Techniktipps

10 Tipps zur Steigerung der Sicherheit Ihrer VMware Horizon-Bereitstellung

Schutz Ihrer IT im Zeitalter der Virtualisierung

IT-Organisationen kennen die Vorteile der Business Mobility. Sie möchten sich deshalb von ihren unflexiblen Legacy-Architekturen lösen und diese gegen den flexiblen Desktop der nächsten Generation eintauschen. Durch eine Desktop-Transformation mit VMware® Horizon® genießen Anwender flexiblen Zugriff auf virtualisierte Desktops und Anwendungen über eine einzige Plattform.

Jedoch birgt dieses neue Maß an Anwenderflexibilität, einschließlich der BYOD-Unterstützung, ein zunehmendes IT-Sicherheitsrisiko. Ein vielfältigerer Zugriff erfordert auch eine größere Sorgfalt beim Schutz der Daten. In einer Zeit, in der die IT-Sicherheit in Unternehmen bereits sehr aufwändig ist, müssen Sie sich darauf verlassen können, dass Ihre Desktop-Transformation sowohl effizient als auch sicher vollzogen wird – denn die Anzahl an Sicherheitsvorfällen wächst jährlich um 66 Prozent, wobei sich die Kosten pro Vorfall auf 5,9 Millionen US-Dollar[1] belaufen.

WAS IST VMWARE HORIZON?

VMware Horizon erweitert die Leistungsfähigkeit der Desktop- und Anwendungsvirtualisierung. Die Lösung bietet Anwendern virtualisierte Desktops und Anwendungen über eine einzige Plattform. Diese Desktop- und Anwendungsservices – zu denen RDS-gehostete Anwendungen und mit VMware ThinApp® paketierte Anwendungen zählen – sind unabhängig von Geräten, Medien, Verbindungen und Standorten über eine einheitliche Arbeitsumgebung zugänglich. Weitere Informationen zu Horizon erhalten Sie unter vmware.com/go/horizon.

Virtualisierte Anwender erfordern neue IT-Sicherheitsüberlegungen

Während die Desktop-Transformation Anwendern und IT-Organisationen eine Reihe von Vorteilen bietet, z.B. OpEx-Einsparungen, einfacheres Management, gesteigerte Anwenderproduktivität, Hochverfügbarkeit und CapEx-Senkungen, dürfen IT-Führungskräfte die damit verbundenen Herausforderungen nicht außer Acht lassen.

- Durch die Bereitstellung von Desktops und Anwendungen in Echtzeit ermöglicht die Desktop-Transformation den IT-Administratoren, neue Anwender schnell einzurichten und echte „zustandsfreie Desktops“ in Sekunden bereitzustellen. Wie skalieren Sie Bereitstellungen rasch horizontal, ohne dabei die Transparenz oder Kontrolle über Ihr Netzwerk zu verlieren?

- Ihre Organisation bedient möglicherweise Tausende – oder gar Hundertausende – Anwender, die direkten Kontakt mit geschäftskritischer Infrastruktur haben. Werden virtuelle Desktops kompromittiert, kann dies ein äußerst kostspieliges Datenleck nach sich ziehen.

- Die „Ost-West“-Aktivität, also der interne Datenverkehr zwischen Servern oder Desktops, kann Sie angreifbar machen. Alltägliche Aktionen von vertrauenswürdigen Anwendern – z.B. mit Viren infizierte E-Mails oder ein falscher Klick im Internet – können eine Bedrohung für das Netzwerk darstellen.

Hier sind zehn Techniktipps, wie Sie sich und Ihre Horizon-Bereitstellung besser schützen können:

1 Golden Images

Mit einem „Golden Image“, einer Vorlage für virtuelle Desktops, können IT-Teams virtuelle Desktops so konfigurieren, dass Anwender nur geschäftlich relevante Aktivitäten sehen. Folglich kann sich die IT ganz auf die Bereinigung des Golden Image konzentrieren, das sich innerhalb des Rechenzentrums befindet. Falls ein virtueller Desktop kompromittiert wird, kann die IT das Image löschen und im Gegenzug einen neuen Desktop bereitstellen.

