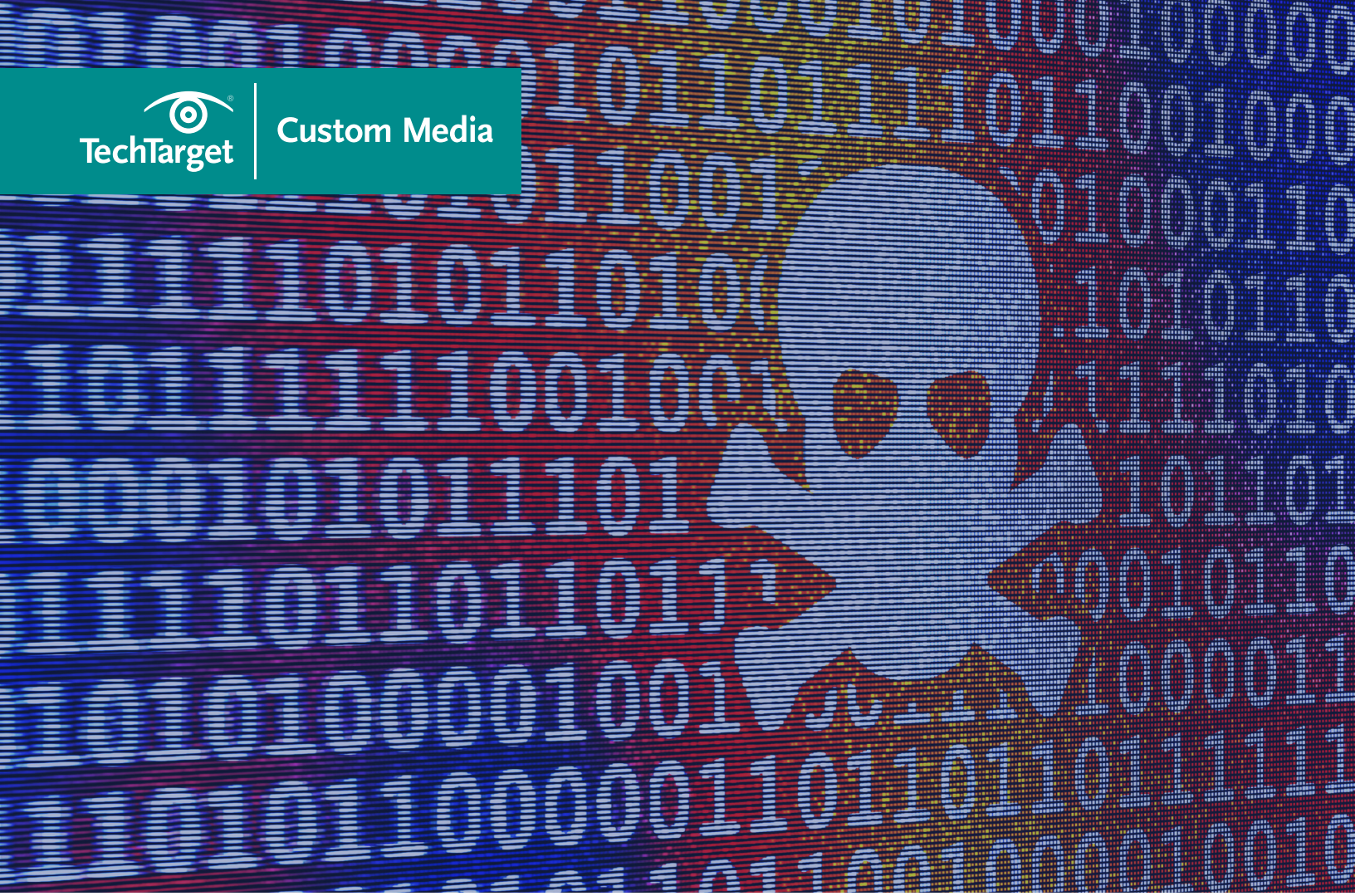

TechTarget | Custom Media

Un nuevo enfoque para defender su red contra el ransomware

Por David Strom

Defender su red y evitar que sus usuarios se infecten con ransomware significa mucho más que solo implementar varios firewalls y sistemas de prevención de intrusos en la red. Se trata de crear una cultura de lo que Rick Vanover, director de estrategia de productos para Veeam Software, denomina ser resiliente. Se trata de desarrollar un proceso de backup y recuperación coordinado que cubrirá sus sistemas y sus activos de datos, para que estén protegidos cuando ocurra un ataque y su negocio pueda regresar a un estado operativo de la manera más rápida y económica posible. Vanover compartió algunos de sus consejos para hacer que sus sistemas sean más resilientes.

Afirma que, tradicionalmente, los backups "fueron la parte aburrida de administrar un centro de datos". "Pero eso está cambiando, en particular porque el almacenamiento es económico y el costo de oportunidad de la pérdida de datos es caro. Sus datos son valiosos y necesita protegerlos de la manera correcta". Estos son algunos de sus consejos sobre cómo volverse más resiliente en la lucha contra el ransomware y para la consolidar sus procesos de backup y recuperación.

VEEAM

“Me rompe el corazón ver cuántas empresas no prueban sus planes de recuperación de manera regular”.

En primer lugar, comprenda qué puede automatizar en el proceso de recuperación, o qué puede automatizar mejor. “Escuché que una organización, que no usaba nuestro software, pagó el rescate en vez de tratar de recuperar sus datos. Evaluaron que sería más rápido y menos costoso pagar el rescate”, menciona Vanover. Esa no debería ser la decisión. En su lugar, comprenda cómo se necesitan sus backups y cómo se pueden organizar de la manera más apropiada para reducir el tiempo de recuperación general.

