KONTEXTBEZOGENE MIKROSEGMENTIERUNG MIT VMWARE NSX DATA CENTER

Schutz des Netzwerks vor der lateralen Ausbreitung von Bedrohungen

Moderne Anwendungen sind komplex, verteilt und dynamisch

In einer zunehmend vernetzten Welt, in der Anwendungen und Daten unser Lebensnerv sind, suchen Unternehmen nach Möglichkeiten zur Optimierung ihres Geschäftsbetriebs. Moderne Anwendungen sind auf mehrere Rechenzentren und Clouds verteilt und reichen bis an die Grenzen der Umgebung.

Durch Virtualisierung, die Einführung von DevOps, Containerisierung und Mikroservices lassen sich Anwendungen schneller denn je entwickeln und ändern. Moderne Anwendungen sind auf die Umgebung verteilt und werden häufig geändert, was wesentliche Herausforderungen im Hinblick auf die Sicherheit mit sich bringt.

Herkömmliche Sicherheitsstrategien greifen nicht mehr

Da die Zahl der Anwendungen immer weiter zunimmt, reichen herkömmliche perimeterorientierte Sicherheitskonzepte nicht mehr aus, um Anwendungen und Anwender zuverlässig zu schützen. Angreifer haben immer wieder gezeigt, dass sie Sicherheitsmaßnahmen im Perimeter umgehen können. Innerhalb des Perimeters können sie sich dann ungehindert lateral von Server zu Server ausbreiten, um Daten auszuspionieren oder zu verschlüsseln und Lösegeld zu fordern.

Moderne, verteilte Anwendungen stellen die für IT-Sicherheit und Netzwerke zuständigen Teams häufig vor das Problem, separate Sicherheitsrichtlinien für die unterschiedlichen Bereiche der Umgebung definieren zu müssen. Daraus ergeben sich Lücken im allgemeinen Sicherheitsstatus.

Konsistente Sicherheit vom Rechenzentrum bis in die Cloud und bis zum Edge

Mit VMware NSX® Data Center lassen sich Sicherheitsrichtlinien konsistent für die gesamte Umgebung definieren – unabhängig davon, wo eine Anwendung bereitgestellt wurde und um welche Art von Anwendung es sich handelt. Richtlinien werden auf Ebene der einzelnen Workloads durchgesetzt. Dadurch können alle Workloads auf einem physischen Host segmentiert werden, ohne den Datenverkehr umständlich durch eine externe physische oder virtuelle Firewall leiten zu müssen. Diese detaillierte Sicherheit wird als „Mikrosegmentierung“ bezeichnet.

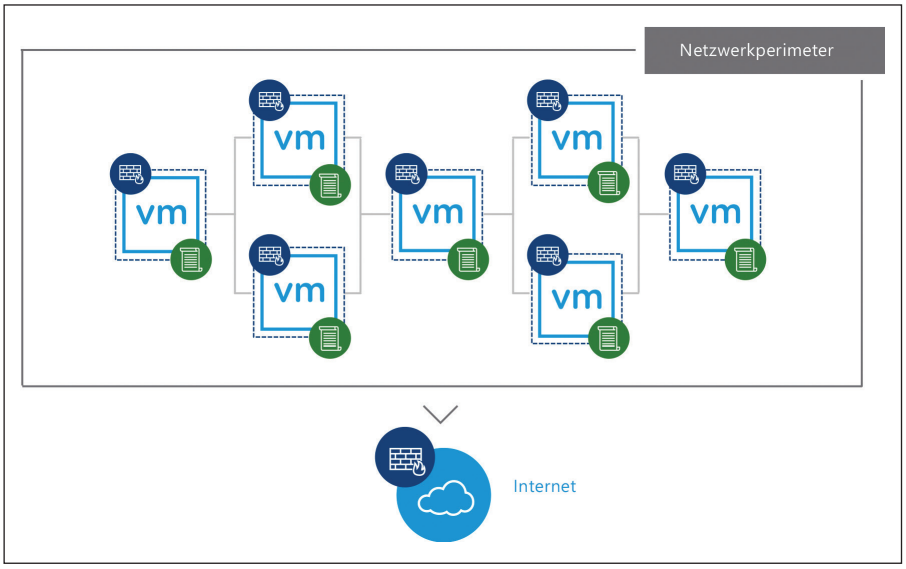

Abbildung 1: Mikrosegmentierung bezeichnet das Durchsetzen von Netzwerksicherheitsrichtlinien auf Ebene einzelner Workloads.

„Angesichts der zunehmenden Zahl von IoT-Geräten ist eine stärkere Segmentierung unseres Netzwerks für uns auch mit größeren Vorteilen verbunden. So können sich Bedrohungen nicht lateral im Rechenzentrum ausbreiten.“

CHRISTOPHER FRENZ
DIRECTOR OF INFRASTRUCTURE
INTERFAITH MEDICAL CENTER

HIGHLIGHTS

- Für moderne, dynamisch verteilte Anwendungen reichen herkömmliche perimeterorientierte Sicherheitsfunktionen nicht mehr aus.
- VMware NSX Data Center schützt Anwendungen durch Mikrosegmentierung vor der lateralen Ausbreitung von Bedrohungen.
- Sicherheitsrichtlinien lassen sich abhängig vom Kontext einer Anwendung definieren und für einzelne Workloads durchsetzen.
- Die Lösung gewährleistet konsistente Sicherheit vom Rechenzentrum bis in die Cloud und bis zum Edge.

