TRANSFORMAR LA SEGURIDAD

Una prioridad estratégica de TI

La seguridad es una prioridad para todos los negocios

A medida que aumenta la conexión entre las personas, los dispositivos y los objetos, la protección de todas estas conexiones y entornos se vuelve más importante que nunca. Las organizaciones de TI necesitan proteger cada interacción entre los usuarios, las aplicaciones y los datos, sin importar cómo y dónde están conectados. Deben hacerlo en un entorno cada vez más dinámico que cambia constantemente.

Los riesgos en materia de seguridad son altos para las empresas de todos los sectores y siguen aumentando. Según un estudio reciente, el costo promedio total de una infracción de datos aumentó de 3.520.000 de USD a 3.790.000 de USD en tan solo un año.[1] Para las organizaciones que están adoptando entornos virtualizados y de nube, la visibilidad y el control totales son clave para reducir este riesgo.

HAY MUCHO EN JUEGO PARA LA SEGURIDAD

El delito cibernético representa la causa de más rápido crecimiento en lo que respecta a interrupciones del centro de datos: ha aumentado desde un 2 % en 2010 hasta un 22 % en 2016.[2]

El costo promedio de una interrupción del centro de datos ascendió a 740.357 USD en 2016.[3]

El cambio de las necesidades de TI en un panorama de amenazas dinámico

Cada empresa es ahora una empresa digital, y esta transformación ha traído cambios importantes en el panorama de TI. Las infraestructuras de aplicaciones han evolucionado de centros de datos en las instalaciones que se ejecutan en la infraestructura física a entornos altamente dinámicos que se encuentran en nubes privadas y públicas.

Las aplicaciones en sí están cambiando también. Las organizaciones están dejando las pilas de aplicaciones monolíticas y están optando por aplicaciones distribuidas de múltiples niveles basadas en microservicios. A medida que la fuerza de trabajo se vuelve más móvil y distribuida, los entornos de usuario final también evolucionan. Ya no se limitan a escritorios administrados desde la empresa, sino que se centran en dispositivos móviles, en iniciativas de dispositivos propios del usuario final (Bring Your Own Device, BYOD) y en el Internet de las cosas (Internet of Things, IoT).

Para TI, los modelos tradicionales de seguridad perimetral de red ya no son suficientes para proteger la expansión de aplicaciones y usuarios, que crece rápidamente, ni para alcanzar los requisitos de cumplimiento en aumento. Los entornos y los usuarios no están contenidos de manera prolija detrás de los firewalls perimetrales, sino que requieren una protección más ágil y flexible. Los atacantes son más sofisticados y el ciberespacio adopta cada vez más armas. En la actualidad, mediante el uso de kits de herramientas como Zeus y BlackPoS, incluso un hacker sin experiencia puede atacar de forma avanzada a una empresa y ocasionar daños reales en la productividad, los recursos y la reputación.

[1] https://www.sdxcentral.com/articles/analysis/securing-cloud-sdn/2016/05/

[2] Cost of Data Center Outages, Ponemon Institute, enero de 2016

[3] Ibid

VMware le permite a TI transformar los entornos y las operaciones de seguridad para abordar los desafíos actuales. A continuación, se presenta cómo lo logra:

- **Protección de la infraestructura de aplicaciones:** separe la infraestructura de las aplicaciones y, de esta manera, mejorará la visibilidad y podrá alinear mejor la seguridad con las aplicaciones.
- **Protección de identidades y terminales:** utilice una capa de software omnipresente en todos los usuarios y terminales para obtener mejor visibilidad y control, sin que esto afecte la experiencia de usuario.
- **Cumplimiento optimizado:** aplique software en la infraestructura de aplicaciones, la identidad y los terminales para simplificar el cumplimiento.

Una seguridad eficaz abarca múltiples áreas

Proteger una organización mediante una solución de seguridad sólida que cumpla con los estándares no es sencillo cuando la infraestructura y los usuarios cambian rápidamente. Las viejas reglas básicas de seguridad de red quedaron obsoletas, y los equipos de TI deben seguir el ritmo de los siguientes cambios:

- Cambios en la infraestructura:la infraestructura que se utiliza para ejecutar aplicaciones como servidores de base de datos y web está evolucionando desde entornos en las instalaciones para ser compatible con aplicaciones distribuidas y de nube.
- Mayor movilidad:TI necesita ampliar las políticas de seguridad para respaldar la avalancha de nuevos modelos y dispositivos.
- Aumento del cumplimiento:el entorno de cumplimiento normativo se vuelve cada vez más complejo a medida que las organizaciones enfrentan nuevos requisitos.

