CONSEJOS Y TRUCOS PARA IMPLEMENTAR CIBERSEGURIDAD DE ÚLTIMA GENERACIÓN CON TECNOLOGÍA DE MICROSEGMENTACIÓN

Reconsiderar la estrategia de seguridad para superar los desafíos de seguridad de última generación

vmware®

Índice

La virtualización de redes ofrece ventajas de seguridad y mucho más 3

Introducción a la microsegmentación 4

Consejos y trucos para una correcta implementación de la microsegmentación 5

Cómo obtener el apoyo de los ejecutivos para una iniciativa de microsegmentación 5

Resumen e información clave para recordar 6

Los ataques informáticos se han convertido en una industria multimillonaria y tienen como fin robar información crítica y obtener acceso a los sistemas más confidenciales de las organizaciones. Detrás de estos ataques, se encuentran hackers e ingenieros muy talentosos que poseen amplios recursos financieros. Y las empresas se están dando cuenta de que las estrategias de seguridad tradicionales centradas en el perímetro ya no son eficaces.

Las infracciones de seguridad siempre suceden. Los profesionales de seguridad empresarial necesitan estar en lo correcto todo el tiempo, pero un hacker debe acertar una sola vez para lograr su cometido. Esto queda claro con las cifras de Ponemon: según los estudios que han realizado, el 89 % de las organizaciones ha sufrido una filtración de datos.[1] Los hackers también buscan robar credenciales de administrador con privilegios para atravesar el firewall y tener acceso a toda la infraestructura de TI. Por lo tanto, se deben implementar nuevas estrategias de ciberseguridad dentro del perímetro.

Sin embargo, simplemente agregar una variedad de nuevos productos exclusivos de seguridad no es la mejor estrategia tampoco. Esta estrategia añade más complejidad a la pila de seguridad y requiere más recursos humanos que son escasos. La estrategia indicada debe simplificar las operaciones diarias, proporcionar un método básico de protección y aumentar la agilidad de TI, lo cual es el objetivo de toda organización. El enfoque debe cambiar: en vez de construir una cerca más grande, se deben proteger los datos y las aplicaciones o cargas de trabajo críticas con mayor eficacia para que, si una organización sufre un ataque, la seguridad implementada pueda impedir la propagación lateral de las amenazas. Los negocios necesitan una plataforma que esté diseñada para satisfacer estas necesidades y facilitar de forma eficiente la interacción y la implementación de políticas y procesos entre los equipos de operaciones de sistemas (System Operations, SysOps), operaciones de redes (Network Operations, NetOps) y operaciones de seguridad (Security Operations, SecOps).

Para alcanzar este nuevo nivel de protección dentro de la infraestructura de TI, las organizaciones deben tener visibilidad total de la red y el tráfico. Es por eso que una red virtual es la mejor manera de alcanzar este objetivo. Una red virtual también proporciona tecnología de microsegmentación que protege de forma eficaz las cargas de trabajo críticas dentro del firewall. También optimiza la comunicación y coordinación entre los equipos de SysOps, NetOps y SecOps, lo que les permite crear e implementar políticas de seguridad detalladas a fin de proteger los recursos más valiosos de la organización. Con la virtualización de red y la microsegmentación, los tres equipos utilizan el mismo lenguaje y los mismos términos y, de esta manera, pueden implementar políticas coherentes con mayor facilidad. Los grupos también comparten la misma visibilidad, lo que les permite realizar sus tareas y actividades específicas.

La virtualización de redes ofrece ventajas de seguridad y mucho más

Este caso de uso del producto se centra en las ventajas que ofrece la implementación de la microsegmentación por medio de una infraestructura de red virtual. No obstante, una red virtual también ofrece otras ventajas muy importantes que ayudan a resolver los problemas comunes que experimentan las pequeñas y medianas empresas. Este "aprovechamiento de la solución" es importante ya que garantiza un mejor retorno de la inversión en una implementación de red virtual. Además, usar una única plataforma común para ejecutar distintas funciones simplifica las operaciones y mejora la eficiencia.

Quizá las ventajas adicionales más notables que proporciona la red virtual son las competencias fundamentales de recuperación ante desastres (Disaster Recovery, DR). Al usar una plataforma de red virtual como VMware NSX®, una organización puede migrar la configuración de redes y seguridad a un sitio diferente o a un sitio de recuperación en caso de que ocurra una falla. De forma automática, NSX reconfigura las direcciones IP, implementa políticas de seguridad y elimina la necesidad de realizar tareas manuales para sincronizar la configuración en múltiples sitios físicos.

1 "The Evolving Role of CISOs and Their Importance to the Business", (El rol dinámico de los CISO y por qué son importantes para el negocio), Ponemon Institute, 2 de noviembre de 2017

Otra ventaja que se obtiene al usar una red virtual es el balanceo de cargas. Esta función elimina la necesidad de utilizar soluciones puntuales que añaden costos y complejidad al entorno. Además, el uso del balanceo de cargas en la plataforma de red virtual suministra un panorama más completo a fin de garantizar niveles de servicio, especialmente cuando la plataforma está vinculada con información sobre las cargas de los servidores.