2 Abgestufte Sicherheit

In einer virtualisierten Umgebung müssen Sicherheitsrisiken an verschiedenen Fronten beachtet werden. Durch das Ergreifen zusätzlicher Sicherheitsmaßnahmen wie Anwendungs-Whitelists mithilfe von VMware NSX™ können Sie Anwendungen genehmigen, die auf Ihrem Netzwerk ausgeführt werden dürfen. Diese Vorgehensweise sorgt für mehr Sicherheit im Netzwerk und die Einhaltung der Compliance durch die Anwender selbst. Darüber hinaus lässt sich so dem Problem der Schatten-IT entgegenwirken, wenn Anwender und Geschäftsbereichsleiter Business-Anwendungen und Services ohne Kenntnis der IT nutzen. Die Anwendungsintegrität lässt sich auch durch Verfahren für die Anwendungsbereitstellung aufrechterhalten. Hierzu eignen sich Tools wie VMware App Volumes™.

1. PwC, „Managing cyber risks in an interconnected world“, September 2014

ÜBER VMWARE APP VOLUMES

Mit VMware App Volumes können IT-Administratoren innerhalb von Sekunden Anwendungen und Daten für Anwender oder Desktops in großem Umfang bereitstellen. Mit App Volumes können Sie die Kosten für Infrastruktur und Management durch die Nutzung von verwalteten Volumes reduzieren. Mitarbeiter können Anwendungen wie nativ installierte Anwendungen nutzen. Darüber hinaus folgen diese Anwendungen den Mitarbeitern über Sitzungen und Geräte hinweg.

Überzeugende Vorteile:

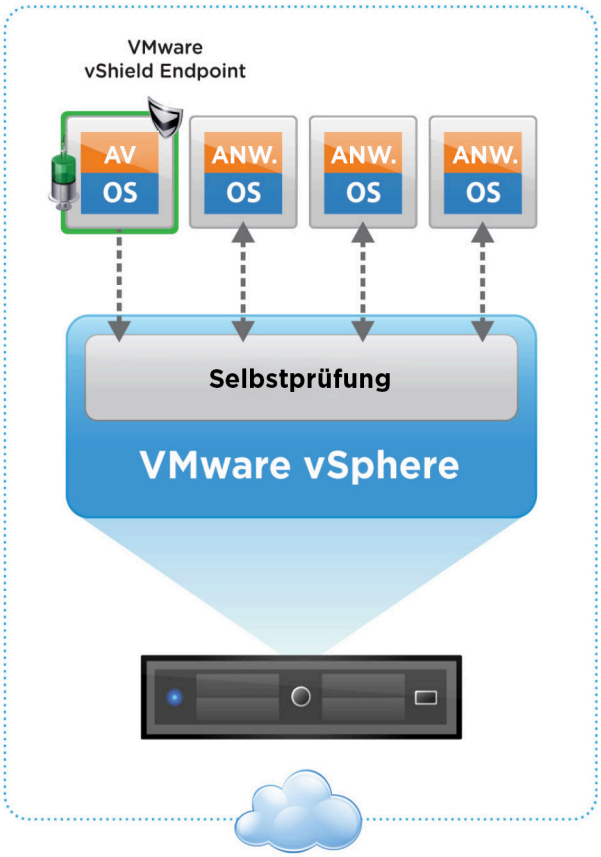
- Zentrales Anwendungsmanagement
- Einfache Anwendungsbereitstellung
- Anwendungsbereitstellung pro Anwender

Weitere Informationen zu App Volumes erhalten Sie unter https://www.vmware.com/de/products/appvolumes/.

3 Keine Kompromisse bei der Sicherheit von Endpunktgeräten

Durch Investitionen sowohl in Hardware- als auch Softwarefunktionen lässt sich die Sicherheit Ihrer Horizon-Endpunktgeräte steigern. Bei Verlust oder Diebstahl eines Geräts etwa verhindern hardwarebasierte Funktionen wie Trusted Platform Module (TPM) das Starten des Geräts durch Plattformauthentifizierung. Außerdem müssen Sie sicherstellen, dass Virenschutzdefinitionen, Anti-Malware-Software und die Firewall des Endpunktgeräts immer auf dem neuesten Stand und aktiviert sind.

Vielleicht sind Ihnen IT-Administratoren bekannt, die Virenschutzpraktiken auf ihren virtuellen Desktops umgehen, um deren Auswirkungen auf Arbeitsspeicher, CPU und Festplatten zu reduzieren. Jedoch kann der Schaden, der durch einen Virus auf einem virtuellen Desktop angerichtet wird, genauso groß sein wie bei einem Virus auf einem physischen Desktop, insbesondere dann, wenn die regelmäßige Aktualisierung der virtuellen Maschinen (VMs) vernachlässigt wird. VMware vShield Endpoint™ stellt eine ausgezeichnete Alternative dar: Sie lagert die Verarbeitung von Virenschutz- und Anti-Malware-Agents von VMs auf eine sichere virtuelle Appliance aus.