Visibilidad y contexto para transformar la seguridad

VMware puede ayudar a las organizaciones a alcanzar la información que necesitan para estar a la vanguardia de las cambiantes necesidades de seguridad. El ingrediente secreto de las soluciones de VMware es una capa de software omnipresente en la infraestructura de aplicaciones y los terminales que es independiente de la ubicación o la infraestructura física subyacente. Esta estrategia le da al software de VMware una posición única dentro de la infraestructura que le permite proporcionar una amplia visibilidad de cada interacción entre los usuarios y las aplicaciones para el Departamento de TI. Con similar importancia, proporciona contexto para comprender lo que significan esas interacciones. En conjunto, esta visibilidad y un contexto más amplio les permitirán a las organizaciones lograr una mejor alineación de las políticas y los controles de seguridad con las aplicaciones que estos protegen.

Asimismo, una seguridad eficaz necesita múltiples capas de protección, y la ubicación de VMware dentro de la infraestructura le permite tener el mejor punto de control posible para que TI haga cumplir las políticas e inserte servicios de terceros a fin de obtener una protección inteligente adicional.

Protección de la infraestructura de aplicaciones

A medida que evolucionan los modelos de infraestructura de aplicaciones, la estrategia tradicional de seguridad de red centrada en el perímetro no puede proporcionar visibilidad y control suficientes dentro del centro de datos. Al mismo tiempo, los datos estáticos almacenados se han vuelto un blanco mucho más valioso para los atacantes. Para abordar estos problemas, las organizaciones deben transformar la manera en que protegen la infraestructura de aplicaciones.

La solución comienza con la virtualización y la capacidad de separar la infraestructura subyacente de las aplicaciones que se ejecutan en ella, independientemente de si esa infraestructura se encuentra en las instalaciones o en la nube pública. Esta capa de separación proporciona una visibilidad completa de la ruta de datos, así como un punto de cumplimiento ideal para compartimentar aplicaciones mediante la microsegmentación de la red. El uso de la microsegmentación en el software les proporciona a las organizaciones la posibilidad de simplificar las políticas de seguridad y alinearlas de manera más estrecha con las necesidades de las aplicaciones. Además, permite que las políticas sigan a la aplicación a medida que esta se desplaza en nubes públicas y privadas. Una capa de separación también proporciona a TI una plataforma para la inserción de servicios adicionales de terceros a fin de obtener una protección de la seguridad más avanzada.

Asimismo, la microsegmentación ayuda a TI a evitar que las amenazas contra la seguridad violen las defensas. Esto se logra habilitando el principio de la estrategia de menor privilegio centrada en las aplicaciones, la cual reduce la superficie de ataque de la infraestructura.

Una capa de separación entre las aplicaciones y la infraestructura subyacente no solo ayuda a TI a evitar los ataques, sino que también proporciona un punto ideal para el cifrado de datos almacenados. Mediante el cifrado de datos estáticos, en el nivel de las cargas de trabajo, las organizaciones pueden garantizar la seguridad de los datos de la infraestructura de aplicaciones, incluso si caen en manos equivocadas.

"VMware NSX® permite que los datos fundamentales de los pacientes estén disponibles más rápidamente para los pacientes y profesionales médicos del hospital, mientras se mantienen segmentados y protegidos".

CHRISTOPHER FRENZ
DIRECTOR OF IT INFRASTRUCTURE, INTERFAITH MEDICAL CENTER

Protección de identidades y terminales

A medida que las empresas se vuelven digitales, los dispositivos móviles proliferan con rapidez. Las organizaciones utilizan dispositivos basados en diversos sistemas, desde Android e iOS hasta Windows y macOS, para fortalecer las fuerzas de trabajo y rediseñar los procesos empresariales tradicionales. La compatibilidad con todos estos dispositivos y plataformas es un desafío, especialmente a medida que las empresas adoptan las iniciativas de IoT y BYOD y la movilidad empresarial.

VMware ayuda a TI a abordar este desafío mediante la aplicación de una capa de software omnipresente en todos los usuarios y terminales que permita verificar la identidad del usuario y la postura del dispositivo. Esta estrategia proporciona un control y una visibilidad integrales del usuario y el terminal, que se extienden hasta el centro de datos o la nube, donde se encuentra la infraestructura de aplicaciones. El software de VMware permite que TI pueda agregar una capa de seguridad adaptativa y condicional en cada nivel de transacción, desde el usuario hasta los recursos a los que accede. Esto ayuda a proteger los datos corporativos y reducir la superficie del ataque cibernético, sin afectar la experiencia de usuario.