Mit NSX Data Center erstellte Mikrosegmente werden in Software definiert und verwaltet. Dadurch sind sie agil und automatisierbar. Bei der Bereitstellung neuer Workloads übernehmen diese automatisch die Sicherheitsrichtlinien, die während des gesamten Lebenszyklus der Workloads gelten – unabhängig davon, wo sie bereitgestellt wurden oder wohin sie migriert werden.

Kontextbezogene Mikrosegmentierung und auf Anwendungen und Daten abgestimmte Sicherheit

Ebenso wichtig wie eine konsistente Bereitstellung von Richtlinien ist die Möglichkeit, den Richtlinien die Aspekte zugrunde zu legen, auf die es am meisten ankommt. NSX Data Center entkoppelt Sicherheitsrichtlinien von statischen Netzwerkattributen wie IP-Adresse, Port und Protokoll. Richtlinien können auf der Grundlage von Kontextwissen zu einer Anwendung und der Infrastruktur definiert werden. Zu einem solchen Kontext gehören Anwender-, Identitäts- und Workload-Attribute (z.B. das Betriebssystem) oder auch gesetzliche Anforderungen.

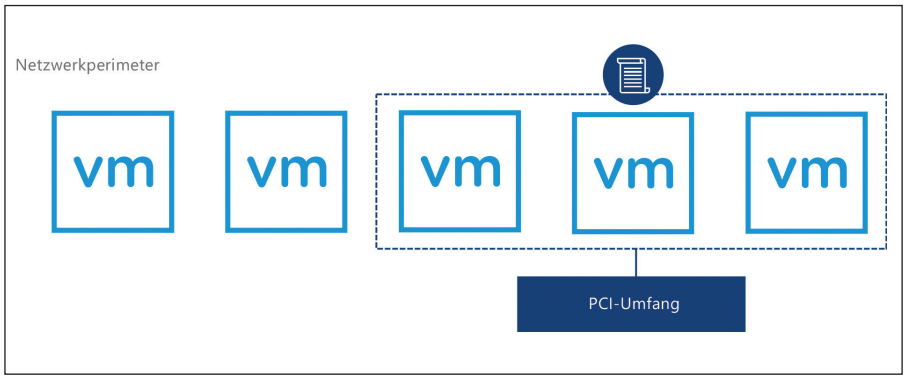

Abbildung 2: In NSX Data Center können Mikrosegmente abhängig vom Kontext definiert werden, beispielsweise auf der Grundlage gesetzlicher Anforderungen.

Die kontextbezogene Mikrosegmentierung mit NSX Data Center bietet den für die Netzwerksicherheit zuständigen Teams die nötige Flexibilität, um ihre Anwendungen und Daten abhängig von den Faktoren abzusichern, die für das Unternehmen am wichtigsten sind. So kann mit NSX Data Center beispielsweise eine virtuelle Desktop-Infrastruktur (VDI) mit einer Netzwerkrichtlinie abgesichert werden, die auf dem Anwenderkontext bis hinab auf die Ebene einzelner RDSH-Sitzungen basiert. Alternativ lassen sich Sicherheitsrichtlinien auf alle Workloads anwenden, für die die PCI-Standards gelten, ohne dabei berücksichtigen zu müssen, auf welchem System der Umgebung diese Workloads ausgeführt werden.

Erweiterte Sicherheitsservices jederzeit und überall

Mit NSX Data Center lassen sich moderne Sicherheitsservices von Drittanbietern in ein bestimmtes Mikrosegment einbinden. Anstatt den gesamten Netzwerkdatenverkehr über ein physisches Gerät oder eine virtuelle Appliance wie eine Firewall der nächsten Generation (NGFW) oder Systeme zur Erkennung von Eindringversuchen (IDS/IPS) zu steuern, kann NSX Data Center bestimmten Datenverkehr dynamisch auf diese Services auf der virtuellen Netzwerkebene leiten. Dadurch können erweiterte Sicherheitsservices zum richtigen Zeitpunkt an der richtigen Stelle eingebunden werden, was eine optimale Effizienz des Netzwerkdatenverkehrs zur Folge hat und zugleich die Effektivität der Sicherheitsservices selbst verbessert.

Transparenz des Netzwerkdatenverkehrs in der gesamten Umgebung

Der erste Schritt der Mikrosegmentierung besteht darin, den Datenverkehrsfluss in modernen Netzwerken zu verstehen. VMware Network Insight™ bietet einen umfassenden Überblick über den gesamten Netzwerkdatenverkehr im Rechenzentrum – sowohl über den physischen als auch über den virtuellen Netzwerkdatenverkehr. Nach einer Analyse dieses Datenverkehrs empfiehlt VMware Network Insight automatisch Mikrosegmentierungsrichtlinien, die von NSX Data Center umgesetzt werden können.

Machen Sie jetzt mit einem kostenlosen Virtual Network Assessment den ersten Ihres Mikrosegmentierungsprojekts zu beginnen. Weitere Informationen finden Sie unter www.vmware.com/de/products/nsx/security.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com Zweigniederlassung Deutschland Willy-Brandt-Platz 2 81829 München Telefon: +49 89 370 617 000 Fax: +49 89 370 617 333 www.vmware.com/de