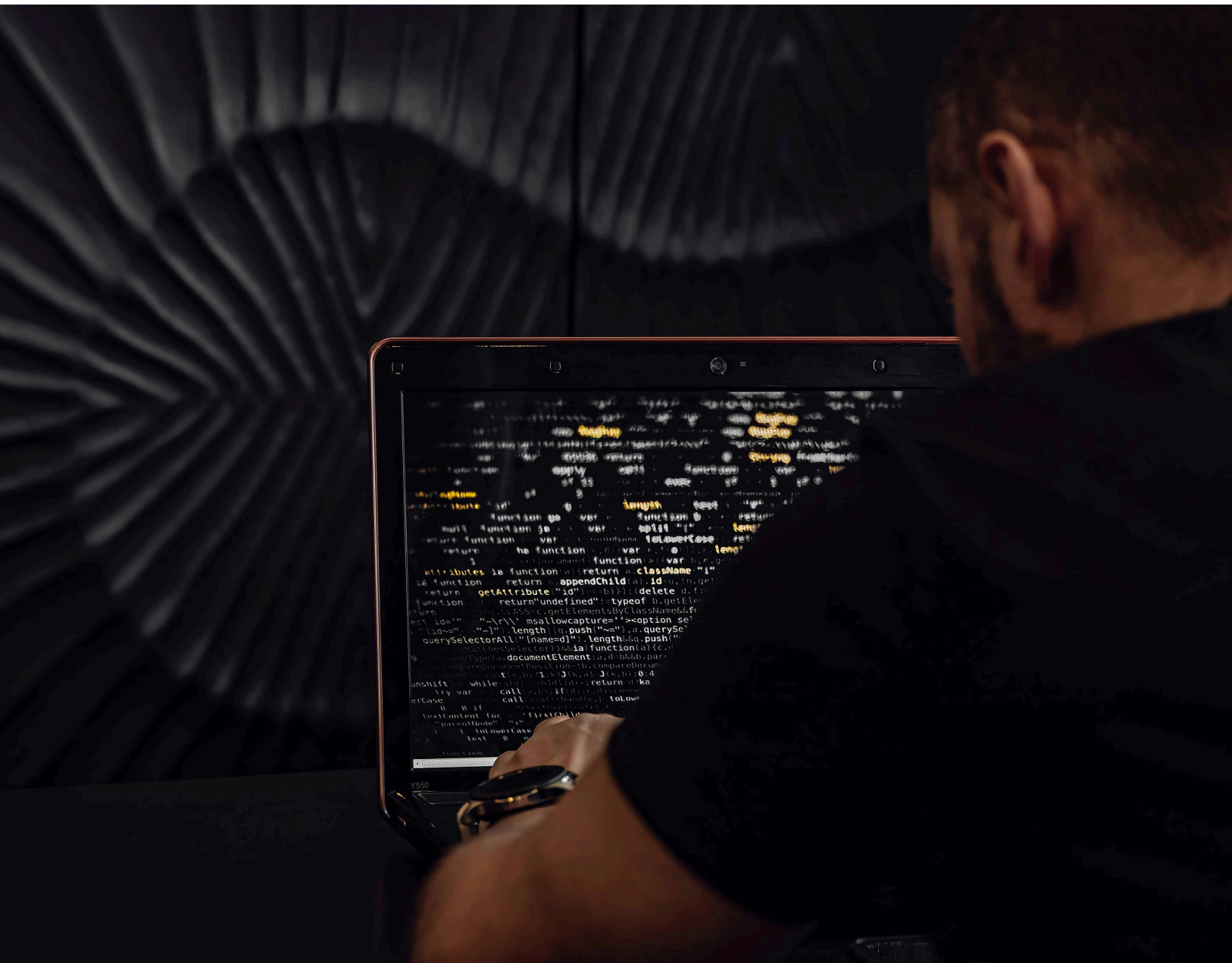



La rotación excesiva en ciberseguridad está dejando brechas en los planes de recuperación ante desastres



44

Desde el comienzo de la pandemia, los departamentos de TI han agudizado su enfoque colectivo en la ciberseguridad. Han duplicado las medidas de protección para evitar que los hackers les roben sus datos y lancen cantidades récord de ataques de **ransomware**. En el proceso, es posible que muchos hayan perdido de vista a otras amenazas que pueden causar tanto daño como los ataques cibernéticos.





El error humano sigue siendo la causa más común de pérdida de datos. **Estudios demuestran que las organizaciones pierden casi 5 veces más datos mediante eliminaciones y sobreescrituras accidentales que a través de incidentes maliciosos.** Los errores accidentales de configuración y administración de aplicaciones y usuarios también pueden bloquear los sistemas, borrar datos y causar costosas interrupciones.

Los desastres naturales son un problema creciente. En los últimos dos años se ha incrementado el número de tormentas tropicales que han azotado México, así como Estados Unidos, y los expertos esperan que el cambio climático causará más y más daños. Tan sólo los impactos financieros provocados por el huracán Ida (que también cruzó la República Mexicana), costaron a las empresas, consumidores y comunidades **\$100 millones de dólares** en el vecino país del norte.