No confunda reparar una máquina con restaurar sus datos. “La única manera de recuperar sus datos después de un ataque es mediante un proceso de restauración. Nunca es una buena idea reparar los sistemas de manera individual”, afirma Vanover. “No puede garantizar que los hackers vayan a entregar realmente una reparación como lo prometieron. Después de todo, usted está tratando con desconocidos y existe un riesgo al trabajar con esta clase de personas. Puede que su solución no esté completa o no pueda deshacer completamente sus problemas y devolverle sus datos perdidos”. La única opción segura es usar las opciones de recuperación.

¿Cómo sabe cuándo tiene datos críticos a los que no se les realiza un backup? Por este motivo, necesita **probar sus procedimientos de recuperación con frecuencia**. “Me rompe el corazón ver cuántas empresas no prueban sus planes de recuperación de manera regular. Algunos solo lo hacen anualmente, les compran pizzas a todos y aceptan la cantidad de fallas como parte del costo de hacer negocios. Eso no es suficiente, tiene que poner mucho más esfuerzo en las pruebas regulares de su proceso de recuperación de datos. Siempre veo un momento de iluminación, cuando mis clientes comprenden finalmente lo que es importante. Si pueden aprender a realizar una recuperación rápidamente, pueden ahorrar mucho tiempo cuando realmente tengan que recuperarse de una filtración o un ataque. Se trata más sobre educación que un problema técnico”, explica. Vanover recomienda que las organizaciones prueben los procedimientos de recuperación a diario, o al menos todas las semanas. Menciona que Veeam tiene un proceso de verificación de recuperación automatizado que ha sido parte de su producto por más de siete años.

Sepa cuándo sus sistemas no realizan backups, o qué sucede cuando los sistemas cambian. Vanover cuenta la historia sobre un Windows Server que tuvo un cambio de registro, pero recién tuvo efecto cuando se reinició el sistema, y luego no inició. “Si sus backups solo sirven para las últimas tres semanas, y ha pasado más tiempo desde que reinició ese sistema, no tiene un backup sólido para la recuperación. En estas circunstancias, un problema pequeño se puede convertir en un problema mayor al tratar de restaurar ese sistema”.

Parte del problema es que nuestros entornos informáticos cambian constantemente.

Una de las formas de probar los cambios para los sistemas de producción es mediante el uso de la característica Veeam Virtual Lab. Los clientes pueden ver cuáles son las implicaciones de cualquier cambio en sus procedimientos de backup y restauración, y hacerlo de manera fluida y no destructiva, que no desconectará los sistemas mientras se realizan las pruebas. “Vimos cómo los clientes usan los virtual labs para probar varios problemas de seguridad”, afirma Vanover. “Como usar un rango cibernético, para ver el impacto y los riesgos que suceden cuando se implementa un cambio. Por ejemplo, muchas veces es difícil evaluar si un servidor de SQL puede recibir ataques de inyección, y nuestro virtual lab puede ilustrar los posibles riesgos.

Parte del problema es que nuestros entornos informáticos cambian constantemente. Al ejecutar servidores en la nube y trabajar en dispositivos móviles, es fácil ver que la cantidad de datos es muy dinámica estos días. Vanover recomienda usar un proveedor de backup que tenga **informes programados con frecuencia que les diga a los administradores de la red a qué no se le realiza un backup**, para que puedan tomar las medidas correspondientes.

Asegúrese de que tiene todo lo que necesita para una recuperación completa. Algunas organizaciones operan un sitio informático ante desastres completamente distinto, mientras otras emplean proveedores de servicios administrados que se especializan en esta clase de protección basada en la nube. “Muchas personas no planean una experiencia completa de recuperación ante desastres”, explica Vanover. “No comprenden lo

“En algunas ocasiones, no quiero restaurar el sistema completo, tan solo un conjunto en particular de datos relevantes a una sola aplicación.”

que realmente se requiere para proporcionar todas sus aplicaciones, servidores y datos”. En algunas ocasiones, las organizaciones no realizan un inventario completo de todos sus activos digitales, y solo encuentran las brechas cuando llega el momento de recuperar un servidor perdido al que no se le efectuó un backup de manera correcta. “Incluso las organizaciones que solo tienen un único centro de datos pueden sufrir este problema,” afirma. “Pueden depender de servidores de aplicación fuera de línea o algo fuera de su centro de datos para sus operaciones. Necesitan administrar correctamente sus aplicaciones”.

Comprender esta situación se trata de **hacer coincidir las aplicaciones con sus necesidades de datos** y poder recuperar exactamente lo que cada aplicación necesita, en especial las aplicaciones de línea de negocios. “En algunas ocasiones, no quiero restaurar el sistema completo, tan solo un conjunto en particular de datos relevantes a una sola aplicación. Entonces tengo que asegurarme de que mis backups se hayan hecho de manera correcta y de tener la certeza de que mis aplicaciones estarán en línea rápidamente”.

Esto lleva a otro punto, que las organizaciones **necesitan tener la cantidad correcta de Disponibilidad con sus objetivos de tiempo de recuperación**, lo que Vanover denomina “estar lo suficientemente disponible”. Esto se debe a que la empresa moderna depende cada vez más de las operaciones digitales y también de que sus datos estén en línea todo el tiempo. La clave es tener los tipos correctos de backups que permitan una restauración flexible. Por ejemplo, Veeam ofrece una característica de recuperación especializada que permite que las máquinas virtuales vuelvan de un backup a los pocos minutos y se puedan usar.

Volverse más resistentes al ransomware no es un proceso simple. Y, de hecho, se trata más de un viaje que de un solo destino. Afortunadamente, estos consejos pueden ayudarlo a proteger su organización y operaciones.