Prevención del ransomware

Revise su estrategia de mitigación de riesgos. Proteja sus puntos finales y sus datos de backup contra el ransomware y los ciberataques relacionados.

El ransomware lleva entre nosotros desde hace mucho tiempo. Así, mientras sus autores vean la oportunidad de obtener beneficios económicos, con toda seguridad el ransomware está aquí para quedarse.

El Centro de Denuncias de Delitos en Internet del FBI informó de 2084 denuncias de ransomware en el primer semestre de 2021, lo que supone un aumento interanual del 62 %.[1] Un informe de Gartner afirmaba que "a corto plazo, el ransomware puede costarles a las empresas millones de dólares, e incluso una pérdida potencialmente mayor a largo plazo, lo que afecta a su reputación y fiabilidad".[2]

Junto con el impacto económico que conlleva un ataque de ransomware se encuentra el impacto de intentar recuperar todos los datos comprometidos. Según una encuesta de Forrester, solo el 25 % de los encuestados afirmaba que era capaz de recuperar entre el 75 y el 100 % de sus datos tras un ataque. Un número mucho mayor de encuestados (39 %) aseguraba que solo había logrado recuperar entre el 50 y el 74 % de sus datos.[3]

¿Podría dirigir su empresa únicamente con el 50 o el 74 % de los datos que solía tener?

Los modelos de ransomware están cambiando. Lo mismo debería ocurrir con su estrategia de protección de datos.

Ante los altos niveles de amenaza y los elevados costes asociados al ransomware, los administradores de tecnología informática y de los backups están reevaluando con ansiedad sus estrategias de protección de datos.

El ransomware se mueve con diferentes formas y disfraces. Los ataques que siguen el modelo de sembrar y esperar, como CryptoLocker, muy popular hace varios años, lanzan una amplia red para alcanzar al mayor número de víctimas posible.[4] Los modelos han evolucionado para apuntar a sectores específicos, como los servicios públicos, las universidades y la sanidad.[5] Algunos ataques parecen ransomware, pero en realidad pretenden simplemente destruir datos e infraestructuras.[6]

Incluso los modelos financieros están cambiando. Los días en los que los hackers pedían 300 dólares en bitcoins para descifrar los datos ya son historia. Una encuesta reciente reveló un rescate medio próximo a los 2 millones de dólares.[7] También se informó del pago de 4,4 millones de dólares autorizado por el director ejecutivo de Colonial Pipeline tras el ataque de ransomware a esa empresa.[8] Incluso peor aún, los autores han adoptado tácticas como la amenaza de publicar los datos rescatados.

El papel de la seguridad de los puntos finales y los backups

Cuando cada dispositivo conectado a su empresa es un vector potencial de ataque, la seguridad de los puntos finales se convierte en un imperativo. Esto conlleva identificar y proteger todos los dispositivos que acceden a su red, con independencia de dónde se encuentren.

Según el Centro de Recursos para el Robo de Identidad (ITRC), las 1291 infracciones de datos en los primeros nueve meses de 2021 supusieron un 17 % más que en todo el año 2020.[9] Las infracciones de datos siempre comienzan en los puntos finales, por lo que el riesgo de que su organización sufra infracciones de datos sigue creciendo a medida que se añaden dispositivos.

Además de proteger los puntos finales, piense en la estrategia para los backup. El almacenamiento de una copia de los datos en una cinta, en un dispositivo independiente o incluso en una ubicación independiente como la nube ayuda a garantizar la recuperación tras un ataque. Muchas organizaciones de tecnología informática replican sus backups externamente con vistas a la recuperación ante desastres.

El problema consiste en que sus sistemas de backup siguen dependiendo de los servidores. Esos servidores dependen de componentes potencialmente vulnerables como un sistema operativo y Active Directory, lo que significa que sus backups también son vulnerables. Asimismo, dado que los recursos compartidos de red son un objetivo para la mayoría del ransomware, los productos de backup que utilizan recursos compartidos para almacenar datos conllevan más riesgo.

Para proteger realmente a su organización contra el ransomware, proteja los datos de producción de sus puntos finales y los datos de sus backups.

Soluciones de Quest® para la protección contra el ransomware

Las soluciones de Quest pueden ayudar a evitar que el ransomware ataque sus puntos finales y backups.

KACE® Unified Endpoint Manager de Quest

KACE Unified Endpoint Manager automatiza el escaneo de vulnerabilidades, la aplicación de parches y la actualización de la seguridad no solo de los sistemas operativos sino también de las aplicaciones de terceros y las actualizaciones in situ. Su gestión unificada de puntos finales (UEM) automatizada identifica con suma rapidez los dispositivos con parches inadecuados o con vulnerabilidades y exposiciones comunes (CVE) conocidas, y los actualiza.

