VMware NSX for Horizon

AUF EINEN BLICK

VMware NSX™ for Horizon® vereinfacht und beschleunigt das VDI-Networking. IT-Administratoren können innerhalb von Sekunden Richtlinien erstellen, die virtuellen Desktops dynamisch folgen. Dabei ist keine zeitaufwendige Netzwerkbereitstellung erforderlich. Durch Erweiterung der Sicherheitsrichtlinien vom Rechenzentrum auf Desktops und Anwendungen bietet die Kombilösung außerdem eine erweiterbare Plattform, die sich in branchenführende Sicherheitslösungen integrieren lässt.

VORTEILE

- Höhere Sicherheit für virtuelle Desktops, die sich zwischen anderen Rechenzentrums-Workloads befinden
- Einfachere und schnellere Verwaltung von Netzwerk- und Sicherheitsrichtlinien für Anwender basierend auf logischen Gruppierungen, Rollen oder Tags
- Automatische Zuweisung von Richtlinien zu Desktops bei deren Erstellung, die der VM unabhängig von der zugrunde liegenden Infrastruktur folgen
- Integration von branchenführenden Antiviren- und Anti-Malware-Lösungen, Lösungen für die Abwehr von Eindringversuchen und Sicherheitsservices der nächsten Generation

Netzwerke und Sicherheit für virtuelle Desktops und Anwendungen: schnell, einfach und erweiterbar

Viele Organisationen implementieren Desktop- und Anwendungsvirtualisierung, um die Client Computing-Sicherheit zu verbessern und die Enterprise Mobility zu erhöhen. Durch die Zentralisierung von Desktops und Anwendungen werden gespeicherte Daten geschützt, der unerlaubte Zugriff auf Anwendungen wird verhindert und es wird ein effizienteres Patchen, Verwalten und Aktualisieren von Images ermöglicht.

Die Desktop- und Anwendungsvirtualisierung kann jedoch auch neue Sicherheitsrisiken hinter der Rechenzentrums-Firewall bergen, wo Hunderte oder sogar Tausende von Desktops platziert sind. Diese Desktops befinden sich in unmittelbarer Nähe zu anderen Anwendern und unternehmenskritischen Workloads, was sie weitaus anfälliger für Malware und andere Angriffe macht. Diese Angriffe können sich vom Desktop auf den Server erstrecken und eine große Angriffsfläche im Rechenzentrum offenlegen. Dieses Szenario der „Ost-West“-Bedrohung betrifft heute viele Kunden, insbesondere solche mit strengen Sicherheits- und Compliance-Vorgaben.

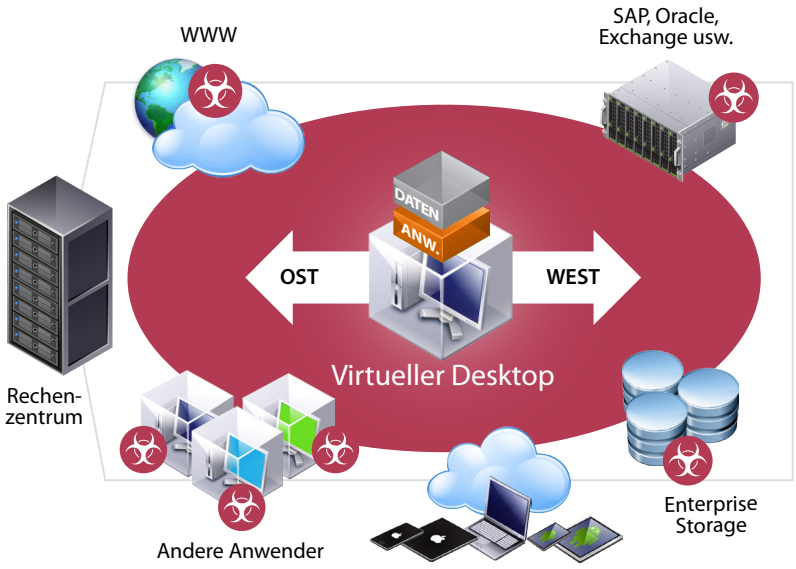

Abbildung 1: Ost-West-Sicherheitsrisiken im Rechenzentrum

Bisher mussten Organisationen zur Verwaltung einer Netzwerk- und Sicherheitsrichtlinie, die Anwendern und Workloads rund um die Uhr folgt, zudem erhebliche Investitionen in eine hardwarezentrierte Architektur tätigen, deren Betrieb komplex ist und die nur langsam an die typisch dynamische Business-Umgebung angepasst werden kann.

VMware NSX for Horizon

VMware NSX for Horizon bietet effektiven Schutz für den Ost-West-Datenverkehr im Rechenzentrum. Gleichzeitig wird der IT die schnelle und einfache Verwaltung von Netzwerk- und Sicherheitsrichtlinien ermöglicht, die den virtuellen Desktops und Anwendungen der Anwender infrastruktur-, geräte- und standortübergreifend folgen.