Las redes virtuales también optimizan el trabajo que realizan los equipos de redes y seguridad, ya que el uso de una plataforma común en la cual pueden interactuar los tres equipos de SecOps, NetOps y SysOps reduce las frustraciones diarias y elimina las exigencias de uno de los equipos que generan dificultades en los otros dos. Todos los equipos trabajan en las mismas condiciones. Y si bien la ventaja más importante que se obtiene al microsegmentar una red virtual es la reducción total o parcial del impacto de una infracción de seguridad, la microsegmentación también protege la carrera de los miembros de cada equipo: ser parte de un equipo que no pudo evitar una infracción de seguridad importante nunca se ve bien en el perfil laboral del empleado.

Introducción a la microsegmentación

La microsegmentación es una nueva solución de ciberseguridad que muchas pequeñas y medianas empresas están comenzando a utilizar. No obstante, para que la solución dé resultado, los equipos deben desarrollar un proceso eficaz de implementación. El punto de partida del proceso está dividido en tres pasos importantes:

1. **Determinar los flujos de red en la organización:** la organización se debe centrar en los flujos de datos que ingresan y salen del centro de datos, así como en los que se encuentran dentro del centro de datos. Mediante esta actividad, es muy probable que se identifiquen las ineficiencias que afectan la latencia de las aplicaciones y crean cargas en la red. Para iniciar el análisis, se deben revisar las reglas de firewall perimetral e identificar el tráfico vertical y el tráfico horizontal. Se pueden usar distintas herramientas para recopilar y analizar flujos de tráfico. Una de estas herramientas es IPFIX, un protocolo de monitoreo que se utiliza para recopilar y analizar tráfico. También puede ir más allá y usar herramientas comerciales de monitoreo para desarrollar un nivel más profundo de análisis y asignar políticas de firewall a flujos de tráfico.
2. **Identificar patrones y relaciones en el tráfico:** en el modelo de microsegmentación, se pueden crear las primeras políticas de seguridad mediante la asignación de las políticas de firewall perimetral actuales a los patrones de flujo recopilados en el paso anterior. Estos patrones de flujo proporcionan información fundamental sobre las relaciones entre las cargas de trabajo dentro del centro de datos. Es importante comprender cómo las cargas de trabajo interactúan entre ellas. Esto incluye, por ejemplo, comprender cómo una carga de trabajo específica interactúa con servicios de TI compartidos, otras aplicaciones y otras cargas de trabajo. También es importante comprender las interacciones entre distintos entornos, como los entornos de producción y de desarrollo y prueba. Después de comprender y documentar estas relaciones, obtendrá información clave para definir cómo será la interacción entre los microsegmentos y las políticas.
3. **Crear y aplicar el modelo de políticas:** una estrategia comprobada es aplicar la microsegmentación en una aplicación por vez. Esta estrategia ofrece numerosas ventajas ya que no es excesivamente compleja para el personal y le permite a la organización microsegmentar la red a su propio ritmo. Muchas pequeñas y medianas empresas comienzan con una estrategia de bloqueo predeterminado ("Default block") que impide la comunicación entre las cargas de trabajo de la aplicación sobre la que trabajan. Luego pueden comenzar a habilitar la comunicación según el análisis realizado sobre los patrones de tráfico. Si necesitan una mayor comunicación, pueden habilitarla según demanda. Pero si la inquietud es que esta estrategia de bloqueo predeterminado interrumpa el servicio, también es posible comenzar con una estrategia de permiso predeterminado ("Default allow") a fin de habilitar la comunicación. No obstante, esta estrategia se debe implementar con suma precaución. Se pueden agregar restricciones ya que se ha comprobado que no

perjudican el funcionamiento de la aplicación. Además, a medida que se vayan conociendo nuevos requisitos relacionados con las aplicaciones, los usuarios y los datos, el modelo de microsegmentación se puede actualizar a fin de adaptarse a estas nuevas exigencias. Para facilitar aun más este proceso, VMware NSX también proporciona Application Rule Manager, una herramienta automatizada que sugiere políticas de microsegmentación según los datos obtenidos.

