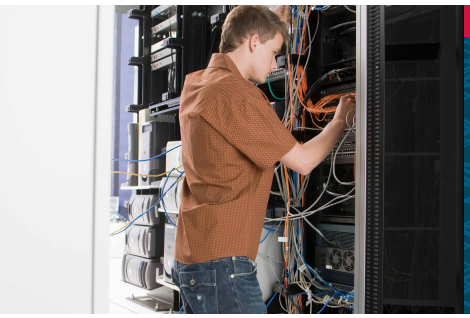

Mehr Virtualisierung, gleicher Schutz

Wichtige Sicherheitsentscheidungen für virtualisierte Umgebungen

Mit zunehmendem Einsatz von Virtualisierungstechnologien für geschäftskritische Server und Desktops müssen IT-Abteilungen immer mehr Endbenutzer, Arbeitsprozesse und Standorte sowie neue Anforderungen wie Just-in-Time-Bereitstellung und Selbstverwaltung unterstützen. McAfee® Management for Optimized Virtual Environments AntiVirus (McAfee MOVE AV) optimiert Sicherheitssysteme für die speziellen technischen und Verwaltungsanforderungen der Virtualisierung. Die Lösung unterstützt Sie bei der sicheren Nutzung aller Virtualisierungsvorteile und gewährleistet gleichzeitig hohe Benutzerfreundlichkeit.

Für CIOs haben Virtualisierungstechnologien im Jahr 2012 höchste Priorität.[1] Durch die Unterstützung wichtiger Initiativen wie Cloud Computing und BYOD (Bring your own Device) sowie die Konsolidierung von Server- sowie Rechenzentren können sie mit Virtualisierung zwei wichtige unternehmerische Ziele miteinander verbinden: Kostensenkung und geschäftliche Flexibilität. Virtualisierung ist eine wichtige Komponente für den Unternehmenserfolg. Dabei stellt sie jedoch – verglichen mit herkömmlichen physischen Installationen von Sicherheitslösungen – ganz eigene Herausforderungen in Bezug auf Arbeitsabläufe und Risiko-Management. Das neue Einsatzmodell für Virtualisierung erfordert eine Neubewertung traditioneller Sicherheitsprozesse, Richtlinien und Bereitstellungsoptionen.

Leistungsengpässe

Das offensichtlichste Problem ist die Scan-Leistung. In einer traditionellen Umgebung wird auf jedem System – sei es ein Desktop-Computer oder Server – lokal eine Malware-Schutz-Software ausgeführt. Diese scannt die Daten beim Zugriff oder nach einem Zeitplan, um die Sicherheit des Hosts zu gewährleisten. Dieses Modell ist jedoch für virtuelle Umgebungen zu ressourcenintensiv. Im Fall so genannter „Scan-Stürme" werden sämtliche verfügbare Speicher- und Verarbeitungsressourcen des Hypervisors belegt und so der Start neuer Benutzersitzungen blockiert. Um die Verfügbarkeit zu gewährleisten, entschieden sich viele Administratoren bislang dafür, Scans zu deaktivieren oder Software-Aktualisierungen zu überspringen.

Seit der breiten Einführung in Unternehmen werden virtualisierte Umgebungen für Internetkriminelle, die Schwachstellen in Software und Konfiguration ausnutzen, immer interessanter. Ohne regelmäßige und aktive Sicherheits-Scans stellt die virtualisierte Infrastruktur für Datendiebe und Angreifer ein offenes Scheunentor dar.

Veraltete Sicherheits-Software

Das erste Ziel von Kriminellen sind Abbilder, die ohne aktuellen oder gänzlich ohne Malware-Schutz ausgeführt werden. Daher müssen Sie Sicherheits-Software auf ausgeführten und Offline-Abbildern sowie auf Abbild-Vorlagen (so genannten „Gold-Standard"-Abbildern) betreiben. Nur mit frisch aktualisierten Systemsicherheitsfunktionen sowie Malware-Schutzmaßnahmen ist die Hacker-Abwehr effektiv.