Abbildung 2: NSX for Horizon bietet schnelle, einfache und erweiterbare VDI-Netzwerke und -Sicherheit

Mit dieser Lösung profitieren Organisationen von schneller und einfacher VDI-Netzwerkerstellung und -Sicherheit. IT-Administratoren können innerhalb von Sekunden Richtlinien erstellen, die virtuellen Desktops dynamisch folgen. Dabei ist keine zeitaufwendige Netzwerkbereitstellung erforderlich.

Durch Erweiterung der Sicherheitsrichtlinien vom Rechenzentrum auf Desktops und Anwendungen stellt die Lösung außerdem eine erweiterbare Plattform bereit, die sich in die branchenführenden Sicherheitslösungen der VMware-Partner integrieren lässt und Kunden einen wirksamen Schutz für den gesamten Desktop bietet.

Funktionsweise

VMware NSX for Horizon verbessert die Sicherheit bei der Desktop-Virtualisierung und ermöglicht Administratoren die zentrale Definition von Richtlinien zur Eindämmung von Ost-West-Sicherheitsrisiken. Diese Richtlinien werden dann in der Hypervisor-Schicht in jedem vSphere-Host angewendet und automatisch zu den einzelnen virtuellen Desktops zugewiesen, wenn diese erstellt werden. Zum Schutz der virtuellen Desktops und der benachbarten Workloads im Rechenzentrum erfolgt mit VMware NSX eine „Mikrosegmentierung“, d.h., jeder Desktop erhält eine eigene Perimeterverteidigung. Diese komprimierte Sicherheit nutzt die Funktion von VMware NSX für verteilte virtuelle Firewalls, um den Datenverkehr zu und von jeder VM zu überwachen und nicht erlaubte Zugriffe auf Desktops und benachbarte Workloads zu verhindern. Wenn der virtuelle Desktop von einem Host zum anderen oder innerhalb des Rechenzentrums verschoben wird, folgt die Richtlinie ihm automatisch.

Funktionen und Vorteile

VMware NSX for Horizon vereinfacht und beschleunigt das VDI-Networking mit Sicherheitsrichtlinien, die Anwendern infrastruktur-, geräte- und standortübergreifend dynamisch folgen.

Schnelles und einfaches VDI-Networking

Mit VMware NSX for Horizon können Administratoren mit nur wenigen Mausklicks Sicherheitsrichtlinien für alle virtuellen Desktops erstellen, ändern und verwalten. Diese Sicherheitsrichtlinien können schnell zu Anwendergruppen zugeordnet werden, um die Einrichtung virtueller Desktops zu beschleunigen. Da die Möglichkeit zur Bereitstellung von Funktionen für virtualisierte Netzwerke besteht (wie Switching, Routing, Firewall und Lastausgleich), können Administratoren virtuelle Netzwerke für VDI ohne komplexe VLANs, ACLs oder Hardwarekonfigurationssyntax einrichten.

Automatisierte Richtlinien, die Anwendern und Desktops dynamisch folgen

Administratoren können Richtlinien festlegen, die sich dynamisch an die Computing-Umgebung des Anwenders anpassen. Netzwerksicherheitsservices können Anwendern basierend auf Rolle, logischer Gruppierung, Desktop-Betriebssystem und mehr zugeordnet werden – unabhängig von der zugrunde liegenden Netzwerkinfrastruktur. Jeder Desktop-VM werden mit Erstellung des Desktops automatisch zentral verwaltete Richtlinien zugewiesen. Dies ermöglicht Organisationen eine zuverlässige Skalierung mit umfassendem Schutz für den virtuellen Desktop, unabhängig davon, wo dieser sich innerhalb des Rechenzentrums befindet.

Plattform für erweiterte Sicherheit

VMware NSX bietet eine erweiterbare Plattform, die in die erstklassigen Funktionen der etablierten Sicherheitspartner von VMware integriert werden kann. Durch dynamisches Hinzufügen von Services kann die Sicherheit virtueller Desktops vom Rechenzentrum auf Desktops und Anwendungen ausgeweitet werden. Das Partnernetzwerk, das u.a. Trend Micro, Intel Security und Palo Alto Networks umfasst, bietet Lösungen, die Betriebssystem, Browser, E-Mail und mehr schützen – mit Antiviren- und Anti-Malware-Funktionen, Funktionen für die Abwehr von Eindringversuchen und Sicherheitsservices der nächsten Generation.

Weitere Informationen

Besuchen Sie die VMware-Website und folgen Sie uns auf Twitter, um weitere Informationen zu Horizon und VMware NSX zu erhalten.

VMware Horizon – Ressourcen

Web: http://www.vmware.com/de/products/horizon-view

Blog: http://blogs.vmware.com/euc/

Twitter: @VMwareHorizon

VMware NSX – Ressourcen

Web: http://www.vmware.com/de/products/nsx/

Blog: http://blogs.vmware.com/networkvirtualization/

Twitter: @VMwareNSX

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
Zweigniederlassung Deutschland Freisinger Str. 3 85716 Unterschleißheim/Lohhof Telefon: +49 89 370 617 000 Fax: +49 89 370 617 333 www.vmware.com/de