Zuletzt können Sie die Sicherheit Ihrer Endpunktgeräte mit Lösungen von Drittanbietern weiter steigern. Anbieter wie Trend Micro Deep Security bieten erweiterte Funktionen wie Malware-Schutz, IDS/IPS, Integritätsüberwachung, URL-Filterung und Patching. Tief greifende Sicherheitsfunktionen werden auf Hypervisor-Ebene ausgeführt und bieten umgehend Schutz, sobald ein neuer virtueller Desktop bereitgestellt wird. Außerdem folgen die Sicherheitsfunktionen automatisch dem Endpunkt, egal wohin dieser im Rechenzentrum wandert.

ÜBER VMWARE VSHIELD ENDPOINT

VMware vShield Endpoint erhöht die Sicherheit von virtuellen Maschinen und verbessert die Performance beim Schutz von Endpunkten in erheblichem Umfang. vShield Endpoint dient der Nutzung vorhandener Investitionen und ermöglicht Kunden das Management von Virenschutz- und Anti-Malware-Richtlinien für virtualisierte Umgebungen über dieselben Managementoberflächen, die sie für die Sicherheit von physischen Umgebungen verwenden. Die Lösung lässt sich in Produkte der folgenden Anbieter integrieren: Trend Micro, Intel Security, Symantec, Sophos und Kaspersky.

4 Implementierung von Gruppenrichtlinien und erweiterten Richtlinien

Gruppenrichtlinien können zur Abwendung von Gefahren beitragen, wenn ein Verstoß an einem Endpunkt erkannt wird, z.B. eine veraltete Virenschutz- oder Anti-Malware-Software. Mit einer Gruppenrichtlinie können Sie außerdem Konsistenz über virtuelle Desktops hinweg erzwingen, Services deaktivieren, die der Anwender nicht benötigt, und Zugriff auf bestimmte Teile des Desktops oder Netzwerks sperren. Durch Richtlinieneinstellungen lässt sich darüber hinaus verhindern, dass Anwender Änderungen am Desktop vornehmen können, die zu Sicherheitsrisiken führen.

Außerdem lohnt es sich, einen Blick auf VMware User Environment Manager™ zu werfen – eine leistungsstarke, einfache und skalierbare Lösung für das Management von Anwendungsumgebungen, die das Anwendungs- und Anwendermanagement sowie die Einrichtung dynamischer Richtlinien erleichtert. Mit Richtlinien und Anwendungseinstellungen, die Anwendern über Geräte und Standorte hinweg folgen, sowie einem Zugriffsmanagement, das darauf basiert, ob der Anwenderzugriff über einen internen Desktop oder ein externes Gerät erfolgt, lassen sich alltägliche IT-Abläufe nicht nur effizienter, sondern auch sicherer gestalten.

Durch Verwendung der Horizon Group Policy Administrative(ADM)-Vorlagendateien, welche die Active Directory-Gruppenrichtlinie erweitern, können Sie auf dem Desktop eingehende und ausgehende Informationen regulieren, z.B. durch Deaktivierung der Zwischenablage.

5 Sicherstellen einer geeigneten Architektur

Eine sichere Bereitstellung von Horizon hängt stark von der Firewall- und DMZ-Konfiguration sowie der Trennung von Desktop-Pools ab. Platzieren Sie zunächst eine Firewall zwischen dem Rechenzentrumsnetzwerk und dem Büronetzwerk. Falls Sie virtuelle LANs oder Firewalls nutzen, um Server von Desktops zu segmentieren, müssen Sie sicherstellen, dass sich Ihre VDI-Umgebung auf der Desktop-Seite der Firewall befindet.

Um die Sicherheit für Remote-Anwender zu gewährleisten, müssen Sie Ihren Sicherheitsserver oder Access Point in der DMZ einrichten. So bieten Sie Anwendern einen Verbindungspunkt, ohne direkten Zugriff auf das Netzwerk zu gewähren. Auch im Hinblick auf Gateway-Funktion müssen Sie die Vorteile von Access Point gegenüber einem Sicherheitsserver berücksichtigen. Mit Access Point implementieren Sie beispielsweise eine gehärtete, gesperrte, vorkonfigurierte Linux-basierte virtuelle Maschine anstatt lediglich einer Software, die auf einem allgemeinen Windows-Betriebssystem ausgeführt wird. Außerdem können Sie Access Point mit einem einzelnen View Connection Server oder für eine höhere Verfügbarkeit mit einem Load Balancer verbinden, der mehreren View Connection Servers vorgeschaltet ist.