In einer ausgebauten virtualisierten Desktop-Infrastruktur (VDI) werden unter Umständen tausende virtuelle Maschinen (VMs) eingesetzt, die täglich bereitgestellt und stillgelegt werden. Dadurch ist eine zuverlässige Sicherheitsverwaltung kaum möglich. Während die Sicherheitsaktualisierungen für permanent aktive physische Server auf günstige Zeiten – zum Beispiel auf Zeiten mit typischerweise geringer Last – verlegt werden können, muss bei Desktop-Benutzern Rücksicht auf die dynamischen Abläufe von VMs genommen werden. Aktive Abbilder werden offline geschaltet, gespeichert oder sind über Nacht bzw. für einige Stunden inaktiv. Dennoch erwarten Benutzer, sofort und ohne Verzögerungen durch Boot- und Scan-Vorgänge auf ihre virtualisierten Systeme zugreifen zu können.

Kombinierte Ressourcen

Durch Rechenzentren werden die Prozesse noch komplizierter. Server, Speicher und Netzwerkressourcen werden integriert, um maximale Auslastung zu erreichen. Diese Verschmelzung hat jedoch zwei Konsequenzen. Erstens gehen Sicherheitvorteile verloren: Die physische Trennung von Datenbanken, Anwendungs- sowie Web-Servern und anderer Software bildete bislang den besten Schutz vor Malware-Autoren und Hackern. Um dies zu kompensieren, müssen stärkere Sicherheitsfunktionen in die virtualisierten Systeme integriert werden.

Zweitens müssen sich die Verwaltungsprozesse ändern, da die zuvor getrennt betriebenen Server-, Speicher- und Netzwerkfunktionen über eine zentrale Verwaltungskonsole kontrolliert werden. Während für diese Ressourcen bislang separate Administratoren und Richtlinien zuständig waren, müssen sie jetzt von einer Richtlinie abgedeckt werden und in einer Umgebung koexistieren. Dabei werden sie häufig von einem einzigen Virtualisierungs-Administrator verwaltet, einem „Super User". In dieser Situation fordern Prozesse und Warnungen die Aufmerksamkeit von Administratoren. Zudem müssen eventuell Richtlinien an die geänderte Umgebung angepasst werden. Daher benötigen die Administratoren Möglichkeiten zur Kooperation bei den Arbeitsabläufen.

„McAfee MOVE AV bietet der virtualisierten Umgebung von McKesson umfassenden und nahtlosen Schutz vor Malware. Wir setzen immer stärker auf neue Technologien wie Cloud-Computing-Lösungen. Daher bietet uns die Implementierung von McAfee MOVE AV zusätzliche Sicherheit für unsere virtuelle Umgebung. Diese Lösung vereinfacht die Planung sowie Bereitstellung und gewährleistet, dass jedes System mit dem gleichen Schutz ausgestattet ist."

– Patrick Enyart
Senior Director
McKesson Information Security

Verschiedene Anbieter

Zu diesen Veränderungen gesellen sich in vielen Unternehmen Herausforderungen durch den Einsatz mehrerer Anbieter. Jeder Virtualisierungsanbieter hat andere Stärken, und viele Unternehmen benötigen eine zweite Quelle für geschäftskritische Software. Daher werden in Ihrer Umgebung möglicherweise verschiedene Hypervisoren eingesetzt. Sie müssen Abbilder sichern und Ihre Compliance nachweisen, gleichzeitig jedoch die Besonderheiten der jeweiligen Lösung beachten.

