TRES PASOS CLAVE PARA TRANSFORMAR LA SEGURIDAD DEL ENTORNO DE TI

La seguridad es una prioridad en cualquier empresa

A medida que las personas, los dispositivos y los objetos están más conectados, la protección de todas estas conexiones y entornos se ha vuelto más necesaria que nunca. En un estudio reciente sobre las prioridades en el entorno de TI, el 69 % de los encuestados afirmaron a Tech Pro Research que mejorar la seguridad representaba su principal iniciativa de TI para 2017.[1]

En el mismo estudio, los encuestados también afirmaron que la seguridad sería su mayor dificultad de TI para el año siguiente. Esto se debe a que las organizaciones de TI necesitan proteger todas las interacciones entre usuarios, aplicaciones y datos, independientemente de la manera y el lugar en que se conecten. Y necesitan hacerlo en un entorno en constante cambio y que cada vez es más dinámico.

Los riesgos de seguridad son muy altos para las empresas de todos los sectores y continúan aumentando. Según un estudio reciente, el coste total medio de una filtración de datos aumentó de 3,52 millones de dólares a 3,79 millones de dólares en solo un año.[2] Para las organizaciones que están adoptando entornos de cloud y virtualizados, disponer de máxima visibilidad y control son elementos fundamentales para mitigar este riesgo.

Riesgos en constante evolución ante un panorama de amenazas dinámico

Ahora todas las empresas son digitales, una transformación que ha supuesto cambios significativos en el panorama de TI y, por consiguiente, nuevas dificultades para la seguridad del entorno de TI.

Empecemos con la evolución de las infraestructuras de las aplicaciones, que han pasado de ser centros de datos locales que ejecutan una infraestructura física a entornos altamente dinámicos que residen en clouds privadas y públicas. Y consideremos cómo las aplicaciones en sí están cambiando. Las organizaciones están abandonando las pilas de aplicaciones monolíticas para adoptar aplicaciones de múltiples niveles basadas en microservicios. Dado que los empleados están cada vez más distribuidos y se mueven más, los entornos de usuario final evolucionan con ello. Ya no se limitan a escritorios de gestión corporativa, sino que están centrados en dispositivos móviles, iniciativas Bring Your Own Device (BYOD) y el Internet de las cosas (IoT).

En consecuencia, los modelos tradicionales de seguridad del perímetro de red ya no son suficientes para proteger la proliferación de aplicaciones y usuarios, ni tampoco para satisfacer el incremento de los requisitos de cumplimiento normativo. Los entornos y usuarios no están tranquilamente protegidos tras los cortafuegos perimetrales, sino que requieren una protección más flexible y ágil contra los atacantes, que ahora son más sofisticados. El ciberespacio es cada vez más peligroso. Incluso un hacker con poca experiencia, mediante kits de herramientas como Zeus y BlackPoS, puede asaltar a empresas con ataques avanzados que pueden dañar considerablemente su productividad, recursos y reputación.

Mientras nos adaptamos para afrontar estas nuevas dificultades, los estándares de cumplimiento normativo son cada vez más complejos lo que obliga a un equipo de TI tipo a dedicar el 20 % de su tiempo a tareas relativas al cumplimiento.

ES MUCHO LO QUE ESTÁ EN JUEGO EN TÉRMINOS DE SEGURIDAD

- La ciberdelincuencia es la causa de interrupciones en los centros de datos que más ha crecido; aumentó de un 2 % en 2010 a un 22 % en 2016.[3]
- El coste medio de una interrupción del centro de datos ascendió a 740 357 $ en 2016.[4]

[1] «IT Budget Research: Where CXOs are placing their bets for 2017», Tech Pro Research, julio de 2016.

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

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

[4] Ibíd.

Tres áreas en las que centrarse para una seguridad eficaz del entorno de TI

Proteger una organización con una solución robusta que cumpla con los estándares de seguridad no es fácil cuando la infraestructura y sus usuarios cambian constantemente. Las antiguas reglas básicas de seguridad de las redes han dejado de ser válidas y los equipos de TI deben ponerse al día:

- Infraestructuras en continuo cambio: la infraestructura que solía ejecutar aplicaciones como servidores web y de bases de datos desde entornos locales, está evolucionando para admitir aplicaciones distribuidas y la cloud.
- Más movilidad: el departamento de TI debe ampliar sus políticas de seguridad para respaldar un amplio abanico de dispositivos y modelos nuevos.
- Más requisitos de cumplimiento normativo: las exigencias normativas son cada vez más complejas, ya que las organizaciones deben hacer frente a nuevos requisitos.

Proporcionar visibilidad y contexto para transformar la seguridad

Para adelantarse a las necesidades de seguridad en constante cambio, necesita una gran visibilidad de todas las interacciones entre los usuarios y las aplicaciones. También necesita una solución que proporcione contexto para entender qué significan dichas interacciones. El contexto, junto con una visibilidad más amplia, pueden ayudarle a adaptar sus controles y políticas de seguridad a las aplicaciones que debe proteger.

