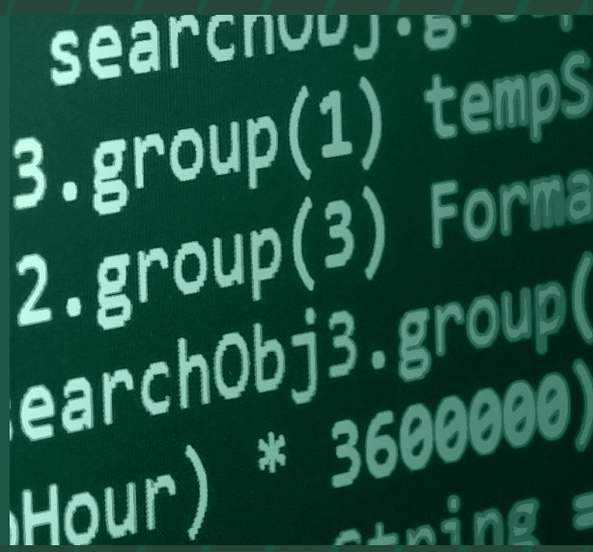
DELL Technologies

5 Recomendaciones para sobrevivir a un ataque de ransomware



1 Mantenga un plan integral de respuesta ante incidentes

Céntrese en minimizar el efecto de un ataque

Practique, pruebe y actualice con frecuencia

Tenga un equipo de respuesta ante incidentes preparado con antelación

Considere contratar un ciberseguro como parte de su estrategia general de resiliencia

Incluya planes para trabajar con las fuerzas de seguridad

2 Establezca una estrategia de comunicación clara

Cree plantillas de comunicación por adelantado

Fomente comunicaciones oportunas y claras dentro de la organización

Prepárese para comunicarse de forma externa, si es necesario

Cumpla con la normativa aplicable en materia de notificaciones

3 Garantice una protección de datos sólida

Proteja los datos críticos en un vault de datos inmutable y aislado

Priorice la recuperación por servicio/infraestructura

Ponga en práctica la capacidad de recuperación

Combine capacidades como el "cuarto limpio" con su objetivo de tiempo de recuperación

Garantice la integridad de los datos recuperables

4 No asuma una vuelta inmediata a la normalidad

Pagar el rescate debe ser el último recurso

Garantice el cumplimiento de los requisitos legales y normativos antes de pagar

No hay garantía de que el hacker devuelva los datos incluso si se paga el rescate

5 Enfatice la formación y la educación

Realice simulaciones de ataques

Supervise y ponga a prueba las prácticas de higiene de seguridad de los empleados

Utilice herramientas como las pruebas de phishing y la formación en seguridad de correo electrónico

Copyright © 2024 Dell Inc. o sus filiales. Todos los derechos reservados.

Ya no es una cuestión de "si", sino de "cuándo".

Las empresas deben planificar como si un ataque fuera inevitable, a pesar de sus mejores defensas. Para hablar sobre qué hacer en caso de desastre, los expertos en la materia de Dell, Jim Shook (director internacional de ciberseguridad y cumplimiento normativo) y Steven Granat (consultor principal de soluciones de ciberseguridad y asociaciones estratégicas) hablaron con Brian White, consultor sénior de marketing de producto de Dell Data Protection.

> Es necesario tener a las personas adecuadas y realizar un simulacro y ejecutar acciones para que cuando ocurra un ataque, todos sepan inmediatamente lo que están haciendo".
>
> ***Steven Granat**, consultor principal,*
> *Soluciones de ciberseguridad y asociaciones estratégicas, Dell Technologies*

Mantenga un plan integral de respuesta ante incidentes

Cuando se produce un ataque, todas las partes interesadas clave, prácticamente todas las personas de la organización y terceros, como los proveedores, deben saber qué hacer. Un plan escrito de respuesta ante incidentes debe describir una secuencia clara de medidas, aconseja Shook. Un plan integral abordará los pasos tecnológicos, de proceso y de comunicación, desde la acción inmediata hasta la recuperación. Asegúrese también de contar con un documento escrito en papel, ya que los canales de comunicación digitales pueden no estar operativos. "Necesita un plan que pueda directamente sacar de una estantería", dice Granat.

Establezca una estrategia de comunicación clara

La mayoría de las empresas necesitarán comunicarse con las partes interesadas clave y, en muchos casos, deberán cumplir con los requisitos normativos. Cree diferentes plantillas para las comunicaciones internas y externas con instrucciones sistemáticas sobre a quién notificar en qué secuencia y en qué momento. Planifique en consecuencia por si los sistemas de telefonía y correo electrónico están inactivos.

Implemente una estrategia sólida de protección de datos

Un objetivo clave tras superar un ataque de ransomware es restaurar los datos y recuperarse de la forma menos dolorosa posible, evitando al mismo tiempo pagar el rescate. Una estrategia de protección de datos sólida es clave para lograr esos objetivos, pero deberá incluir tanto la tecnología como los procesos. "Utilice datos inmutables y vaults virtuales para almacenar suficientes datos en los que pueda confiar o, al menos, como puntos de validación que le permitan recuperar los sistemas", aconseja Shook. Asegurarse de que los datos estén protegidos es el primer paso. También debe contar con las personas y los procesos necesarios para recuperarlos. Los expertos externos pueden ayudar, pero deben involucrarse en la fase de planificación.

No dé por sentado que volverá inmediatamente a la normalidad, aunque pague un rescate

El pago de un rescate, que solo debe considerarse como último recurso, no garantiza que el interruptor se vuelva a encender de inmediato. Recuerde que está negociando con un delincuente, e incluso si obtiene las claves del decodificador, necesita una estrategia para los datos recién recuperados. Para empezar, debe probar los datos descifrados y reconstruir todos los sistemas metódicamente. Prestar una atención meticulosa a los eventos hipotéticos antes incluso de que se produzca un ataque contribuirá en gran medida a lograr la resiliencia. "Comprender las diferentes aplicaciones y dependencias de su infraestructura tecnológica es fundamental para un retorno eficiente a la normalidad. '¿Tengo una fuente de recuperación viable y un objetivo recuperable?' '¿Hay datos que no están comprometidos?' Estas son consideraciones importantes en las que pensar", dice Granat.

En la fase de recuperación, también debe asegurarse de que el adversario haya abandonado sus sistemas. "Debe asegurarse de que se haya sofocado el incendio en su casa y también averiguar qué provocó ese incendio en primer lugar, porque sin estos dos elementos críticos de información, sigue siendo vulnerable ante futuros ataques", dice Shook.

La formación y la práctica son esenciales

Una parte importante de la ciberresiliencia es contar con una formación exhaustiva, que abarca desde garantizar que los empleados practiquen una buena higiene en materia de ciberseguridad hasta aplicar de forma rutinaria el plan de recuperación. "Es necesario tener a las personas adecuadas y realizar un simulacro y ejecutar acciones para que cuando ocurra un ataque, todos sepan inmediatamente lo que están haciendo", dice Shook.

El ransomware puede ser inevitable en el panorama de amenazas actual, pero mediante la planificación y la ejecución puede minimizar el impacto operativo, financiero y en la reputación. El objetivo es volver a la normalidad de la manera más rápida e indolora posible.

Descubra cómo afrontar algunos de los principales retos de ciberseguridad actuales en **dell.com/cybersecuritymonth**

Copyright © 2024 Dell Inc. o sus filiales. Todos los derechos reservados.

DELL Technologies