Compliance

Zusätzlich zur Bewältigung dieser Probleme müssen Sie Compliance-Vorschriften einhalten, die von physischen Systemen bekannt sind und dort immer noch gefordert werden, sowie die Einhaltung dieser Vorschriften nachweisen können. Die aktuellen Vorgaben schreiben die regelmäßige Pflege von Malware-Schutzmechanismen vor. Das Datenschutzgesetz von Massachusetts (201 CMR 17:00) fordert beispielsweise „im Rahmen des Angemessenen aktuelle Systemsicherheits-Software-Agenten, die Malware-Schutzfunktionen sowie im Rahmen des Angemessenen aktuelle Patches und Virendefinitionen umfassen müssen, oder eine Version dieser Software, für die aktuelle Patches und Virendefinitionen bereitgestellt werden können und regelmäßig mit den neuesten Sicherheitsaktualisierungen versorgt werden."

Alle diese Probleme stellen im Alltag praktische Hindernisse für den Sicherheitsbetrieb virtualisierter Systeme in einem dynamischen Bedrohungsszenario dar. Traditionelle Sicherheitsmodelle aus der physischen Welt müssen für den Einsatz in virtualisierten Umgebungen erweitert oder ersetzt werden.

Optimierte Abläufe mit McAfee MOVE

Als McAfee vor einigen Jahren die Zusammenarbeit mit den Anbietern von Virtualisierungslösungen begann, zeichneten sich die oben genannten Probleme mit den Betriebsabläufen ab. Unsere Antwort war eine spezialisierte Technologie, dank der sich unsere herausragenden Sicherheitsfunktionen auf virtualisierte Server- und Desktop-Umgebungen ausdehnen lassen. McAfee MOVE AntiVirus bietet Malware-Schutz und Sicherheit, ohne dass Sie Kompromisse bei der Leistung eingehen müssen. Mit dieser Lösung können Sie leistungsfähige Virtualisierungstechnologien optimal nutzen und dabei die Benutzerproduktivität sowie Sicherheit auf dem Gastbetriebssystem in der VM gewährleisten.

Mit unserer Lösung können Sie flexibel das für Sie ideale Bereitstellungsmodell auswählen, z. B. eine Variante, die auf mehreren Virtualisierungsplattformen eingesetzt werden kann, oder eine agentenlose Variante, die die VMware vShield-APIs nutzt. In beiden Fällen können Sie die bewährten und branchenweit führenden[2] Malware-Schutzlösungen von McAfee vollständig nutzen. Die Ergänzung von Eindringungs- sowie Web-Anwendungsschutz bedeutet zusätzliche Sicherheit vor gefährlichen Angriffen.

Scans bei Bedarf und Notwendigkeit

McAfee MOVE AntiVirus entlastet Hypervisor-Ressourcen, damit sie andere Funktionen übernehmen können, und gewährleistet gleichzeitig, dass die regelmäßigen Sicherheits-Scans den Richtlinien entsprechen. Eine abgesicherte virtuelle oder physische Appliance übernimmt Scan-Aufgaben, überwacht Konfigurationen und aktualisiert DAT-Signaturen. Dadurch kann sich der Hypervisor auf die Unterstützung von Gastabbildern beschränken.

Durch die Integration von McAfee MOVE AntiVirus in die Virtualisierungsverwaltungs-Software können wir „Scan-Stürme" vermeiden, die dadurch verursacht werden, dass zahlreiche Abbilder gleichzeitig ihre Bereitstellung sowie Scan-Vorgänge anfordern. Außerdem kann McAfee MOVE AntiVirus for Virtual Servers die Scans auf Grundlage der Verfügbarkeit von Hypervisor und Ressourcen intelligent planen. Aktive VMs müssen zum Scannen nicht offline geschaltet werden. Wenn die Abbilder jedoch offline geschaltet werden, kann McAfee sie scannen und aktualisieren, um sie für den nächsten Einsatz bereit zu halten.

