



TotemGuard



Terry Noonan
Vicepresidente
Productos Shavlik
Technologies

Cómo mejorar tu postura de seguridad a través de la virtualización

La Virtualización fuerza a las organizaciones a pensar diferente

La tasa de adopción de máquinas virtuales se ha disparado en la mayoría de organizaciones, en parte, impulsada por el aumento de la relación calidad/precio de los servidores. Esto ha creado un auge de servidores que representa un aumento sustancial del número de dispositivos conectados a la red, con el hecho de que muchas organizaciones no tienen en cuenta que cada servidor tiene distintas necesidades y debe configurarse, parchearse y securizarse de forma individual. Muchos pueden pensar que como los requisitos de los dispositivos físicos son reducidos, se reducen también los requisitos operacionales. Las máquinas virtuales, al igual que las físicas, tienen acceso a la red y pueden ser vulneradas, infectadas y estar en peligro al igual que un dispositivo físico dedicado. Son más dinámicas, yendo y viniendo a capricho de la creciente cantidad de usuarios experimentados. Pero, si se gestionan adecuadamente, pueden mejorar sustancialmente la postura de seguridad.

Establece prácticas de gestión

Las organizaciones reconocen que no son conscientes de cuántas máquinas virtuales están operativas con exactitud. No tienen estrategias efectivas de gestión, no las rastrean ni llevan un control de forma individual. Además, las máquinas virtuales presentan el mismo riesgo y ofrecen los mismos peligros que las máquinas físicas. La expansión virtual no gestionada, rápidamente puede causar que todas las prácticas de gestión que se estaban llevando a cabo sean descentralizadas, y permitir a varios usuarios crear y eliminarlas antes de que cualquier medida de seguridad razonable se ejecute. Debido a esto, los analistas de Gartner estiman que el 60 por ciento de la producción de máquinas virtuales serán menos seguras que sus equivalentes físicas. En caso que este impulso continúe, sin que se consideren cuestiones de seguridad y gestión, los administradores están en riesgo de deshacer 15 años de inversiones en fuertes defensas para sus sistemas físicos.

Automatiza todas las tareas críticas

La Virtualización fuerza a las organizaciones a pensar de manera diferente y a cambiar los procesos. Nuevos servidores y aplicaciones pueden aparecer de forma mucho más rápida, a menudo sin la autorización y coordinación del equipo de seguridad.

Con el aumento del número de máquinas a proteger y securizar, los administradores de TI necesitan monitorizar continuamente nuevos dispositivos, servidores y servicios de forma agresiva.



TOTEMGUARD

902 360 645

www.totemguard.com

info@totemguard.com



TotemGuard

Una respuesta agresiva exigirá la automatización de los procesos de la gestión de vulnerabilidades, incluida la gestión y configuración de parches. Muchos ya han adoptado diversas herramientas para hacer esto, pero el resultado ha sido semi-automático, ya que requieren intervención manual a la hora de desplegar, verificar e informar sobre la actividad de la red. El volumen de máquinas virtuales que se han añadido a la red requiere una respuesta más continua, totalmente automatizada y vinculada en cada etapa, desde la detección hasta a la remediación y notificación de las medidas adoptadas por los parches, los errores de configuración y otras vulnerabilidades. Si las nuevas herramientas y las prácticas de seguridad mejoran la automatización de la gestión de máquinas virtuales, entonces la virtualización será mucho más fiable.

Aprovecha la capacidad de asegurar offline

En determinados períodos, muchas empresas tienen intencionadamente un número significativo de máquinas virtuales offline para hacer frente a requisitos tales como la continuidad del negocio, o para conservar el consumo de energía (Green IT). Estas máquinas se ponen en línea sólo cuando hay necesidades operacionales. A menudo, volver estas máquinas online sólo para configurarlas para que sean seguras contra amenazas potenciales es una tarea difícil y que consume mucho tiempo. Si las máquinas virtuales pueden gestionarse y securizarse en un estado offline, su ventana de vulnerabilidad ante una amenaza concreta se reduce significativamente.

La seguridad se aumenta por la capacidad de utilizar máquinas virtuales, las cuáles han sido parcheadas offline, para un backup de sistema críticos cuando un parche requiere un reinicio del sistema. La estrategia actual más común es esperar hasta encontrar un momento en que los sistemas críticos pueden ser reiniciados, dejándolos funcionar de forma insegura con la vulnerabilidad hasta que se pueda abordar.

La implementación de la virtualización sin una seguridad adecuada aumenta las vulnerabilidades de una organización. Sin embargo, cuando están debidamente salvaguardadas a través de procesos continuos y permanentes, con el descubrimiento automatizado de nuevas máquinas virtuales, incluso antes de entrar en línea, las vulnerabilidades a amenazas quedan reducidas, y una organización sí puede experimentar un mayor nivel de seguridad con esta virtualización.



TOTEMGUARD

902 360 645

www.totemguard.com

info@totemguard.com