Eine Trennung der Desktop-Pools wird empfohlen, wenn Desktops vom Rest der Organisation getrennt werden müssen, z.B. die Desktops von Personalabteilung, freien Mitarbeitern und Entwicklern. Durch die Verwendung von VMware NSX als Add-on für die VMware vSphere®-Plattform kann die Trennung erleichtert werden.

6 Mehrfach- und Pass-Through-Authentifizierung

Dank Kompatibilität mit führenden Mehrfachauthentifizierungslösungen wie RSA SecurID, VASCO DIGIPASS, SMS Passcode und SafeNet bildet Horizon die Grundlage für eine grundlegende Desktop-Sicherheit. Horizon kann außerdem mit einer Pass-Through-Authentifizierungstechnologie verwendet werden, bei der Anwender ihre Anmeldeinformationen zweimal eingeben oder sich mit einem gesonderten Konto auf dem Desktop anmelden.

Ziehen Sie auch VMware Identity Manager™ in Betracht. Diese Lösung für das Identitätsmanagement ermöglicht bedingungsabhängigen Zugriff und Single Sign-On (SSO), damit Sie die Business Mobility erleichtern und eine vollständige Anwendererfahrung auf Geräten aller Art ohne Beeinträchtigung der Sicherheit Ihrer Umgebung bieten können.

7 Schutz von Peripheriegeräten

Bei externen Laufwerken besteht das Risiko, dass schädliche Viren ins Netzwerk gelangen oder Anwender sogar geistiges Eigentum stehlen können. Mit Horizon können Sie Datenschutzmaßnahmen ergreifen, die das Kopieren von Daten auf lokale tragbare Speichergeräte wie USB-Sticks und ungesicherte Drucker unterbinden. Wenn darüber hinaus die Umleitungsfunktion des Client-Laufwerks auf dem virtuellen Desktop installiert ist, können Anwender „remote“ auf die auf ihrem lokalen PC gespeicherten Dateien zugreifen. Komprimierung und Verschlüsselung erfolgen bei der Übertragung von Dateien vom Endpunkt auf den virtuellen Desktop.

8 Durchführung regelmäßiger Wartungen/Scans

Bei einem sorgfältigen Umgang mit dem Thema Sicherheit darf auch die Wartung nicht vergessen werden. Mithilfe der folgenden Maßnahmen vermeiden Sie Sicherheitslücken:

- Aktualisieren Sie Software mit Virenschutz- und Anti-Malware-Funktionen, die das zuständige Personal vor bevorstehenden Angriffen warnen.
- Definieren Sie eine akzeptable Richtlinie für das regelmäßige Recomposing oder Aktualisieren von Horizon-Desktops, um Sicherheitspatches, Anwendungspatches und -Updates sowie Betriebssystem-Updates einzuspielen.
- Wenden Sie Sicherheitspatches und -Updates nicht nur regelmäßig auf das Betriebssystem, sondern auch auf Anwendungen im „Golden Image“ an.
- Führen Sie regelmäßige Portscans auf den primären und sekundären Firewalls durch, um sicherzustellen, dass die Firewall-Richtlinie ordnungsgemäß implementiert wurde und kein unautorisierter Zugriff auf die DMZ möglich ist.
- Analysieren Sie das Datenverkehrsmuster hinsichtlich des innerhalb der Firewalls und DMZ erlaubten Datenverkehrs und überwachen Sie die Firewall im Hinblick auf ungenutzte Ports.
- Führen Sie regelmäßige Audits durch. Unterziehen Sie die Konfiguration des Lastausgleichs und die Firewall regelmäßigen Audits, um zu prüfen, ob ein unautorisierter Zugriff stattgefunden hat.
- Beim Anwenden von Patches und Updates müssen Sie zuerst das übergeordnete Image aktualisieren, testen und dann schnell und zuverlässig auf allen virtuellen Desktops bereitstellen.

WARUM AKTUALISIEREN? VERBESSERUNG VON SICHERHEIT UND PERFORMANCE

Durch Aktualisierung Ihrer virtuellen Desktops beim Abmelden stellen Sie sicher, dass Anwender stets einen bereinigten und funktionsfähigen Desktop erhalten. Neben der gesteigerten Sicherheit durch das Entfernen potenzieller Viren und Malware von dem virtuellen Desktop profitiert der nächste Anwender von derselben Anwenderfreundlichkeit und Performance.