Anwendung neuester Erkenntnisse

McAfee MOVE AntiVirus schützt VMs mithilfe des gleichen McAfee VirusScan®-Moduls, das in unseren marktführenden Virenschutzprodukten für physische Umgebungen zum Einsatz kommt. Um die Aktualität von Scans zu gewährleisten, ohne die Leistung einzuschränken, lädt die Appliance die aktuellsten Signaturen lediglich auf den Offload-Scan-Server herunter und wendet sie dort an, anstatt die einzelnen VMs zu belasten. McAfee MOVE AntiVirus ruft die Bedrohungsinformationen von McAfee Global Threat Intelligence™ ab und erhält in Echtzeit Reputationsdaten zu unbekannten Dateien, die verdächtig erscheinen.

McAfee MOVE AntiVirus for Virtual Desktops bietet nicht nur Malware-Scans, sondern enthält auch eine Desktop-Firewall sowie erweiterten Speicherschutz, um böswillige Aktivitäten zu blockieren und die Dateiintegrität zu gewährleisten. Um die Benutzer vor riskanten Webseiten zu warnen, die das Abbild im laufenden Betrieb mit Malware verseuchen können, bietet die McAfee-Lösung Web-Reputationswarnungen sowie richtlinienbasierte Kontrollmöglichkeiten für die Web-Nutzung. Zusammen reduzieren diese Tools die Angriffsfläche Ihrer virtualisierten Systeme. Für stärkeren Schutz können zusätzliche Tools wie Anwendungs-Whitelists hinzugefügt werden, die Ausfälle durch unerwünschte Anwendungen oder Malware verhindern.

Sicherheit im Netzwerk

Virtualisierung verändert auch den Sicherheitsansatz im Unternehmensnetzwerk. Wenn eine physische Infrastruktur virtualisiert wird, macht das neue Strategien zur Schaffung und Verwaltung von Sicherheitsgrenzen erforderlich, da keine physischen Trennungen mehr vorhanden sind. Eine weitere Herausforderung ist die Portabilität von VMs und die Auswirkungen auf die Netzwerk-Sicherheitsrichtlinien. Unternehmen müssen unabhängig vom physischen Standort der virtualisierten Anwendungen und Server konsistente Netzwerksicherheit gewährleisten können.

McAfee bietet integrierte Netzwerksicherheit für physische und virtuelle Umgebungen. Die vollständige Integration der VMware vShield-Netzwerksicherheits-API ermöglicht der McAfee Network Security Platform die native Überprüfung virtueller Umgebungen. Damit können Sie Datenverkehr untersuchen und Richtlinien für und zwischen virtuellen Maschinen durchsetzen – unabhängig von deren physischem Standort. Zudem können Sie dank des nativen Zugriffs auf VMware vCenter-Tools die Integration der Netzwerksicherheit über virtuelle Umgebungen hinweg ermöglichen.

Zentrale Verwaltung

McAfee MOVE AntiVirus setzt auf die gleiche McAfee ePolicy Orchestrator®-Verwaltungsumgebung (McAfee ePO™), mit der Administratoren bereits McAfee-Tools für physische Endgeräte, Informationen und Netzwerksicherheit verwalten. In einem zentralen Richtlinien- und Konsolensystem kann jeder Administrator benutzerdefinierte Dashboards zur Überwachung seiner Daten und Aufgabengebiete erstellen sowie Berichte zu bestimmten Ressourcen generieren. Dazu gehören physische ebenso wie virtuelle Hosts, d. h. sowohl Endgeräte als auch Server. Diese Unterstützung für Rollen erleichtert die Einhaltung von Sicherheitsvorgaben für gemeinsam verwaltete virtualisierte Rechenzentren. In die McAfee ePO-Software können zudem über 100 weitere Produkte unserer Security Innovation Alliance-Partner integriert werden, mit denen IT-Abteilungen Arbeitsabläufe in der gesamten IT-Infrastruktur optimieren können.

Standardisierung oder Spezialisierung

Dank der Wahl zwischen agentenloser und Multiplattform-Implementierung werden aktuelle und zukünftige Anbieterlösungen unterstützt. Bei der Multiplattform-Variante wird auf jedem Gastabbild ein ressourcenschonender Agent installiert, der Richtlinien verwaltet und Scans durchführt. Für On-Access-Scans wird ein Offload-Scan-Server genutzt. Durch diesen Ansatz ist der parallele Einsatz von Citrix-, Microsoft-, VMware- und Microsoft-Hypervisoren möglich, was stärkere Flexibilität sowie die Unterstützung unterschiedlicher Benutzerumgebungen erlaubt.