¿La base de una solución de este tipo? Una capa de software ubicua en toda la infraestructura de aplicaciones y puntos de acceso que sea independiente de la infraestructura física subyacente o de la ubicación.

FIGURA 1. Una capa de software ubicua significa que la seguridad es omnipresente

De hecho, para que la seguridad sea eficiente se necesitan múltiples capas de protección. Y la solución de software adecuada dentro de la infraestructura le proporciona el mejor punto de control posible para aumentar la visibilidad, aplicar las políticas y permitir la inserción de servicios de terceros para una protección inteligente adicional.

Analicemos detalladamente estos tres pasos clave para transformar la seguridad del entorno de TI:

- Proteger la infraestructura de aplicaciones: infraestructura independiente de las aplicaciones, lo cual mejora la visibilidad y protege mejor las aplicaciones.
- Proteger la identidad y los puntos de acceso: emplee una capa de software presente en todos los usuarios y terminales para una mejor visibilidad y control, sin que ello afecte a la experiencia de usuario.
- Cumplimiento optimizado: aplique el software en toda la infraestructura de aplicaciones, la identidad y los puntos de acceso para simplificar el cumplimiento.

« Cada vez son más las compañías que compiten por talentos en un mercado limitado, y la carencia de conocimientos se convertirá en un problema aún mayor. Las compañías pueden verse obligadas a reconsiderar estrategias y buscar soluciones (de seguridad) que sean más proactivas y que requieran una menor gestión para permitirles el mejor uso posible de los recursos».[5]

JAMES MAUDE
INGENIERO DE SEGURIDAD
AVECTO

1. Proteger la infraestructura de aplicaciones

A medida que los modelos de infraestructura de las aplicaciones evolucionan, el enfoque de seguridad de red tradicional basado en el perímetro no puede proporcionar suficiente visibilidad y control dentro del centro de datos. Al mismo tiempo, los datos almacenados inactivos se han convertido en un objetivo mucho más valioso para los atacantes. Para abordar estos problemas, debe transformar la forma en que protege la infraestructura de aplicaciones.

La solución empieza con la virtualización y la capacidad de abstraer la infraestructura subyacente de las aplicaciones que se ejecutan por encima de ella, tanto si la infraestructura es local como si está en la cloud pública. Esta capa de abstracción ofrece una posición privilegiada para obtener visibilidad total de la ruta de datos, y el punto de aplicación ideal para compartimentar las aplicaciones a través de la microsegmentación de la red. Emplear la microsegmentación en el software permite a las empresas simplificar la política de seguridad y ajustarla mejor para satisfacer las necesidades de aplicaciones. También permite a la política seguir a la aplicación al desplazarse entre las clouds privadas y públicas. Una capa de abstracción ofrece además una plataforma para añadir servicios adicionales de terceros y lograr así una protección de seguridad más avanzada.

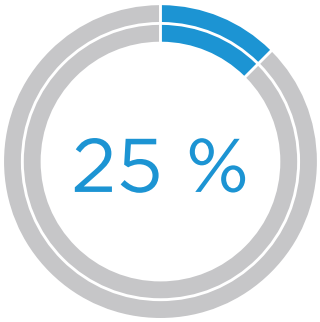
La microsegmentación también ayuda al equipo de TI a evitar las amenazas de seguridad permitiendo el principio de mínimo privilegio centrado en la aplicación, que reduce la superficie de ataque de la infraestructura.

Una capa de abstracción entre las aplicaciones y la infraestructura subyacente no solo ayuda al equipo de TI a evitar ataques, sino que además proporciona un punto ideal para cifrar datos almacenados. Al cifrar los datos inactivos, al nivel de la carga de trabajo, las organizaciones pueden garantizar que los datos de infraestructura de las aplicaciones estén a salvo, aunque caigan en manos equivocadas.

2. Proteger la identidad y los puntos de acceso

A medida que su empresa se adentra en el mundo digital, los dispositivos móviles proliferan con rapidez. Organizaciones como la suya están utilizando todo tipo de recursos, como Android, iOS, Windows, MacOS y otras plataformas, para impulsar la productividad de los empleados y rediseñar los procesos empresariales tradicionales. Ofrecer compatibilidad para todos estos dispositivos y plataformas es complejo, especialmente cuando las empresas adoptan las iniciativas de movilidad empresarial, BYOD e IoT.

[5] http://www.information-management.com/gallery/6-top-it-security-trends-for-2017-10030567-1.html.



En 2020, más del 25 % de todos los ataques identificados en la empresa implicarán el Internet de las cosas (IoT).[6]

Al aplicar una capa de software que esté presente en todos los usuarios y terminales para verificar la identidad de los usuarios y la situación de los dispositivos, estará equipado para afrontar esta dificultad. Este enfoque proporciona visibilidad y control integrales del usuario y del terminal, que se extienden hasta el centro de datos o a la cloud, donde reside la infraestructura de aplicaciones. Con una capa de software, el departamento de TI puede añadir una capa condicional adaptable de seguridad en cada nivel de transacción, desde los usuarios hasta los recursos a los que acceden. Ayuda a proteger los datos corporativos y reducir la superficie de ciberataque, sin que ello afecte a la experiencia de usuario.