Desde un único panel, KACE permite descubrir, gestionar y proteger todos los puntos finales que acceden a su red, incluidos los siguientes:

- Equipos de sobremesa, portátiles, servidores y dispositivos móviles con Windows
- Equipos de sobremesa y portátiles Mac
- Máquinas y servidores Linux
- Chromebooks
- Dispositivos móviles iOS y Android
- Dispositivos que no sean ordenadores como impresoras
- Dispositivos del Internet de las cosas (IoT)

En lugar de investigar, comprar, aprender y mantener múltiples soluciones puntuales, obtenga una UEM completa en una única consola KACE. Centraliza el control de registro, borrado/bloqueo, descubrimiento, inventario, administración de activos de hardware/software y creación de scripts. Además, ofrece un servicio de ayuda integrado para los tickets de servicio de tecnología informática.

Gestione su negocio en lugar de gestionar sus sistemas. Con KACE Unified Endpoint Manager, tendrá una visión general de todo su entorno de puntos finales en un solo lugar, de modo que no tenga que reunir datos de diferentes productos.

Quest NetVault® Plus

NetVault Plus ofrece backups potentes y fáciles de usar para las empresas junto con una protección integrada contra el ransomware. Combina el software de backup y recuperación de NetVault con el almacenamiento secundario definido por software de Quest QoreStor®.

Tanto en entornos locales como en la nube, NetVault Plus refuerza su protección contra el ransomware con el cifrado de datos para sus backups. Proporciona un almacenamiento secundario inmutable para que los datos de backup escritos en QoreStor no puedan sobrescribirse, modificarse ni eliminarse fuera de los parámetros de retención que especifique.

NetVault Plus protege aún más contra los ataques de ransomware al conservar una copia de todos los datos de los backups eliminados en la papelera de reciclaje de datos de QoreStor durante un periodo especificado por el administrador. Para mayor seguridad, su tecnología Secure Connect envuelve la transferencia de datos y los comandos de control en una capa TLS 2.0 para evitar ataques a sus datos de backups.

Para el almacenamiento de datos, NetVault Plus admite los protocolos Rapid Data Access (RDA), que, a diferencia del protocolo Server Message Block (SMB) utilizado para los recursos compartidos de Windows, no son abiertos. El sistema operativo no puede acceder directamente a RDA y dispone de un requisito de autentificación que se sitúa fuera del servidor local o de las construcciones controladas por el dominio.

Por último, NetVault Plus ofrece un sólido acceso basado en roles sin necesidad de integrarse con servicios como Active Directory. Esto ofrece otro grado de separación del entorno de producción e impide el acceso de un atacante.

Ya es hora de proteger a su organización contra el ransomware

Al final, incluso la organización mejor preparada no puede protegerse completamente contra todos los ataques de ransomware. No obstante, se puede mitigar el riesgo cuando se dispone de una solución que no solo protege los puntos finales, sino que también permite restaurar todos los datos de forma rápida y completa.

Las soluciones de Quest para la prevención del ransomware están diseñadas para ayudarle a lo siguiente:

- Mitigar el riesgo de que el ransomware perjudique a su negocio
- Reducir el número de componentes básicos que puedan atacarse
- Limitar su exposición a las técnicas de captura de datos
- Proteger sus datos de copia de seguridad contra el ransomware

Obtenga más información sobre KACE Unified Endpoint Manager y NetVault Plus.

1 Centro de Denuncias de Delitos en Internet del FBI, "Ransomware Awareness for Holidays and Weekends", septiembre de 2021. Las denuncias ascendieron a 2084 desde enero hasta el 31 de julio de 2021.
2 Gartner, "6 Ways to Defend Against a Ransomware Attack", noviembre de 2020.
3 Forrester Research, "Ransomware Recoverability Must Be a Critical Component of Your Business Continuity Plans", octubre de 2019.
4 KrebsonSecurity.com, "2014: The Year Extortion Went Mainstream", junio de 2014.
5 CyberWire, "Ransomware: healthcare, utilities, and universities. REvil's old sites are stirring", septiembre de 2021.
6 The Register, "Ukraine blames Belarus for PC-wiping 'ransomware' that has no recovery method and nukes target boxen", enero de 2022.
7 Ransomware.org, "Ransomware Attacks Ramped Up In 2021", diciembre de 2021.
8 CNN, "Colonial Pipeline CEO admits to authorizing $4.4 million ransomware payment", mayo de 2021.
9 ITRC, "Number of Data Breaches in 2021 Surpasses All of 2020", octubre de 2021.