Consejos y trucos para una correcta implementación de la microsegmentación

Como sucede con todas las soluciones tecnológicas, existen consejos y trucos específicos que pueden ayudar a que un proceso de implementación sea más eficiente y eficaz. Alguno de los más importantes son los siguientes:

- Utilice VMware Application rule Manager (ARM): ARM es una función que recopila toda la información sobre los flujos de tráfico que pueda ser útil o desee evaluar en un subconjunto de máquinas virtuales del entorno. ARM sugiere políticas de microsegmentación de forma automática según la inteligencia analítica de la herramienta para luego insertarlas en la tabla de reglas con solo unos clics.
- Defina los grupos de seguridad primero: comenzar con un sentido de la estructura y definición de los grupos de seguridad que creará le garantizará un punto de partida adecuado para la organización.
- Desarrolle convenciones de nombres coherentes para los grupos de seguridad, ya que las convenciones de nombres y los nombres en sí facilitan de forma significativa la implementación coherente de la microsegmentación. Los nombres se deben definir de forma coherente y en común acuerdo entre los equipos de SysOps, SecOps y NetOps antes de usarlos.
- Forme un equipo de funcionamiento interdisciplinario para facilitar la implementación de la microsegmentación: la implementación correcta de la microsegmentación está directamente relacionada con el trabajo que realizan los tres equipos que la utilizarán. Por lo tanto, es fundamental que el equipo que diseñe e implemente la solución incluya personal de los equipos de SysOps, SecOps y NetOps.

Cómo obtener el apoyo de los ejecutivos para una iniciativa de microsegmentación

Para garantizar el apoyo financiero y los recursos necesarios para que el proyecto se desarrolle de forma exitosa, es importante contar con el apoyo de los equipos de administración ejecutiva y administración de TI. Por lo tanto, es fundamental que hablen el mismo idioma.

Administración ejecutiva

Los directores ejecutivos se centrarán en las ventajas empresariales. La conversación se debe centrar en la capacidad de reducir el impacto de cualquier infracción de seguridad al impedir que los atacantes accedan a las aplicaciones y los datos confidenciales. Además, la microsegmentación también ayuda a satisfacer las directivas de cumplimiento mediante la reducción total o parcial de la pérdida de datos.

Los ejecutivos también deben saber que, por medio de la microsegmentación de la red, se pueden administrar y explicar con facilidad las nuevas aplicaciones, los cambios en los procesos empresariales y las nuevas demandas de seguridad. Desde un punto de vista monetario, implementar la microsegmentación en una red virtual como NSX le permitirá a la organización ahorrar dinero, ya que se elimina la necesidad de tener dos herramientas distintas de DR y balanceo de cargas. Lo que se le debe decir a estos ejecutivos es que existe una única plataforma mucho más rentable que proporciona mayor seguridad y ventajas adicionales.

CIO y vicepresidente de TI

Es probable que estos ejecutivos ya sepan cuáles son las principales ventajas de la microsegmentación; por lo tanto, la conversación con ellos se debe centrar en lo que los beneficios que la microsegmentación ofrece con respecto a sus principales inquietudes: la seguridad de los datos, la agilidad y la eficiencia de costos.

Desde la perspectiva de la seguridad de los datos, la microsegmentación es la mejor herramienta, debido a que protege de forma eficaz los datos y las aplicaciones confidenciales. Además, protege las aplicaciones y los datos de forma ágil ya que permite modificar en tiempo real las políticas de seguridad. Es en este aspecto que la microsegmentación garantiza agilidad. A medida que se publican nuevas aplicaciones o se definen nuevos orígenes de datos, las políticas de microsegmentación se pueden usar para proteger estos recursos de inmediato y, de esta manera, eliminar las "demoras" de seguridad.

La microsegmentación también permite una comunicación y coordinación clara entre los equipos de SecOps, SysOps y NetOps a fin de asegurar que la colaboración entre ellos sea coherente. Por otro lado, la plataforma de red virtual que suministra microsegmentación proporciona funcionalidad de DR y balanceo de cargas, lo que elimina la necesidad de adquirir otras soluciones costosas.

Resumen e información clave para recordar

Las pequeñas y medianas empresas se enfrentan a las mismas exigencias de ciberseguridad que las grandes empresas, pero disponen de muchos menos recursos para proteger la organización. Por lo tanto, estas empresas deben crear una estrategia más inteligente y eficiente para implementar la ciberprotección. La microsegmentación es la herramienta indicada para satisfacer estas demandas. Esta tecnología expande el firewall perimetral al brindar protección contra las amenazas que logran atravesar la seguridad perimetral e impedir que puedan acceder a los sistemas confidenciales. También es una solución más fácil de usar.

La microsegmentación de una red virtual mejora la ciberseguridad, pero la red virtual también ofrece otras grandes ventajas operativas, como la recuperación ante desastres y el balanceo de cargas, sin tener que comprar soluciones adicionales y costosas. Para obtener más información, consulte estos recursos adicionales:

- Cinco pasos hacia la microsegmentación
- Forrester: The Total Economic Impact™ of VMware NSX (informe sobre el impacto económico total de VMware NSX)
- Micro-segmentation for dummies, 2nd edition
- VMware Virtual Network Assessment (herramienta de evaluación de la red virtual de VMware)

Estos recursos, junto con los consejos y trucos detallados en este documento, le ayudarán a implementar esta importante tecnología con total éxito.

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

2/18