Las organizaciones pueden usar una solución de VMware única para proteger todos sus terminales, incluidos teléfonos inteligentes, tabletas, computadoras portátiles, dispositivos portátiles y dispositivos de IoT. Como resultado, TI puede implementar sin inconvenientes cualquier aplicación, incluidas aplicaciones virtuales, remotas, nativas y web, y escritorios de Windows, mediante un catálogo de aplicaciones único con inicio de sesión único, seguridad de datos y cumplimiento de terminales incorporados. Desarrollada para los espacios de trabajo dinámicos actuales, la solución de VMware, mediante la microsegmentación, también permite que las empresas extiendan la seguridad más allá de la interfaz de escritorio virtual (Virtual Desktop Interface, VDI) y terminales móviles hasta el centro de datos.

Dado que cada negocio tiene necesidades de seguridad específicas, la solución también ayuda a las organizaciones a personalizar los entornos para que estén alineados con sus prioridades. Proporciona una base para trabajar con los socios de seguridad de VMware, quienes pueden aprovechar la visibilidad y los puntos de control que suministra la solución de VMware para complementar la solución con sus propias ofertas de servicios.

Optimización del cumplimiento

La administración de riesgos y el mantenimiento del cumplimiento continuo son siempre preocupaciones cruciales. Esto es sumamente importante para industrias como organizaciones gubernamentales, de servicios de salud y de servicios financieros, que enfrentan requisitos estrictos como la industria de tarjetas de pago (Payment Card Industry, PCI), la Ley Federal de Administración de Seguridad de la Información (Federal Information Security Management Act, FISMA) y la Ley de Transferencia y Responsabilidad de Seguro Médico (Health Insurance Portability and Accountability Act, HIPAA), entre otros. Las normas y los requisitos están creciendo, a la vez que el panorama digital y las amenazas avanzadas continuas siguen evolucionando. Por lo tanto, más que nunca, es difícil garantizar y demostrar el cumplimiento.

Y, para complicar más las cosas, las organizaciones están realizando rápidamente la transición de los centros de datos en las instalaciones a la nube, lo que dificulta aun más el cumplimiento de las demandas normativas, empresariales y de políticas.

VMware proporciona una capa de software omnipresente en la infraestructura de aplicaciones y los terminales, por lo que usted opta por una estrategia de cumplimiento integral. Esta estrategia única ofrece una ubicación ideal para implementar controles de cumplimiento y obtener la visibilidad necesaria para demostrarlo. La solución proporciona una plataforma tecnológica en la que TI puede insertar de manera dinámica las herramientas y los servicios validados de los socios de la red de VMware para optimizar aun más el proceso de cumplimiento.

MÁS INFORMACIÓN

Obtenga más información sobre esta prioridad estratégica de TI y sus iniciativas de TI correspondientes en vmware.com/latam/it-priorities/transform-security.

El Marco de Arquitectura de Referencia de Cumplimiento de VMware vincula las capacidades integradas de software y hardware y los controles normativos específicos con validación para la auditoría independiente. Las organizaciones pueden aprovechar este programa validado de forma independiente para ejecutar cargas de trabajo altamente reguladas de manera segura. Ya sea que usen un entorno de nube pública o privada, las organizaciones tienen la garantía de que se siguen cumpliendo los requisitos de manera constante. VMware ofrece la velocidad, la eficiencia y la agilidad que los negocios exigen y, al mismo tiempo, permite optimizar el proceso de cumplimiento para la organización.

VMware proporciona seguridad para un panorama y necesidades cambiantes

Contar con una seguridad sólida fue siempre fundamental para las redes de negocio y, a medida que se acelera el ritmo de la transformación digital, resulta más indispensable que nunca. Cuanto más evolucionan los modelos de infraestructura, aplicaciones y fuerza de trabajo tradicionales, más presionado se ve su equipo de TI para proteger el negocio de las nuevas amenazas emergentes.

VMware les permite a las organizaciones transformar la seguridad mediante el aprovisionamiento de una capa de software omnipresente en la infraestructura de aplicaciones y los terminales. Esto les permite maximizar la visibilidad y el contexto de la interacción entre los usuarios y las aplicaciones, de manera que puedan alinear las políticas y los controles de seguridad con las aplicaciones que se protegen. Además, VMware hace que sea más fácil complementar su solución con servicios de seguridad de terceros para obtener una protección inteligente adicional.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel. 877-486-9273 Fax 650-427-5001 www.vmware.com/latam