Si bien se justifica una mayor atención a los ataques cibernéticos, las organizaciones deben volver a priorizar sus estrategias de recuperación ante desastres (DR, por sus siglas en inglés) para cumplir con el panorama de amenazas reales que vemos hoy. Si

no lo hacen, sus operaciones sufrirán: según un informe de UniTrends[1] (con información de la Universidad de Texas), el 94% de las compañías que experimentan una pérdida de datos catastrófica no sobreviven; el 43% nunca vuelven a abrir y más de la mitad (51%) cierran en el lapso de dos años.

Los que permanecen en el negocio tienen pérdidas en ingresos y productividad por \$84,650 dólares por hora, según el Reporte de Protección de Datos Veeam 2021, y pierden más que eso: experimentan impactos externos, incluida la pérdida de confianza del cliente y el daño a la marca; impactos internos, como la moral de los empleados lastimada y la desviación de recursos, e impactos pertenecientes a un tercer grupo de factores, litigios y regulaciones, que pueden tener un efecto significativo en la valoración de la empresa.

A continuación, un recuento de tres acciones necesarias:

1. Invertir en la formación de empleados, un buen punto de partida

Cualquier compañía que no haya implementado una nueva ronda de capacitaciones en ciberseguridad para los trabajadores durante la pandemia debería hacer de esto una máxima prioridad, incluyendo las me-

jores prácticas habituales que van desde seguir los procedimientos de notificación de incidentes hasta seleccionar contraseñas seguras para evitar las estafas de phishing. Pero la formación también debería extenderse a los operadores de TI. Los errores de configuración se pueden reducir siguiendo una serie de mejores prácticas, como la creación de una única fuente de configuración, que brinda una manera fácil de hacer seguimiento de los cambios de configuración y el uso de nombres de servicio DNS para todos los servicios. Como no hay forma de probar todas las condiciones imaginables, habrá errores de aplicación, pero revisar y actualizar los procedimientos de prueba regularmente puede mejorar el rendimiento y reducir la cantidad de fallas por descuido en la práctica diaria.

2. Automatizar funciones en el proceso de DR, prioridad al salir de la pandemia

La automatización no sólo reduce los errores humanos en procedimientos cotidianos, sino que da más tiempo al personal para hacer tareas más estratégicas y de mayor nivel. Esto es tan cierto para TI como para los que están en la oficina. Las inversiones en tecnologías de automatización aumentaron en los últimos dos años, y deben seguir haciéndolo para mejorar la productividad y proveer niveles de seguridad más altos.

La automatización del proceso de DR en particular puede ahorrar tiempo y mejorar la respuesta general. Las aplicaciones y conjuntos de datos actuales son más grandes y complejos, distribuidos e interdependientes que nunca. Esto hace que la recuperación exitosa, incluso de una sola aplicación (sin mencionar sitios completos), sea increíblemente difícil, así que la orquestación de procesos de recuperación es una herramienta indispensable.

3. Asegurar que los planes y procesos de DR están listos para manejar incidentes repentinos e imprevistos que amenacen con la continuidad de los negocios

Por todo lo que está en juego, es buen momento para examinar más de cerca los planes y procedimientos. Aquí algunos consejos a seguir:

- **Verificar los detalles:** es fundamental tener un plan actualizado y validado para las necesidades de negocio específicas de una corporación. Probablemente, las necesidades hayan cambiado desde que comenzó la pandemia; si no ha revisado su plan en más de un año, debería ser una prioridad.
- **Revisar la documentación:** tener documentos completos y fáciles de seguir disponibles durante las restauraciones del sistema puede ahorrar tiempo y evitar el estrés. Estos requieren mucho tiempo para crearlos, y deben revisarse continuamente, de preferencia por las personas que usarán los documentos cuando sea momento de desempolvarlos.



- Actualizar los accesos de identidad: con los cambios en el consumo de servicios, es probable que se hayan desarrollado brechas desde el punto de vista de la confirmación de la identidad. Asegúrese de que las personas adecuadas estén autorizadas para realizar funciones críticas del sistema durante ese periodo urgente cuando los sistemas no funcionan.

- Repensar los planes de DR/resiliencia: con un mayor uso de dispositivos externos, las empresas deben racionalizar sus planes para incorporar protección de extremo a extremo, desde la fuerza laboral hasta el punto final.

- Hacer pruebas de aceleración: pruebe cada aplicación individualmente para asegurarse de que cumplen con sus métricas clave, sobre todo el objetivo de tiempo de recuperación (RTO) y el objetivo de punto de recuperación (RPO).

En conclusión

Los ciberataques van en aumento, y las organizaciones deben dedicar mucha atención para protegerse contra ellos. Pero los desastres se presentan en varias formas. Para garantizar que estamos protegidos cuando uno llegue, las áreas de TI requieren asegurarse de que sus planes y procedimientos de recuperación están en su lugar. Sus negocios dependen de ello.

Autor: –Rick Vanover, director Senior de Estrategia de Producto de Veeam, y Dave Russell, vicepresidente de Estrategia Empresarial en Veeam.