9 Sicherheit des Netzwerks

Die Kombination aus VMware NSX und Horizon stellt das Framework für Automatisierung und Mikrosegmentierung bereit. Mit VMware NSX können Sie eine verteilte Firewall pro Port bereitstellen. Dadurch haben Sie die Möglichkeit zu steuern, welcher Datenverkehr von einem Desktop empfangen wird, woher dieser stammt und wohin Datenverkehr gesendet werden darf. Außerdem können Sie Zonen erstellen, um freie Mitarbeiter zu isolieren und das Netzwerk vor hoch riskantem Web-Browsing zu schützen.

Durch Mikrosegmentierung erhält jede virtuelle Maschine einen eigenen Perimeterschutz. Eine verteilte Firewall überwacht den eingehenden und ausgehenden Datenverkehr jeder einzelnen VM und verhindert so unautorisierten Zugriff und das Eindringen von Bedrohungen in das Rechenzentrum. Sie können das Sicherheits-Provisioning automatisieren und Workloads in Mikrosegmente aufteilen. So erreichen Sie eine schnellere und sicherere Skalierung bei gleichzeitiger Steigerung der Performance des virtuellen Desktops.

10 Minimieren des Risikos

Bei der Vermeidung von Schwachstellen spielt der Detailgrad von Genehmigungen eine besonders große Rolle. In einer Standardumgebung können Anwendungen auf andere Anwendungen zugreifen. Bei Malware kann eine Anwendung zum Beispiel den Arbeitsspeicher einer anderen ausgeführten Anwendung überschreiben. Dies stellt ein potenziell hohes Schadensrisiko dar, da alles, worauf die Anwendung Zugriff hat, kompromittiert wird. Bei der Anwendungsvirtualisierung durch VMware ThinApp erhält jede Anwendung ihre eigene virtuelle Betriebssystem(VOS)-Sandbox. Dies führt dazu, dass Anwendungen oder deren Dateien vor anderen Anwendungen verborgen werden. Gewisse Teile des Betriebssystems können sogar ganz von einer Anwendung isoliert werden. So lässt sich der Umfang einer potenziellen Infektion einschränken und die Infektion im Falle einer Sicherheitslücke auf einfache Weise entfernen.

HÄUFIGE – JEDOCH MANCHMAL VERGESSENE – SICHERHEITSÜBERLEGUNGEN:

- Vermeiden Sie, wenn möglich, die Erteilung von Administratorrechten an Anwender.
- Behandeln Sie virtuelle Desktops im Hinblick auf die Sicherheit wie herkömmliche Desktops, indem Sie Virenschutzanwendungen, die vorgeschriebene Einhaltung von Richtlinien und Sperrungstools nutzen.
- Ersetzen Sie selbstsignierte Standardzertifikate zum Schutz von SSL-Kanälen durch Zertifikate einer vertrauenswürdigen Zertifizierungsstelle, um Man-in-the-Middle-Angriffe zu reduzieren.
- Schränken Sie die Möglichkeit für den Zugriff auf sensible Daten ein, wenn Anwender einen zweiten virtuellen Desktop für Remote-Zugriff oder Telearbeit verwenden.
- Nutzen Sie VMware vRealize® Operations Manager™ zur Überwachung von Datenverkehrsspitzen.
- Nutzen Sie bei externen Bereitstellungen Sicherheitsserver oder Access Point-Server in der DMZ.

Fazit

Trotz höherer Anwenderflexibilität und Managementeffizienz macht eine Desktop-Transformation alleine Ihre IT-Organisation nicht sicherer. Sie kann ihr Unternehmen, wie oben erwähnt, sogar größeren Gefahren aussetzen, wenn Sie nicht proaktiv handeln. Mit einer ordnungsgemäßen Implementierung und Umsetzung der in diesem Dokument erläuterten Tipps können Sie nicht nur Ihre Netzwerksicherheit verbessern, sondern auch all die IT-Vorteile genießen, die eine Desktop-Transformation mit sich bringt.

Testen Sie Horizon kostenlos mit einem Hands-on Lab. Es lässt sich innerhalb von wenigen Minuten ohne Installation im Browser starten. Registrieren Sie sich jetzt: https://www.vmware.com/horizon-hol-labs.

VMware online

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

Twitter: @vmwarehorizon

Facebook: https://www.facebook.com/vmwarehorizon

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

Artikelnr.: 15-VMWA_2942_TechTipsForHorizon_FINAL 01/16