10 formas de prevenir, detectar y recuperar amenazas de ransomware y zeroday

10 formas de prevenir, detectar y recuperar amenazas de ransomware y zeroday. A medida que el ransomware se extiende, la amenaza de extorsión e interrupción cobra mucha importancia. Averigüe qué pasos prácticos puede tomar para evitar que el ransomware se afiance y lo detecte cuando sus defensas fallan. El ransomware es un tipo de malware que generalmente cifra los datos, bloqueando el acceso hasta que se paga una tarifa al atacante. Si bien la exageración utilizada puede superar el riesgo real, el ransomware ha evolucionado , se ha expandido y se ha vuelto más sofisticado rápidamente en respuesta a nuestros esfuerzos por defendernos contra él.

Ha habido algunos ataques de ransomware de alto perfil en los últimos años, como parte de una creciente ola de amenazas. Los volúmenes de ransomware aumentaron un 350% solo en 2017, según un informe reciente de Seguridad de NTT . Los profesionales de seguridad encargados de proteger los datos de la empresa deben tener ransomware en sus radares y es crucial tomar medidas para mitigar la amenaza.

Siempre es mejor prevenir que curar, pero ningún sistema de seguridad es perfecto, por lo que vale la pena prepararse para lo peor creando un plan de recuperación. Aquí tenemos una lista de las 10 mejores prácticas que lo ayudarán a prevenir ataques de ransomware, a detectarlos cuando fallen sus defensas y a recuperarse de ellos con la menor interrupción posible.

Entrenamiento de conciencia de seguridad

Hay varias maneras diferentes en que el ransomware puede ingresar a su red, pero una de las más probables es a través de un ataque de phishing . Tan pronto como un empleado, sin saberlo, pulsa o hace clic en un enlace, no debería o abre el archivo adjunto de correo electrónico incorrecto, el ransomware puede afianzarse en su sistema y propagarse rápidamente a través de su red. Inicie un programa adecuado de capacitación en conciencia sobre seguridad y reduzca la amenaza de error de los empleados que conduce a una infección por ransomware.

Actualizaciones, parches y configuración

La correcta higiene de la seguridad del punto final es esencial para prevenir el ransomware. Los atacantes normalmente buscarán vulnerabilidades y configuraciones erróneas que puedan explotar para obtener acceso a su red. No te lo pongas fácil. Asegúrese de que los dispositivos y sistemas se actualicen periódicamente con los últimos parches

de seguridad, no se conformen con las configuraciones predeterminadas y tómese el tiempo para desactivar las funciones que no necesite.

Inventario actualizado de activos

Si no sabe con precisión qué dispositivos están legítimamente conectados a sus nubes públicas y privadas, ¿cómo puede esperar reconocer o prevenir un ataque? Necesita una descripción general en tiempo real de todos los dispositivos en su red y una comprensión clara de qué permisos debe tener cada dispositivo según el usuario. ¿Sabe cuántos dispositivos no administrados tiene en su red? IoT es un gran objetivo.

Evaluación continua de la vulnerabilidad.

Los ciberdelincuentes siempre tomarán el camino de menor resistencia y, por lo tanto, los ataques de ransomware a menudo explotan vulnerabilidades conocidas en el software popular. Necesita un sistema de seguridad que esté actualizado con las últimas revelaciones en términos de vulnerabilidades, y estos datos deben verificarse de forma cruzada con su red para asegurarse de que no está ofreciendo una ruta fácil.

Monitoreo de tráfico en tiempo real

Se enfoca mucho en filtrar y bloquear las conexiones entrantes, pero también debe hacer lo mismo con las conexiones salientes. El ransomware normalmente tendrá acceso y luego marcará el inicio para obtener más instrucciones. Si puede bloquear los intentos de salida iniciales para conectarse al servidor del atacante, entonces es posible que pueda detener el ataque de ransomware antes de que despegue. Cualquier tráfico sospechoso en cualquier dirección debe marcarse automáticamente y generar alertas para una mayor

investigación.

Detección de intrusiones

Para una protección adecuada, necesita un sistema que pueda reconocer los signos de un ataque de ransomware, ya sea comunicación con un actor mal conocido, envío de datos a través de un canal oculto o desactivación de firewalls o software antivirus. Las actualizaciones sospechosas de las políticas, los análisis no programados y los errores de actualización también pueden ser señales de advertencia. Ubíquelos a tiempo y es posible que pueda poner en cuarentena los sistemas infectados antes de que el ransomware se propague.

Monitoreo de integridad de archivos

Si configura la supervisión de la integridad de los archivos en datos críticos para la empresa, recibirá alertas automáticas si se accede o se modifica algún archivo crítico. Esto puede ayudarte a detectar un ataque de ransomware mucho más rápido y actuar para limitar su impacto. ¿Quién tiene

acceso y a qué están accediendo? Lo mejor es entender el comportamiento normal de un usuario.

Registro de monitoreo y análisis

Es imposible que los ciberdelincuentes inicien y ejecuten un ataque de ransomware sin dejar rastros de su actividad en su red. Considere emplear un software de gestión de eventos e información de seguridad (SIEM) capaz de analizar los registros del sistema, los registros de aplicaciones y los registros de actividades para recopilar y analizar datos y marcar el comportamiento inusual. El análisis de comportamiento de usuarios y entidades (UEBA) es la siguiente pieza del rompecabezas.

Inteligencia continua de amenazas

Debe estar monitoreando su red en tiempo real para obtener una imagen clara de su seguridad, pero cada herramienta de monitoreo es tan buena como la información que tiene. La última información sobre amenazas es vital si esperas detectar los ataques de ransomware rápidamente y evitar que se propaguen. Más allá de las amenazas específicas conocidas en términos de sabores de ransomware, también desea armar el software de seguridad con una comprensión de los últimos tipos de actividad y comportamientos comunes al malware de vanguardia. La inteligencia artificial y el aprendizaje automático se están incorporando en muchas de las últimas tecnologías de seguridad de red para que sean su segundo conjunto de ojos.

Copia de seguridad confiable y recuperación

Incluso si toma todas las precauciones posibles para tratar de evitar que el ransomware ingrese y detecte ataques con

rapidez, aún puede haber ocasiones en que sus defensas se queden cortas. La mejor manera de protegerse contra los ataques de ransomware y disminuir el impacto potencial en su negocio es mantener un sistema de respaldo regular y seguro junto con un plan de recuperación claro que le permita restaurar un respaldo reciente de inmediato si lo necesita.

A medida que los ataques de ransomware y zeroday continúan haciéndose más sofisticados y vemos un aumento en el ransomware y los zerodays utilizados como herramientas de desvío y destrucción, es vital que los profesionales de la seguridad sean conscientes de los riesgos que plantea. Tome las medidas adecuadas para prevenir, detectar y recuperarse del ransomware y puede reducir drásticamente su impacto potencial en su negocio.