Unsere agentenlose Alternativlösung integriert sich tief in VMware, damit Sie Ihre Investition in Hypervisor-Technologie bestmöglich nutzen können. McAfee MOVE AntiVirus nutzt VMware vShield Endpoint zum Scannen virtueller Maschinen außerhalb der Gastabbilder. Dabei befindet sich im Abbild selbst keinerlei McAfee-Software. VMware vMotion wird dazu verwendet, gescannte VMs von einem Host zum anderen zu migrieren, ohne den Benutzer oder die Scan-Systeme zu beeinträchtigen. Durch die Integration der McAfee ePO-Software in vCenter wird die Überwachung sowie die Reaktion auf Zwischenfälle optimiert.

Kontinuierliche Compliance

Richtlinien können mithilfe der zentralen McAfee ePO-Plattform nahtlos auf physischen und virtuellen Systemen durchgesetzt werden. Zur Optimierung der Compliance-Prozesse können Sie eine Auditorenansicht der relevanten Daten erstellen und ad-hoc oder nach Zeitplan Berichte für bestimmte Vorschriften generieren.

Der nächste Schritt

Jetzt haben Sie die Möglichkeit, die Sicherheit mit den Anforderungen der Virtualisierung in Einklang zu bringen. McAfee hat das Design und die Prozesse seiner Malware- und Endgeräteschutzlösungen für den Einsatz inner- und außerhalb von Virtualisierungslösungen optimiert. Aktive Benutzer werden nicht von Scans beeinträchtigt, während bei Sicherheits-Software-Updates sowie Signaturaktualisierungen die dynamischen Eigenschaften von Desktop- und Server-Abbildern berücksichtigt werden.

Unser flexibles Design gibt Ihnen die Möglichkeit, Ihre Virtualisierungsanbieter frei zu wählen und dennoch die Sicherheits- und Compliance-Standards einzuhalten. McAfee unterstützt Sie dabei, die Vorteile der Virtualisierung vollständig auszuschöpfen, ohne Ihre Benutzer und Daten den Gefahren durch Internetkriminelle auszusetzen. Wir arbeiten auch weiterhin an der Integration und Optimierung unseres breit aufgestellten Produktportfolios, damit Sie Virtualisierung in der gesamten Unternehmensumgebung einsetzen können, ohne auf stärkste Sicherheit und größtmögliche Effizienz verzichten zu müssen.

Weitere Informationen zu McAfee MOVE AntiVirus erhalten Sie unter www.mcafee.com/de/solutions/virtualization/virtualization.aspx oder von Ihrem örtlichen McAfee-Vertriebsrepräsentanten bzw. -Händler.

McAfee GmbH
Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.mcafee.com/de

[1] http://www.informationweek.com/news/storage/virtualization/232400150
[2] http://www.av-comparatives.org/images/stories/test/ondret/avc_od_aug2011.pdf

McAfee, das McAfee-Logo, McAfee ePolicy Orchestrator, McAfee ePO, McAfee VirusScan und McAfee Global Threat Intelligence sind Marken oder eingetragene Marken von McAfee, Inc. oder der Tochterunternehmen in den USA und anderen Ländern. Alle anderen Namen und Marken sind Eigentum der jeweiligen Besitzer. Die in diesem Dokument enthaltenen Produktpläne, Spezifikationen und Beschreibungen dienen lediglich Informationszwecken, können sich jederzeit ohne vorherige Ankündigung ändern und schließen alle ausdrücklichen oder stillschweigenden Garantien aus. Copyright © 2012 McAfee, Inc.
45601brf_virtualization_0512_fnl_ETMG