Busque una única solución que pueda proteger todos sus terminales, incluidos los teléfonos móviles, las tabletas, los portátiles, los dispositivos ponibles e IoT. Así, podrá implementar cualquier aplicación (ya sea nativa, web, remota, virtual o de escritorio de Windows) mediante un único catálogo de aplicaciones, en las que están integrados el inicio de sesión único, la seguridad de datos y la conformidad de los puntos de acceso. Para las áreas de trabajo dinámicas de hoy en día, necesita una solución que amplíe la seguridad más allá de la interfaz de escritorio virtual (VDI) y los puntos de acceso móviles para, gracias a la microsegmentación, llegar hasta el centro de datos.

Dado que cada empresa tiene necesidades de seguridad específicas, su solución también debe ayudarle a personalizar su entorno para adaptarlo a sus prioridades. Contará con una base para trabajar con los partners de seguridad, quienes pueden aprovechar la visibilidad y los puntos de control proporcionados para complementar la solución con sus propias ofertas de servicios.

« Los clientes huyen de las empresas que sufren vulneraciones y el entorno normativo es tal que las empresas requerirán una protección considerable, tanto si la integran en sus organizaciones como si externalizan la responsabilidad».[7]

FADI ALBATAL
VICEPRESIDENTE SÉNIOR
ABOVE SECURITY

3. Optimizar el cumplimiento normativo

Gestionar el riesgo y cumplir las normativas en todo momento son siempre cuestiones primordiales. Es especialmente importante para sectores como los servicios financieros, los gobiernos y las organizaciones de asistencia sanitaria que deben respetar requisitos estrictos, como PCI, HIPAA, ECPA, la Directiva europea relativa a la protección de datos, etc. Las normativas y los requisitos están en continuo aumento, mientras que el panorama digital y las amenazas persistentes y avanzadas continúan evolucionando, por lo que garantizar y demostrar el cumplimiento normativo es mucho más complicado.

Para complicarlo todo, las organizaciones están migrando rápidamente de los centros de datos locales para adoptar la cloud, por lo que es todavía más complicado satisfacer los requisitos empresariales, normativos y asociados con las políticas.

Con una capa de software presente en toda la infraestructura de aplicaciones y en todos los terminales, estará aplicando un enfoque integral al cumplimiento normativo. Este enfoque único le proporciona una ubicación ideal para implementar los controles de cumplimiento normativo y obtener la visibilidad necesaria para demostrar dicho cumplimiento. La solución adecuada proporciona una plataforma de tecnología en la que las herramientas y los servicios validados de los partners del ecosistema pueden insertarse dinámicamente para optimizar todavía más el proceso de cumplimiento.

Utilizando un marco de arquitectura de referencia de conformidad, puede vincular las prestaciones de software y hardware integradas y los controles reglamentarios específicos con una validación de auditoría independiente. Y puede aprovechar un programa validado de forma independiente para ejecutar de forma segura las cargas de trabajo sometidas a reglamentación estricta. Tanto si utiliza un entorno de cloud privada como un entorno público, debe garantizar que su organización cumpla siempre las normas. Esto requiere una solución con la velocidad, la eficiencia y la agilidad idóneas para sus necesidades, que optimiza al mismo tiempo el proceso de cumplimiento normativo.

[6] «Gartner Says Worldwide IoT Security Spending to Reach $348 Million in 2016», Gartner Inc., abril de 2016.
[7] http://www.datacenterjournal.com/cybersecurity-trends-2017-companies-fight-back/.

La seguridad para un panorama y unas necesidades en continuo cambio

Una seguridad sólida siempre ha sido esencial para las redes empresariales y a medida que el ritmo de los cambios aumenta, se hace más necesaria que nunca. A medida que los modelos tradicionales de infraestructuras, aplicaciones y empleados evolucionan, su equipo de TI se ve sometido a más presión para proteger la empresa de nuevas amenazas emergentes.

Una capa de software presente en toda la infraestructura de aplicaciones y en todos los terminales puede ayudarle a transformar su seguridad. Le permite maximizar la visibilidad y el contexto de la interacción entre los usuarios y las aplicaciones, de tal modo que puede adaptar sus controles y políticas de seguridad a las aplicaciones que está protegiendo. Además, permite complementar de forma sencilla la solución con servicios de seguridad de terceros, para añadir una protección más inteligente.

EMPIECE HOY MISMO

Transforme la seguridad de su entorno de TI para adaptarse al panorama actual

MÁS INFORMACIÓN >

Síganos:

vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
C/ Rafael Botí, 26 - 2.ª planta, 28023 Madrid, España. Tel. +34 914125000 Fax +34 914125001 www.vmware.es

N.º artículo: 16-VMWA-4177_TS-0222_Solution_Overview_3_Key_Steps_Final
1/17